IntelliBox®-I/O 2100
User Guide

Part Number 900-474
Revision B March 2012

Copyright & Trademark

Ethernet is a trademark of XEROX Corporation. UNIX is a registered trademark of The Open Group. Windows is a trademark of Microsoft Corporation.

Warranty

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

Patents

Patent #4,972,470; other patents pending.

Contacts

Lantronix Corporate Headquarters

167 Technology Drive
Irvine, CA 92618, USA

Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-450-7249

Technical Support

Online: www.lantronix.com/support

Sales Offices

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

Disclaimer & Revisions

Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his or her own expense, will be required to take whatever measures may be required to correct the interference.

Attention: *This product has been designed to comply with the limits for a Class A digital device pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against such interference when operating in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance* with this guide, may cause harmful interference to radio communications.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil num'erique de la classe A est conforme 'a la norme NMB-003 du Canada.

Changes or modifications to this device not explicitly approved by Lantronix will void the user's authority to operate this device.

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

Revision History

Date	Rev.	Comments
May 2007	A	Initial Document.
March 2012	B	Updated for firmware version 1.4.0.0.

Contents

List of Figures

List of Tables

1: Preface

Purpose and Audience

This guide describes how to install, configure, use, and update the IntelliBox-I/O 2100. It is for those who will use the IntelliBox to network-enable their serial devices, primarily industrial automation end users, VARs, and integrators.

Summary of Chapters

The remaining chapters in this guide include:

Chapter	Description
2: Introduction	Main features of the IntelliBox device servers and the applications for which they are suited.
3: EventTrak	Overview of using the IntelliBox to monitor for events, take actions in response to events, and report on attached devices.
4: Installation	Instructions for getting the IntelliBox device server up and running. Includes a description of hardware components.
5: Getting Started	Instructions for starting DeviceInstaller and viewing current configuration settings. Introduces methods of configuring the IntelliBox.
6: Configuration Using the Web Manager	Instructions for using the web interface to configure IntelliBox device servers.
7: Network, Serial Line, Tunnel, and Modbus Settings	Instructions for using the web interface to configure network, serial line, tunnel, and Modbus settings.
8: Terminal and Host Settings	Instructions for configuring terminal and host settings.
9: Services Settings	Instructions for using the web interface to configure settings for DNS, SNMP, FTP, and other services.
10: Security Settings	Instructions for using the web interface to configure SSH and SSL security settings.
11: Maintenance and Diagnostics	Instructions for using the web interface to maintain the IntelliBox, view statistics, files, and logs, and diagnose problems.
12: Advanced Settings	Instructions for using the web interface to configure advanced settings: input/output, email, CLI, and XML.

Chapter	Description
13: EventTrak	Instructions for setting up EventTrak to monitor for, take actions in response to, and notify of events that occur on the attached device.
14: Updating Firmware	Instructions for upgrading the IntelliBox firmware.
A: Factory Default Configuration	Quick reference of the IntelliBox factory-default configuration settings.
B: Networking and Security	In-depth description of networking and network security as it relates to the IntelliBox device servers.
C: Modbus	Explanation and examples of the advantages of using Modbus/TCP with the IntelliBox.
D: Technical Specification	Table of technical data about the products.
E: Isolated I/O Specifications	Table of technical data about the digital I/Os and relay.
F:State Diagram Template	Provides a template for planning EventTrak settings.
G:Technical Support	Information about contacting Lantronix Technical Support.
H: Compliance	Information about the product's compliance with regulatory standards.
I: Warranty	Information about the product's warranty.

Additional Documentation

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

Document	Description
IntelliBox-I/O 2100 Device Server Quick Start Guide	Provides the steps for getting the IntelliBox up and running.
IntelliBox-I/O 2100 Device Server Command Reference	Describes how to configure the IntelliBox using Telnet or the serial port and summarizes the CLI and XML configuration commands.
Secure Com Port Redirector User Guide	Provides information for using the Lantronix Windows-based utility to create secure virtual com ports.

Note: *For detailed application examples, please go to the Lantroix web site.*

2: Introduction

This chapter introduces the Lantronix IntelliBox-I/O 2100 device server. It provides an overview of the product, lists its key features, and describes the applications for which it is suited.

The IntelliBox programmable device server provides a quick and easy method to automate remote equipment with real-time event management and reporting. Powered by Lantronix EventTrak™ technology, the IntelliBox enables customers to connect their industrial, commercial, medical, retail and security equipment to IP networks to proactively monitor and respond to events automatically. IntelliBox also has the ability to notify the end user of detected events and actions taken. Multiple serial ports, digital I/Os, and a relay enable real-time access for remote configuring, event monitoring, and controlling PLCs, motor drives, process controls, power monitoring equipment, barcode scanners, or virtually any RS-232, RS-422/485 factory floor device or discrete digital I/O device.

IntelliBox-I/O 2100 Overview

The IntelliBox is a compact, easy-to-use device server that gives you the ability to network-enable asynchronous RS-232 and RS-422/485 serial devices. It can deliver fully transparent RS-232/422 point-to-point connections and RS-485 multi-drop connections without requiring modifications to existing software or hardware components in your application.

Port 1 supports RS-232 devices, and Port 2 supports 422/485 devices by means of screw terminals. The IntelliBox supports two user-configurable digital I/Os and one relay for industrial sensing and control.

The IntelliBox provides automated and unattended event monitoring, response, and notification, and reporting of attached devices. You can program the IntelliBox to respond to external events automatically, for example, the IntelliBox can detect an event and automatically reboot the attached device, send email notifications, reconfigure the attached device, or trigger an alarm. The IntelliBox notifies users that it has detected an emergency, fixed the problem, and emailed or logged the details.

Figure 2-1 IntelliBox-I/O 2100 Device Server (Front)

Features

The following list summarizes the key features of the IntelliBox-I/O 2100.

- Monitor events in real-time
- Automatically respond to events with user-defined actions
- Query and gather data from attached device (sent to user via email and RSS feed)
- One RS-232 serial port
- One RS-422/485 serial port
- One RJ45 Ethernet port
- Two isolated configurable digital I/Os
- One isolated non-latching relay
- 4 MBytes Flash memory
- 2 MB (or 16 Mbit) SRAM (Static Random Access Memory)
- Based on Lantronix's Evolution OS™
- Supports secure data encryption by means of AES, SSH, or SSL sessions
- Supports three convenient configuration methods (web, command line, and XML)
- Supports Modbus/TCP, Modbus/RTU and Modbus/ASCII protocols
- Simultaneous communication from up to 16 Modbus CP masters
- Operational temp range -40°C to +75°C
- Wall mount tabs and optional dinrail mount clip

Typical Devices

Examples of typical devices that can connect to the IntelliBox digital I/Os:

- Proximity Sensor

- Current sensor
- Magnetic sensor
- Float sensor
- Pressure sensor
- Infra-red sensor
- Photoelectric sensors (LED & Laser)
- Ultrasonic sensor

Typical serial devices that the IntelliBox can automatically monitor and control:

- Phone systems (PBX)
- Fire alarm panels
- Heating and Air-conditioning (HVAC)
- PLCs
- Projectors
- HVAC (Heating , Ventilation and Air conditioning)
- Security Cameras
- Access control panels
- Proximity Readers
- Card readers

EventTrak™ Overview

Automated Monitoring and Control

IntelliBox incorporates EventTrak Technology to monitor and track activity and events on the attached equipment. When it detects an event, the IntelliBox automatically responds with user-defined actions. This enables the IntelliBox to fix problems before they become emergencies. After an event occurs, the IntelliBox can email the user with information on the event and the actions it took.

Automated Reporting

With EventTrak's automated reporting feature, the IntelliBox queries attached devices at specified times to gather information. After gathering the information, IntelliBox imbeds the data in an email and send it to the user or posts the data to a web page using an RSS feed. From a single web browser, you can monitor hundreds of devices in this way. IntelliBox also scans the gathered data for user-specified information. If it detects the information, IntelliBox flags the email as "important" and can take preemptive action that the user has defined.

Evolution OS™

IntelliBox device servers incorporate Lantronix's Evolution OS™. Key features of the Evolution OS™ include:

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

Web-Based Configuration and Troubleshooting

Built upon popular Internet-based standards, the IntelliBox 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 twin advantages of decreased downtime (based on the troubleshooting tools) and the ability to implement configuration changes easily (based on the configuration tools).

In addition, users can load their own web pages onto the IntelliBox to facilitate monitoring and control of their own serial devices that are attached to the IntelliBox.

Command-Line Interface (CLI)

Making the edge-to-enterprise vision a reality, the IntelliBox with the Evolution OS™ uses industry-standard tools for configuration, communication, and control. For example, the Evolution OS™ uses a Cisco®-like command line interface (CLI) whose syntax is very similar to that used by data center equipment such as routers and hubs.

SNMP Management

The IntelliBox 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 IntelliBox device servers.

XML-Based Architecture and Device Control

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

Really Simple Syndication (RSS)

The IntelliBox supports Really Simple Syndication (RSS), a rapidly emerging technology for streaming and managing on-line content. The IntelliBox queries and gathers data from the attached devices and makes it available through RSS feeds. 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 IntelliBox 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.

With built-in SSH and SSL, secure communications can be established between the IntelliBox serial ports and the remote end device or application. 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.

With SSH and SSL, IntelliBox 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 IntelliBox has robust defenses to hostile Internet attacks, such as denial of service (DoS), which can take down the network. Moreover, the IntelliBox cannot bring down other devices on the network.

The IntelliBox 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 by means of 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 instead communicate over an Ethernet network or the Internet.

The IntelliBox also supports a variety of popular cipher technologies including:

- Advanced Encryption Standard (AES)
- Triple Data Encryption Standard (3DES)
- RC4
- Hashing algorithms such as Secure Hash Algorithm (SHA-1) and MD5

Troubleshooting Capabilities

The IntelliBox 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 IntelliBox, including CPU utilization and total stack space available.

Applications

IntelliBox device servers deliver simple, reliable, and cost-effective network connectivity for all your serial devices and address the growing need to connect individual devices to the network over industry-standard Ethernet connections. The IntelliBox is ideal for a variety of applications, including:

- Building automation/security
- Industrial automation
- Medical/healthcare
- Retail automation/point-of-sale
- Traffic management

These applications are described below.

Building Automation/Security

Automating, managing, and controlling many different aspects of a building is possible with the IntelliBox. It can overcome the hurdle of stand-alone networks or individual control systems that are not able to communicate with each other, and not able to share vital data, in a cost effective way.

The IntelliBox can automatically manage equipment and devices centrally over a new or existing Ethernet network to improve the safety and comfort of building occupants, while lowering heating, ventilating, air conditioning (HVAC), lighting, and overall energy operating costs through centralized management and monitoring.

Industrial Automation

Today's manufacturing facilities face the common challenges of productivity improvements, inventory management, and quality control. From warehouse to automotive environments, the need to attach and manage the following devices, whether new or legacy continues to grow:

- Programmable Logic Controllers (PLCs), Computer Numeric Control and Direct Numeric Control (CNC/DNC) equipment, process and quality-control equipment
- Pump controllers
- Bar-code readers and scanners, operator displays, scales, and weighing stations
- Printers, machine-vision systems, and other types of manufacturing equipment

The IntelliBox is well suited to deliver network connectivity and management to all of these devices.

Medical/Healthcare

Hospitals, clinics, and laboratories face a rapidly growing need to deliver medical information accurately, quickly, and easily, whether at bedside, the nurse's station, or anywhere in the facility. The goal to improve healthcare services, however, is balanced with the need to keep the bottom line from exceeding already constrained budgets.

The IntelliBox can network enable medical equipment and devices using the hospital's existing Ethernet network to improve patient care and slash operating costs. This enables medical staff members to easily monitor and control equipment over the network, whether it is located at the point of care, in a laboratory, or somewhere else in the building, all resulting in improved quality of service and reduced operational costs.

Retail Automation/Point-of-Sale

Having the right solution in the store to manage deliveries, track orders, and keep pricing current are all improvements that the IntelliBox can offer to make retail operations more successful. From big to small, one store to thousands of outlets, the IntelliBox can empower point-of-sale (POS) devices to share information across the network effectively.

With the IntelliBox, retailers can increase and streamline productivity quickly and easily by network-enabling serial devices like card swipe readers, bar-code scanners, scales, cash registers, and receipt printers.

Traffic Management

With the ubiquity of Ethernet networks, managing cities over Ethernet is now within reach. The IntelliBox provides an easy conversion from serial ports on traffic cameras, billboards, and traffic lights to Ethernet. The IntelliBox obviates the need for long-haul modems and enables the management of traffic equipment over the network.

Product Information Label

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

- Bar Code
- Serial Number
- Part Number
- Country of Origin
- Product Revision
- Hardware Address (MAC Address)

Figure 2-1 Product Label

3: EventTrak

Overview

Automated Device Management, Monitoring, and Control

The IntelliBox with EventTrak technology enables you to automate tasks related to your industrial and commercial equipment that normally require human input or intervention. Devices typically require manual monitoring and control, necessitating users to periodically check the device or wait for critical equipment failure before taking action.

You can configure the IntelliBox to monitor equipment and respond to events automatically. Upon detecting an event, the IntelliBox fixes a problem before it becomes an emergency and sends an email to the designated user indicating that the IntelliBox proactively discovered and fixed the problem.

Automated Reporting

The IntelliBox consolidates monitoring and reporting of devices, enabling you to automate data capture. Previously, you had to query and review the output of each device separately. With the IntelliBox's easy-to-use web-based interface, you configure the IntelliBox to query the attached devices at configurable intervals and gather the data returned. Users receive data from the attached equipment by email or RSS feed so they can review the data at their leisure or monitor hundreds of devices aggregated on a single page of an RSS client application or RSS-enabled web browser.

With EventTrak's automated monitoring and control functionality, the IntelliBox scans incoming data for specific information, and when it detects that information, takes specific actions, including flagging the email being sent as "important." Thus users reviewing reports from many devices avoid sifting through hundreds of emails and focus on the flagged emails.

Examples

Following are examples of how the IntelliBox with EventTrak can be used.

Industrial

Industrial automation and building automation can use the digital I/O and serial port hardware on the IntelliBox. As there are hundreds of different types of digital sensors, there are also hundreds of different applications for which the IntelliBox can be used. Typical events that the IntelliBox detects include triggers from specific sensors connected to the IntelliBox's digital inputs and user-specified data detected on the IntelliBox's serial ports. Following are some examples.

Detect fluid levels (float sensor connected to the IntelliBox's digital input)

- At low level, the IntelliBox triggers its relay to start a fluid pump. If the fluid lever is abnormally low, the IntelliBox sends an email indicating the problem and the action taken.
- At high level, IntelliBox triggers its relay to stop a fluid pump or open a valve to release the fluid. If the fluid level is abnormally high, the IntelliBox sends an email indicating the problem and the action taken.

Detect pressure (using a digital pressure sensor connected to the IntelliBox digital input)

- Shuts off the valve or opens an emergency valve when it detects high pressure.
- Turns off a pump or motor.
- Notifies the user by email.

Monitor a PLC (connected to the IntelliBox's serial port)

- Queries the device.
- Sends reports by email and RSS Feed (monitor using an RSS client or a web browser).
- Scans for specific data. When the IntelliBox detects the data, it can automatically:
  - Reconfigure the attached device
  - Soft reboot the attached device (through the serial port)
  - Hard reboot the attached device (using the relay)
  - Trigger an alarm (using the relay)

Other Examples

Security

- Controls a camera using proximity sensors (e.g., zoom, pan, and rotate).

Security and Theft Prevention

- Monitors an attached device.
- If the device disconnects, sends an email or triggers an alarm (for example).

HVAC Systems

- Preemptively notifies the user of equipment failure.
- Initiates emergency shutdown or startup.
- Automatically reports HVAC status (email with attached data).
- Performs consolidated monitoring of many HVAC systems (RSS feed to a web browser).

Inputs and Outputs

EventTrak monitors the IntelliBox's various inputs and outputs.

Inputs: Include digital inputs that EventTrak triggers and detects, serial data that it receives and analyzes, and ping responses that it detects.

Outputs: Include digital outputs being triggered, serial data being sent, pings being sent, email being sent, and RSS feeds. Using a simple web interface, you can configure the IntelliBox to initiate an output, wait for one or more expected inputs (an event or chain of events), and take one or more actions (outputs) based on user-definable criteria.

Events

An event is an occurrence or multiple occurrences that the EventTrak detects. For example, it:

- Recognizes a configurable string from the serial port.
- Detects a triggered digital input.
- Monitors serial ports for activity (in or out). Registers an event if the serial port is idle until a user-configurable timeout ends
- Monitors a ping response. Registers an event if it receives no response

Actions

An action is the IntellliBox's response to one or more events. For example, it:

- Sends an email (with optional data from the attached device).
- Switches a relay for a configurable amount of time.
- Sends a string out the serial port
- Triggers a digital output.
- Triggers a separate task

Chain Definitions

Definitions or Monitoring and Control Settings

A chain definition is the combination of settings that define what EventTrak will monitor for and what actions it will take in response to detected events. This includes all the settings on the Monitoring and Control pages under the EventTrak 1 or EventTrak 2 configuration pages. For example, one or more tasks within EventTrak may require the IntelliBox to do one or more of the following:

- Wait for a specified amount of time before continuing to the next step
- Wait for an event to be detected before continuing to the next step
- Send an initial action at the beginning of each step within a task. For example:

- Ping a configurable destination address
- Set a digital output switch
- Set the relay to closed or open

- Take action in response to a detected event or an expired timeout. For example:
  - Send an email (with or without serial data from attached device)
  - Update an RSS feed with user-specified data including attached device data if needed
  - Send a string (or multiple strings) out a serial port
  - Clear the serial line receive buffer
  - Fire a trigger (event) on another task

Automated Reporting

With the IntelliBox, you can use EventTrak settings to schedule automated reporting of devices.

4: Installation

This chapter describes how to install the IntelliBox device server.

Package Contents

Your IntelliBox-I/O 2100 package includes the following items:

- One IntelliBox-I/O 2100 device server
- One DB9F-to-3.5 mm 7-position screw terminal block, RoHS (Lantronix PN 500-172-R)

Note: *The serial cable provided is for configuration set-up (female DB9 to be connected to a host computer).*

- A printed Quick Start Guide

User-Supplied Items

To complete your IntelliBox installation, you must provide:

- RS-232 and/or RS-422/485 serial devices or digital I/O devices that require network connectivity. One IntelliBox serial port supports a directly connected RS-232 serial device; one serial port supports an RS-422/485.

Note: *The IntelliBox supports digital I/Os and has a relay, so you do not necessarily need to supply a serial device.*

- An available connection to your Ethernet network and an Ethernet cable.
- 9-30 VDC or 9-24 VAC connected to the IntelliBox power input.
- Chassis (earth) ground

Caution: *Even though chassis ground is not required for operation, it is mandatory for protection against transient voltages and ESD. Chassis ground is to be connected to earth.*

Identifying Hardware Connectors

Figure 4-1 shows the hardware components on the front of the IntelliBox, and *Figure 4-2* shows the hardware connectors on the back of the IntelliBox.

Figure 4-1 Front View of the IntelliBox-I/O 2100

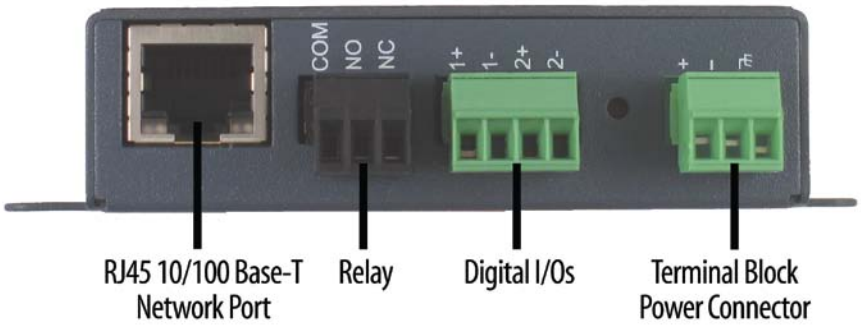
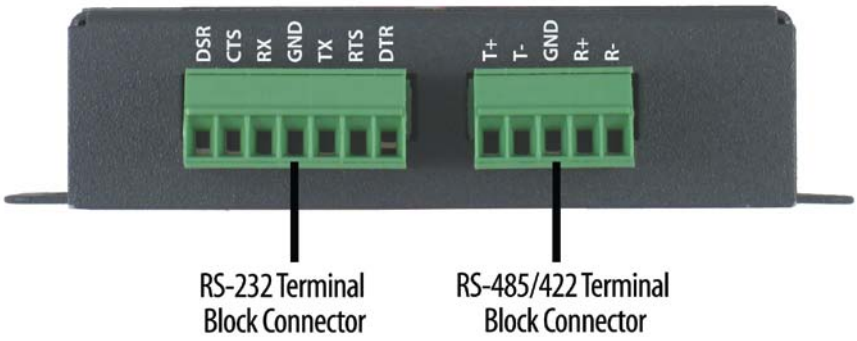


Figure 4-2 Back View of the IntelliBox-I/O 2100



The bottom of the IntelliBox (not shown) has a product information label. This label contains the following information:

- Bar code
- Serial number
- Product ID (name)
- Product description
- Hardware address (also referred to as Ethernet or MAC address)
- Agency certifications

Screw Terminal Serial Connectors

The back of the IntelliBox-I/O 2100 has two terminal block serial ports. These screw-down blocks are set for easy adaptability to industrial environments. Screw down stripped wire into these blocks in wiring locations corresponding to signal names appearing on the case. You do not need special cables to attach to the IntelliBox.

- Serial port 1 supports RS-232 devices.
- Serial port 2 supports RS-422 and RS-485 (4-wire/2-wire) serial devices. See *Figure 4-4* for pin assignments.

Port 1 is configured as DTE and supports baud rates up to 230,400 baud. Serial ports have 15kv ESD protection.

Note: *Shielded cable may be required to avoid character framing errors at high speeds.*

Table 4-1.Serial 1 Pin Assignments

Pin #	Pin Name	Description
1	DSR1	Input
2	CTS1	Input
3	RXD1	Input
4	GND	Ground
5	TXD1	Output
6	RTS1	Output
7	DTR1	Output

Table 4-2 Serial 2 Pin Assignments

Pin #	Pin Name	Description
1	TX2+ / (+)	4-Wire: TX2+. Output from IntelliBox-I/O 2100. 2-Wire: (+)
2	TX2- / (-)	4-Wire: TX2-. Output from IntelliBox-I/O 2100. 2-Wire: (-)
3	GND	Ground
4	RX2+ / DNU	4-Wire: RX2+. Input to IntelliBox-I/O 2100. 2-Wire: Do not use, leave open
5	RX2- / DNU	4-Wire: RX2-. Input to IntelliBox-I/O 2100. 2-Wire: Do not use, leave open

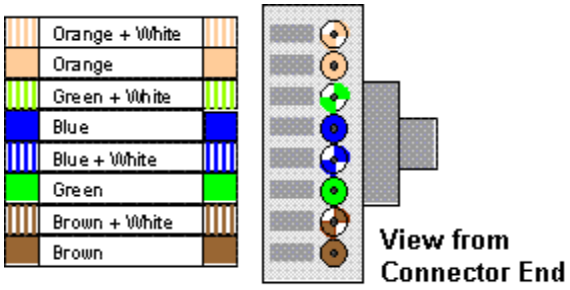
Note: *There is an on-board 120-ohm termination option in 2-wire mode configured using the Web Page, CLI, or XML.*

Ethernet Port

The front panel of the IntelliBox-I/O 2100 provides an RJ45 Ethernet port. This port can connect to an Ethernet (10 Mbps) or Fast Ethernet (100 Mbps) network. There are two bi-color (green/amber) LEDs that indicate speed (10/100 MHz) and activity (full/half duplex). (See *Figure 4-9*.) You can configure the IntelliBox to operate at a fixed Ethernet speed and duplex mode (half- or full-duplex) or auto-negotiate the connection to the Ethernet network.

The drawing below shows a typical RJ45 connector. The color is not standard but very typical of an Ethernet patch cable. Pin 1 is located at the top of the connector (orange + white). The view is from the end of the connector.

Figure 4-3.Typical RJ45 Connector



Terminal Block Power Connector

The front of the IntelliBox-I/O 2100 has a terminal block screw connector for attaching to an appropriate power source, such as those used in automation and manufacturing industries. The terminal block connector supports a power range from 9 to 30 VDC or 9 to 24 VAC.

Table 4-3 Power Input Port Pinouts

Pin #	Pin Name	Description
1	PWRIN+	Power Input, positive contact
2	PWRIN-	Power Input, negative contact
3	GND	Earth Ground

Notes:

- *Voltage input can be 9 to 30 VDC or 9 to 24 VAC. There are polarity indicators of the input. However, since the IntelliBox can accept VAC, polarity reversal still results in a normal operation (IntelliBox still operates normally if the positive contact is hooked to V-, and the negative contact is hooked to V+ of the power input).*
- *The power input port is isolated from the inner circuitry.*
- *Earth ground is not required for normal operation, but is essential and required for transient suppression, ESD protection, and EMC compliance.*

Digital I/Os

The unit has two digital I/Os (UL Class III or Class 2) that you can configure as either input or output. The digital I/Os are isolated from each other and from the inner circuitry of the IntelliBox using opto-isolators.

- **When digital I/Os are configured as inputs:** High-level input logic can be as low as 3 volts with 1 mA current drawn. For higher logic level input, for example 8V or more, a current-limiting resistor is required. The inputs are protected from polarity reversal.
- **When digital I/Os are configured as outputs:** This is a solid-state relay output; thus, it is not sensitive to polarity orientation and has low impedance.

For more information, see *E: Isolated I/O Specifications*.

Table 4-4 Digital I/O Pins

Pin #	Pin Name	Description
1	1+	2-wire configurable digital IO, positive contact, 1st port
2	1-	2-wire configurable digital IO, negative contact, 1st port
3	2+	2-wire configurable digital IO, positive contact, 2nd port
4	2-	2-wire configurable digital IO, negative contact, 2nd port

Relay Port

A 3-terminal relay-controlled dry contact NC, COM, NO (up to 8A) is on the front of the unit. The relay is for SELV applications only (UL Class III or Class 2). The relay contacts are isolated from the inner circuit of the IntelliBox.

Pin 1 = COM, PIN 2 = NO, PIN 3 = NC due to recent change

Table 4-5 Relay Port Pins

Pin #	Pin Name	Description
1	COM	Common contact
2	NO	Normally open when power ON (closed to COM when power is OFF)
3	NC	Normally closed to COM when power ON (open when power is OFF)

LEDs

The IntelliBox has the following LEDs:

Table 4-6 Ethernet Port LEDs

LEDs	Descriptions
Left – Green ON	Link Established – 100BASE-T
Left – Amber ON	Link Established – 10BASE-T
Right – Green ON	Full Duplex (Blinking = Activity)
Right – Amber ON	Half Duplex (Blinking = Activity)

Table 4-7 LEDs on Top Cover

LEDs	Descriptions
Power/Diagnostic - Blue	Power Indicator and Diagnostic
RX Serial 1 - Green	Serial 1 Received Data Activity
TX Serial 1 - Amber	Serial 1 Transmitted Data Activity
RX Serial 2 - Green	Serial 2 Received Data Activity
TX Serial 2 - Amber	Serial 2 Transmitted Data Activity

Reset Button

The reset button is on the front panel. You can use it to reboot the unit or reload factory defaults.

To reboot:

1. Press and hold the reset button for about 3 seconds. The blue power LED blinks quickly.
2. When the fast blinks stop, release the button. When the unit reboots, the power LED changes from a fast blink to a solid ON.

To restore factory defaults:

1. Press and hold the reset button for about 11 seconds. The LED blinks quickly for about 3 seconds, then comes on for about 5 seconds, then blinks slowly for about 2 seconds.
2. When the slow blinks stop, release the button.

Physically Installing the IntelliBox-I/O 2100

Finding a Suitable Location

- Place the IntelliBox on a flat horizontal or vertical surface. The IntelliBox comes with mounting brackets installed for vertically mounting the unit, for example, on a wall.
- If using AC power, avoid outlets controlled by a wall switch.

Connecting the IntelliBox-I/O 2100

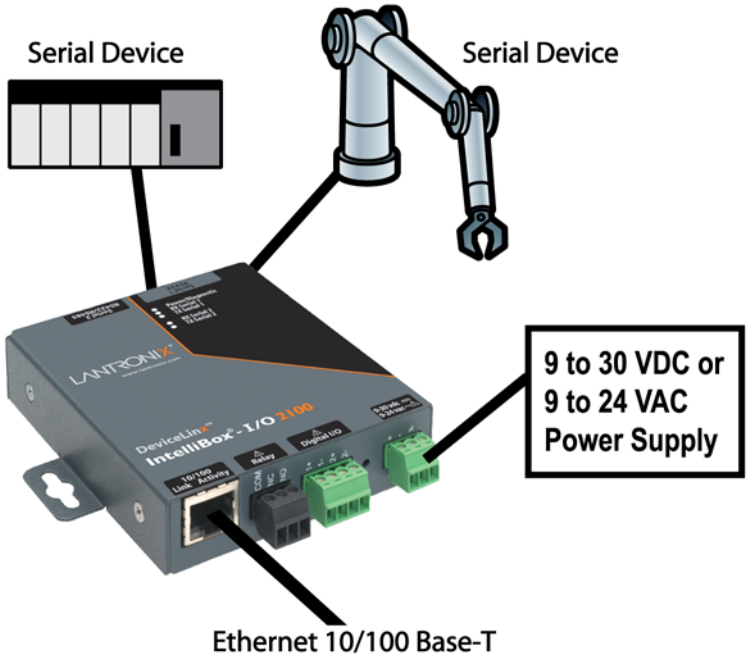
Observe the following guidelines when attaching serial devices:

- Serial port 1 supports RS-232 devices.
- Serial port 2 supports RS-422 and RS-485 (4-wire/2-wire) serial devices. See *Figure 4-4* for pin assignments.

To connect the IntelliBox-I/O 2100 to one or more serial devices:

> ***Note:*** *We recommend you power off the serial devices that will be connected to the IntelliBox.*

Figure 4-4 Example of the IntelliBox-I/O 2100 Connections



1. Connect serial devices to screw-down connectors.
2. Connect an Ethernet cable between the IntelliBox-I/O 2100 Ethernet port and your Ethernet network.
3. Attach the power source to the terminal block connector on the front of the IntelliBox. The terminal block connector supports a power range of 9 to 30 VDC or 9 to 24 VAC.

   The IntelliBox powers up automatically. After power-up, the self-test begins and Evolution OS™ starts.
4. Power up all connected serial devices.

5: Getting Started

Using DeviceInstaller

DeviceInstaller is a free utility program provided by Lantronix that discovers, configures, upgrades and manages Lantronix Device Servers. To use the DeviceInstaller utility, first install the latest version from the downloads page on the Lantronix web site www.lantronix.com/downloads.

Note: *You can also assign an IP address and other basic network settings. For instructions, see the DeviceInstaller Online Help.*

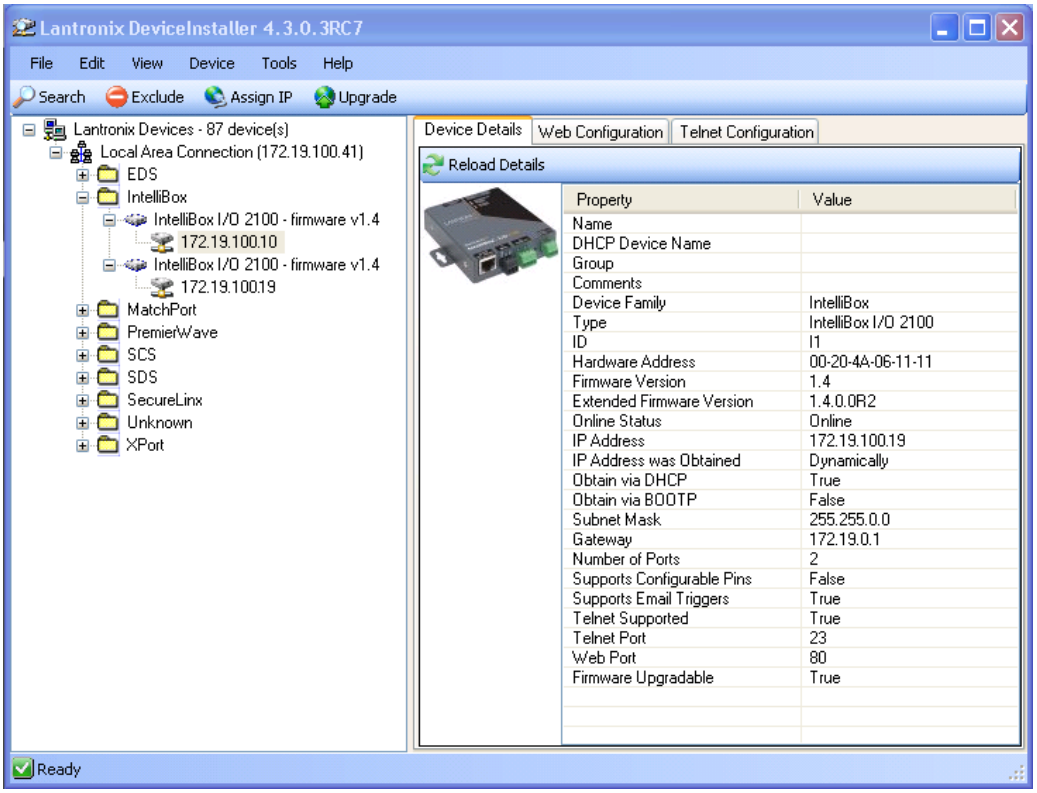
Starting DeviceInstaller

Follow the prompts to install DeviceInstaller.

To run DeviceInstaller:

1. From the Windows Start menu, click **Start→ All Programs, Lantronix→ DeviceInstaller→DeviceInstaller**.
2. When DeviceInstaller starts, it will perform a network device search. To perform another search, click **Search**.
3. Expand the IntelliBox folder by clicking the + symbol next to the folder icon. The list of available Lantronix IntelliBox devices appears.
4. Expand the **IntelliBox-I/O 2100** folder. The list of available devices displays.
5. To view the configuration of the IntelliBox, select the unit by clicking its IP address.

Figure 5-1 Lantronix DeviceInstaller



Viewing IntelliBox-I/O 2100 Properties

To view the IntelliBox's properties, in the right window, click the **Device Details** tab. The current properties for the IntelliBox display. Figure 5-2 lists the IntelliBox properties and whether they are user configurable or read only.

***Note**: On this screen, you can change **Group** and **Comments**. You can only view the remaining properties. To change them, use one of the IntelliBox configuration methods described in Configuration Methods.*

Table 5-1 IntelliBox-I/O 2100 Properties

Property	Description
Name	Displays the name of the IntelliBox, if configured.
DHCP Device Name	The name associated with the IntelliBox's current IP address, if the IP address was obtained dynamically.
Group	Enter a group to categorize the IntelliBox. Double-click the field, enter the value, and press **Enter** to complete.
Comments	Enter comments for the IntelliBox. Double-click the field, enter the value, and press **Enter** to complete.
Device Family	Displays the IntelliBox's device family type as **IntelliBox**.
Type	Displays the device type as **IntelliBox I/O 2100**.
ID	Displays the IntelliBox's ID embedded within the box.
Hardware Address	Displays IntelliBox's hardware (MAC) address.
Firmware Version	Displays the firmware currently installed on the IntelliBox.
Extended Firmware Version	Displays the full version of firmware currently installed on the IntelliBox.
Online Status	Displays the IntelliBox status. Online = the IntelliBox is online. Offline = the IntelliBox is offline. Unreachable = the IntelliBox is on a different subnet. Busy = the IntelliBox is currently performing a task.
IP Address	Displays the IntelliBox's current IP address. To change it, click the **Assign IP** button on the DeviceInstaller menu bar.
IP Address was Obtained	Appears "Dynamically" if the IntelliBox automatically received an IP address (e.g., from DHCP). Appears "Statically" if the IP address was configured manually. If the IP address was assigned dynamically, the following fields appear: Obtain via DHCP with values of True or False. Obtain via BOOTP with values of True or False.
Obtain via DHCP	Indicates whether the IP address was assigned via DHCP, with values of True or False.
Obtain via BOOTP	Indicates whether the IPaddress was dynamically assigned via BOOTP, with values of True or False.
Subnet Mask	Displays the subnet mask specifying the network segment on which the IntelliBox resides.

Property	Description
Gateway	Displays the IP address of the router of this network. There is no default.
Number of Ports	Displays the number of ports on this IntelliBox.
Supports Configurable Pins	Displays **False**.
Supports Email Triggers	Displays **True**.
Telnet Supported	Displays whether Telnet is supported on this IntelliBox.
Telnet Port	Displays the IntelliBox's port for Telnet sessions.
Web Port	Displays the IntelliBox's port for Web Manager configuration.
Firmware Upgradeable	Displays **True** if the IntelliBox firmware is upgradeable. For firmware-upgrade instructions, see *14: Updating Firmware*.

Note: *These parameters are stored on the computer running DeviceInstaller.*

Configuration Methods

When your IntelliBox boots for the first time, it automatically loads its factory-default configuration settings. For a list of the factory-default configuration settings, see *A: Factory Default Configuration*.

For convenience, there are three ways to configure the IntelliBox.

- Using the Web Manager interface
- Using the CLI through an SSH/Telnet session or an IntelliBox serial port.
- Using the XML interface

These unified configuration methods provide access to all features, giving you the same level of control over the IntelliBox regardless of the configuration method you choose.

Configuring from the Web Manager Interface

With this method, you can use a web browser to configure the IntelliBox using a web-based graphical point-and-click interface. The advantages to this method are ease of use and location independence. With this method, you can configure the IntelliBox from any location that has access to a web browser and the Internet.

For more information, see *6: Configuration Using the Web Manager*.

Configuring via an SSH/Telnet Session or Serial Port Using the CLI

The IntelliBox provides a command-line interface (CLI) designed to enable the configuration and systems management functions that can also be performed through the Web Manager and XML interfaces. To configure the IntelliBox using the CLI, you must either start an SSH or Telnet session or use a terminal or a computer attached to one of the IntelliBox serial ports.

The difference between the SSH/Telnet and serial interfaces is the physical connection paths to the IntelliBox. With an SSH/Telnet session, you can configure the unit without having to be in the same location as the IntelliBox. The serial-interface method, however, requires a terminal or computer to be attached to an available IntelliBox serial port. This means the terminal or computer must be in the same location as the IntelliBox.

For more information, refer to the **IntelliBox-I/O 2100 Command Reference**, which is available on the Lantronix web site (www.lantronix.com).

Configuring from the XML Interface

The IntelliBox also provides an XML interface that can be used to perform configuration and systems-management functions. This configuration method lets you automate the configuration process using XML configuration files. This method is particularly convenient if you have multiple IntelliBox device servers that will use the same configuration settings, because you can define a configuration profile that can be imported by, and shared among, your other IntelliBox device servers.

For more information, refer to the **IntelliBox-I/O 2100 Command Reference**, which is available on the Lantronix web site (www.lantronix.com).

6: Configuration Using the Web Manager

This chapter describes how to configure the IntelliBox-I/O 2100 using the Web Manager, Lantronix's browser-based configuration tool. The unit's configuration is stored in nonvolatile memory and retained without power. All changes take effect immediately, unless otherwise noted.

Accessing the Web Manager through a Web Browser

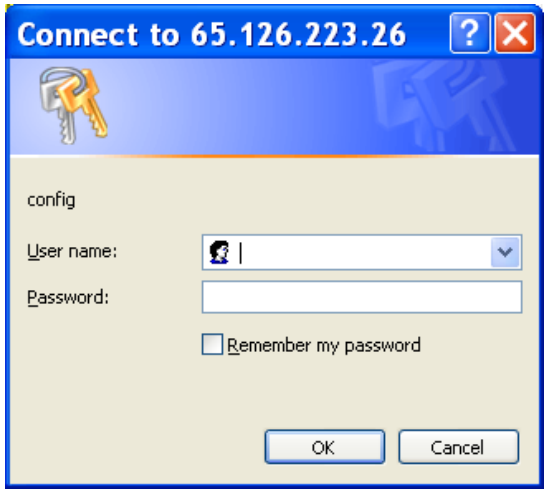
The following procedure describes how to log into the IntelliBox-I/O 2100 using a standard web browser.

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 later, Internet Explorer 5.5 and later, Mozilla Suite, Mozilla Firefox, or Opera.
2. Enter the IP address of the IntelliBox in the address bar. The IntelliBox's built-in security requires you to log in with your user name and password.

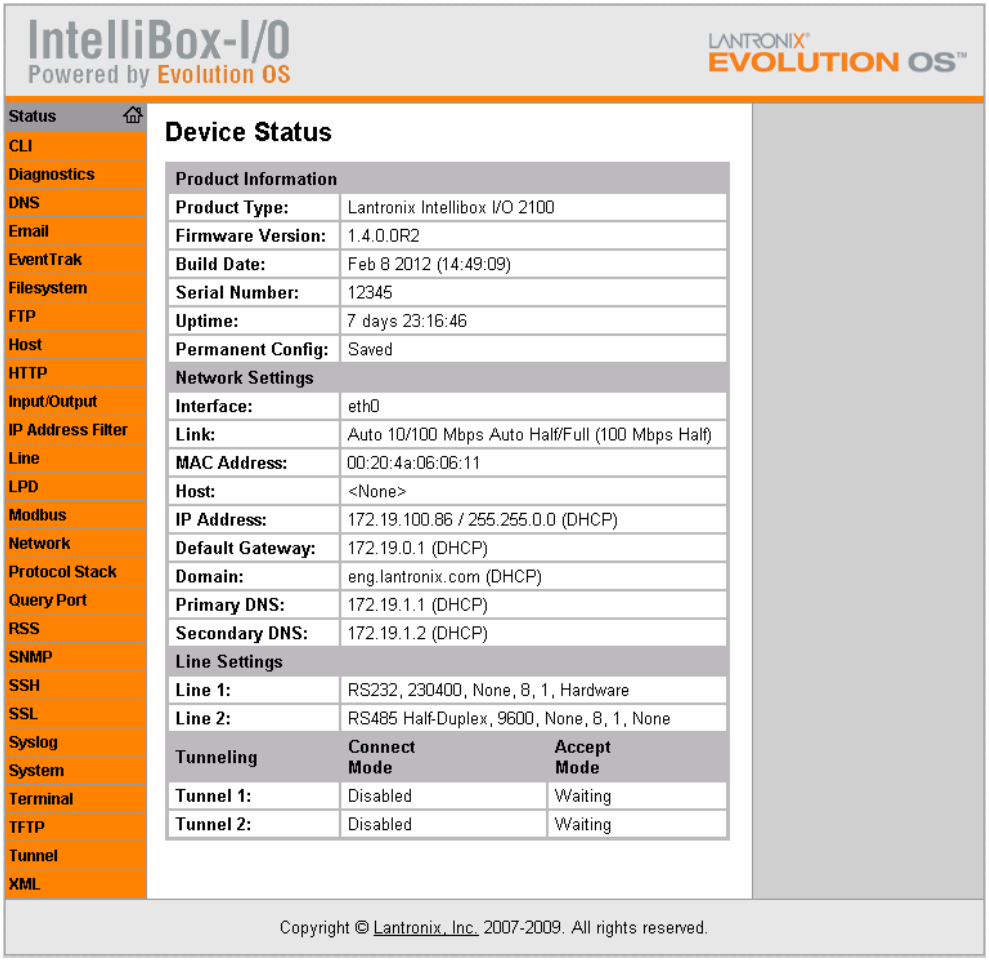
Figure 6-1 Prompt for User Name and Password



3. Enter your user name and password in the appropriate fields. The Device Status page displays (see *Figure 6-2*). This page is the Web Manager home page.

*Note: The factory-default user name is **admin** and the factory-default password is **PASS**. After you log in to the Web Manager, we recommend you use the FTP page to change the default FTP password, see the HTTP Authentication Page to change the HTTP authentication password, and the CLI Pages to change the CLI password.*

Figure 6-2 Web Manager Device Status Page



Navigating Through the Web Manager

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

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

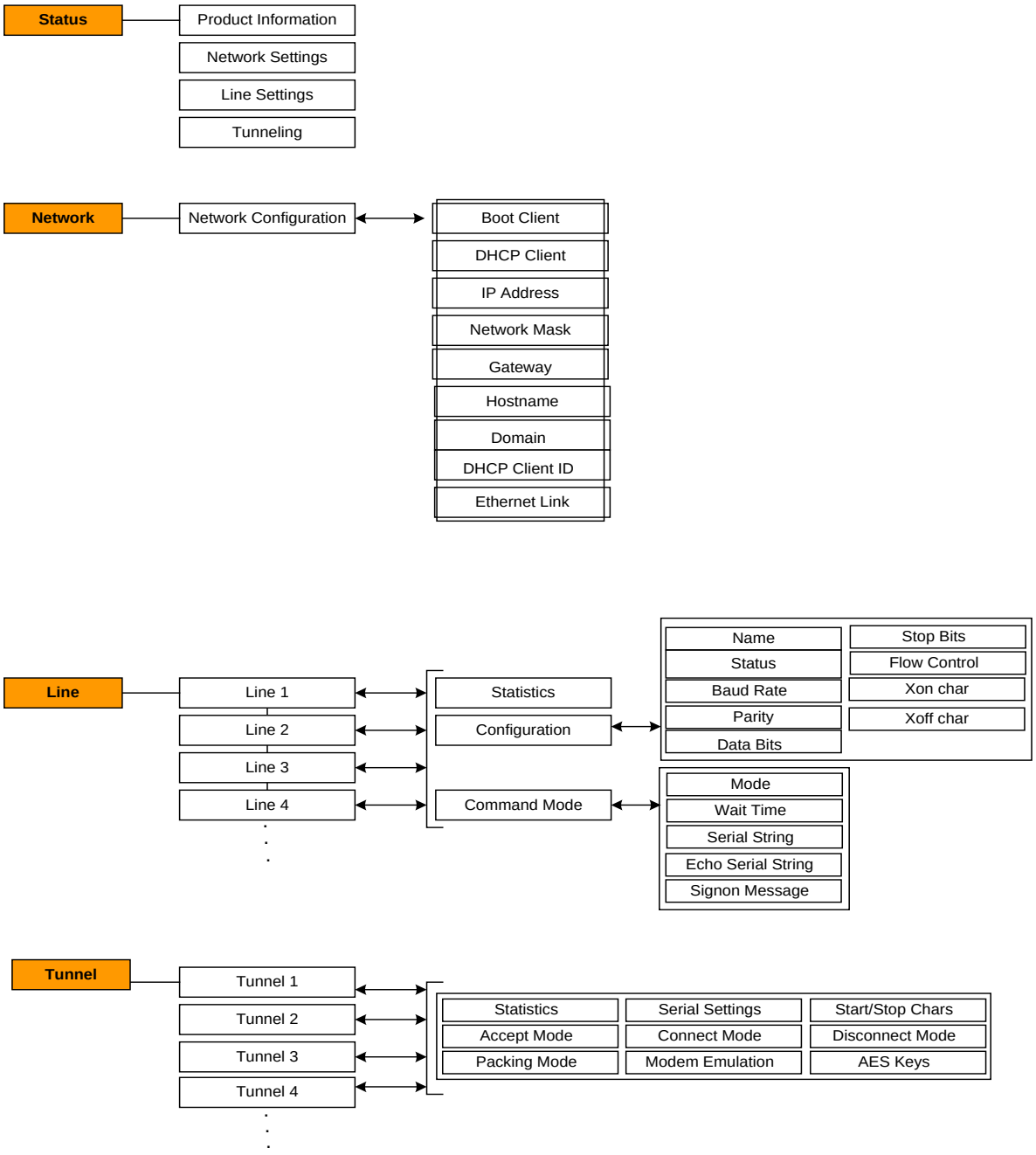
Figure 6-7 shows the structure of the multilevel Web Manager configuration pages.

Table 6-1 Summary of Web Manager Pages

Page	Description	See Page
Status	Displays IntelliBox product information and network, line, and tunneling settings.	*50*
CLI	Displays Command Line Interface (CLI) statistics and lets you change the current CLI configuration settings.	*125*
Diagnostics	Lets you perform various diagnostic procedures.	*107*
DNS	Displays the current configuration of the DNS subsystem and lets you change primary and secondary DNS servers.	*79*
Email	Displays email statistics and enables you clear the email log, configure email settings, and send an email.	*122*
EventTrak	Displays the current settings and enables you set up EventTrak to monitor for, take actions in response to, and notify of events that occur on the attached device.	*139*
Filesystem	Displays filesystem statistics and lets you browse the filesystem to create a file or directory, upload files using HTTP, copy a file, move a file, or perform TFTP actions.	*104*
FTP	Displays statistics and lets you change the current configuration for the File Transfer Protocol (FTP) server.	*82*
Host	Lets you view and change settings for a host on the network.	*78*
HTTP	Displays Hypertext Transfer Protocol (HTTP) statistics and lets you change the current configuration, authentication, and RSS settings.	*85*
Input/Output	Displays the current settings and lets you manage the input and output pins on the IntelliBox.	*120*
IP Address Filter	Lets you specify all the IP addresses and subnets that are allowed to send data to this device.	*138*
Line	Displays statistics and lets you change the current configuration and Command mode settings for the 2 serial lines of the IntelliBox.	*54*
LPD	Shows LPD (Line Printer Daemon) Queue statistics and lets you configure the LPD and print a test page.	*91*
Modbus	Displays the current connection status of the Modbus servers listening on the TCP ports and lets you add a second server.	*74*

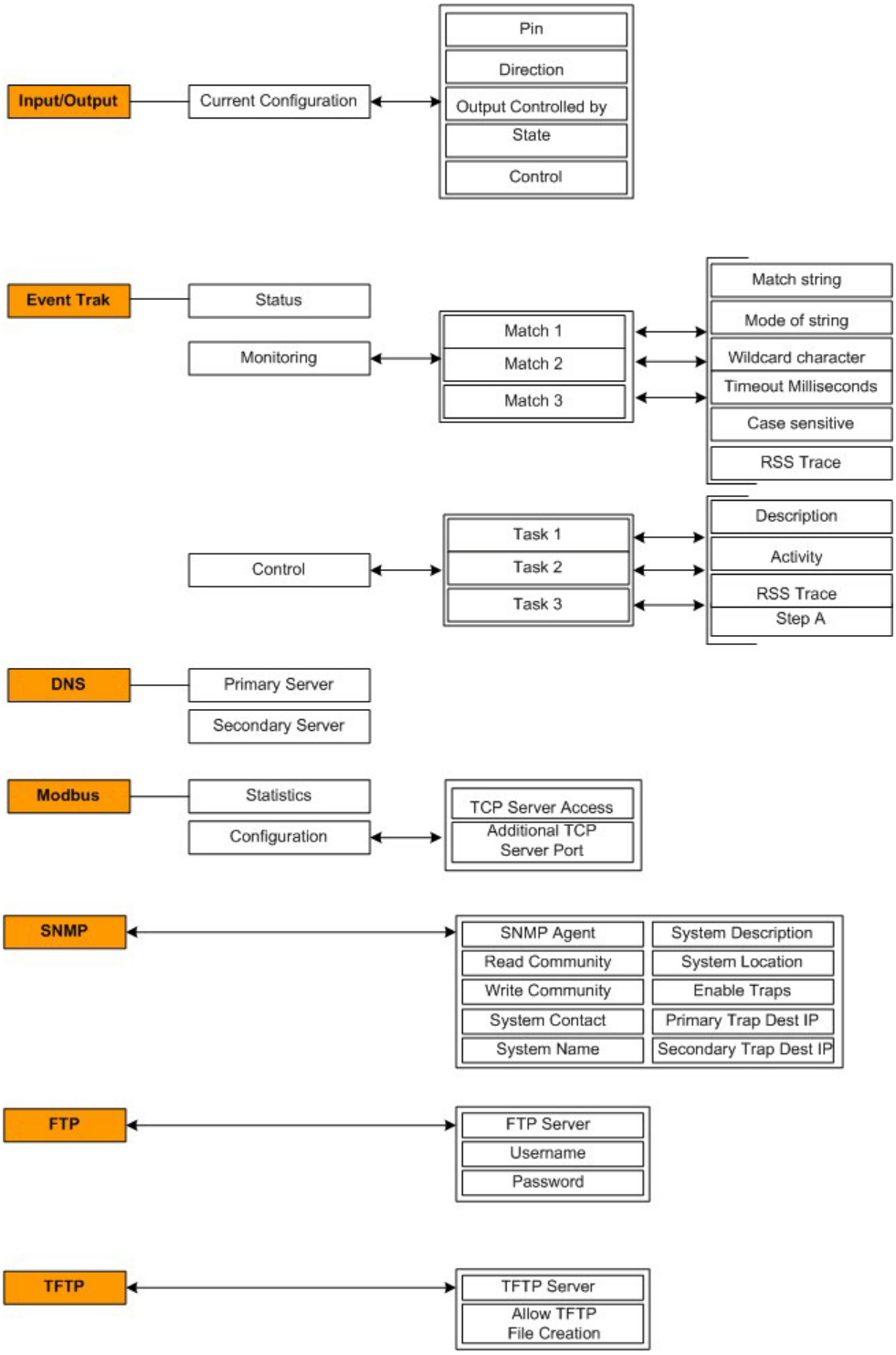
Page	Description	See Page
Network	Lets you configure the current network interface on the IntelliBox.	51
Protocol Stack	Lets you perform lower level network stack-specific activities.	135
Query Port	Displays and lets you change configuration settings for the query port.	118
RSS	Enables you to configure the RSS feed that contains up-to-date information about configuration changes.	90
SNMP	Displays and lets you change the current Simple Network Management Protocol (SNMP) configuration settings.	80
SSH	Displays and lets you change the configuration settings for SSH server host keys, SSH server authorized users, SSH client known hosts, and SSH client users.	165
SSL	Lets you upload an existing certificate or create a new self-signed certificate.	101
Syslog	Lets you specify the severity of events to log and the server and ports to which the syslog should be sent.	84
System	Lets you reboot the IntelliBox, restore factory defaults, upload new firmware, change the IntelliBox's long and short names, and change the time setting.	117
Terminal	Lets you change current settings for a terminal.	76
TFTP	Displays statistics and lets you change the current configuration for the Trivial File Transfer Protocol (TFTP) server.	83
Tunnel	Displays the current connection statistics and lets you change the current configuration settings for 2 tunnels for the IntelliBox.	60
XML	Lets you export XML configuration and status records, and import XML configuration records.	129

Figure 6-3 Web Manager Menu Structure (1 of 5)



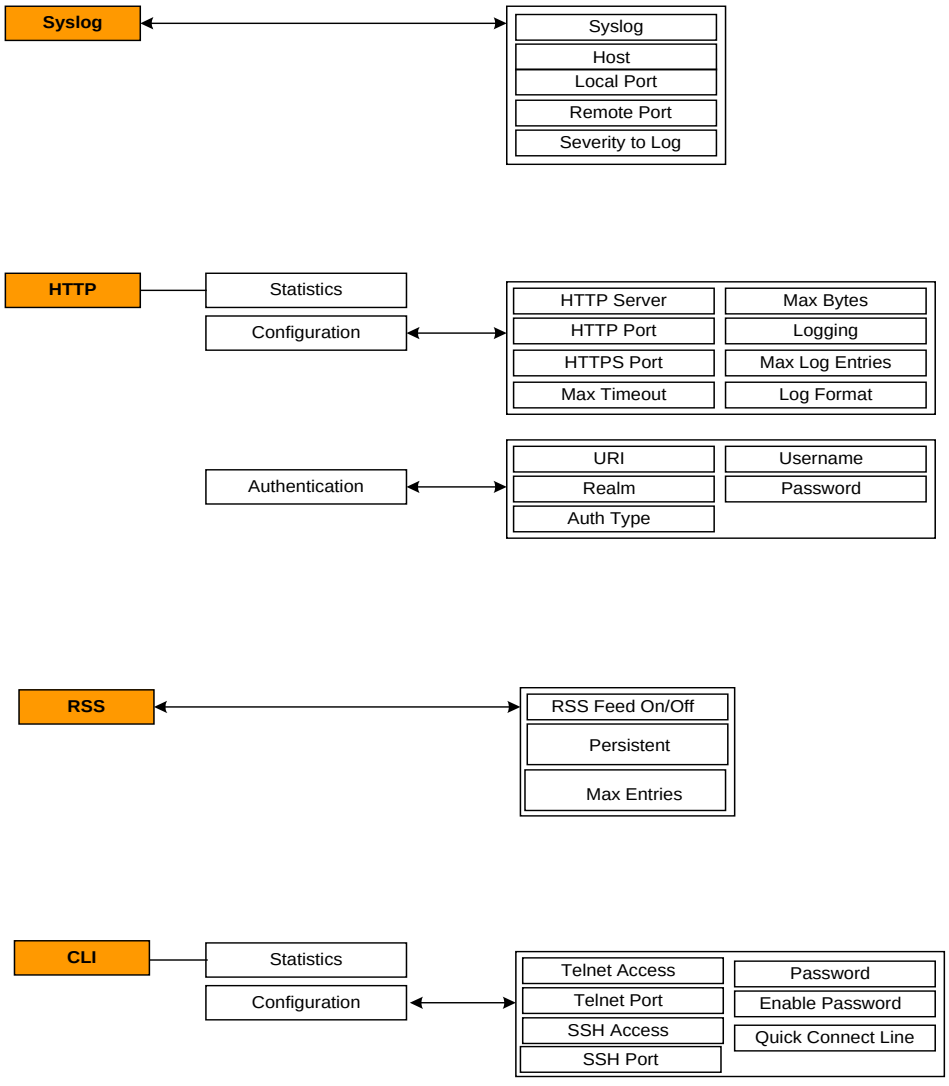
(continued on next page)

Figure 6-4 Web Manager Menu Structure (2 of 5)



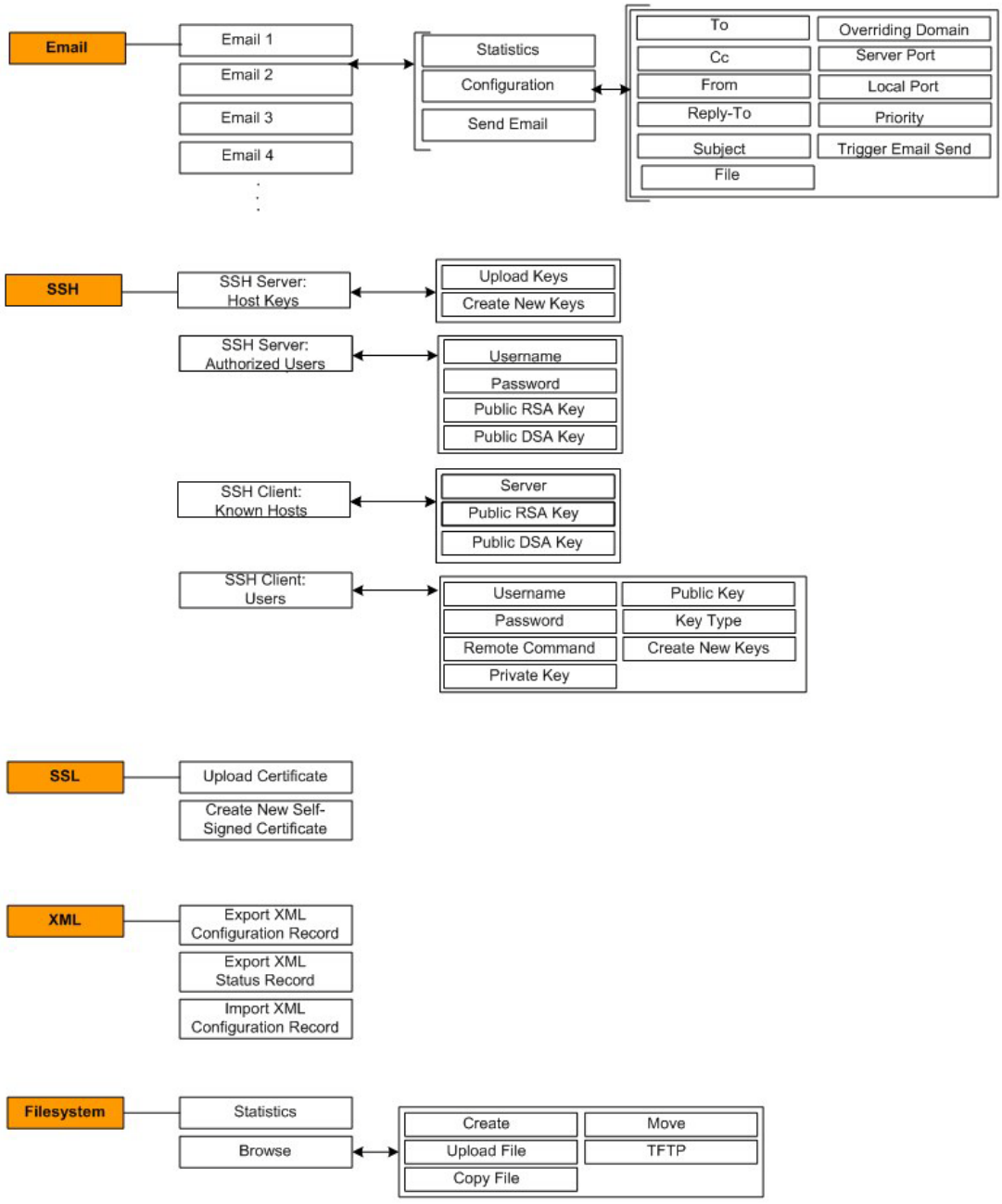
(continued on next page)

Figure 6-5 Web Manager Menu Structure (3 of 5)



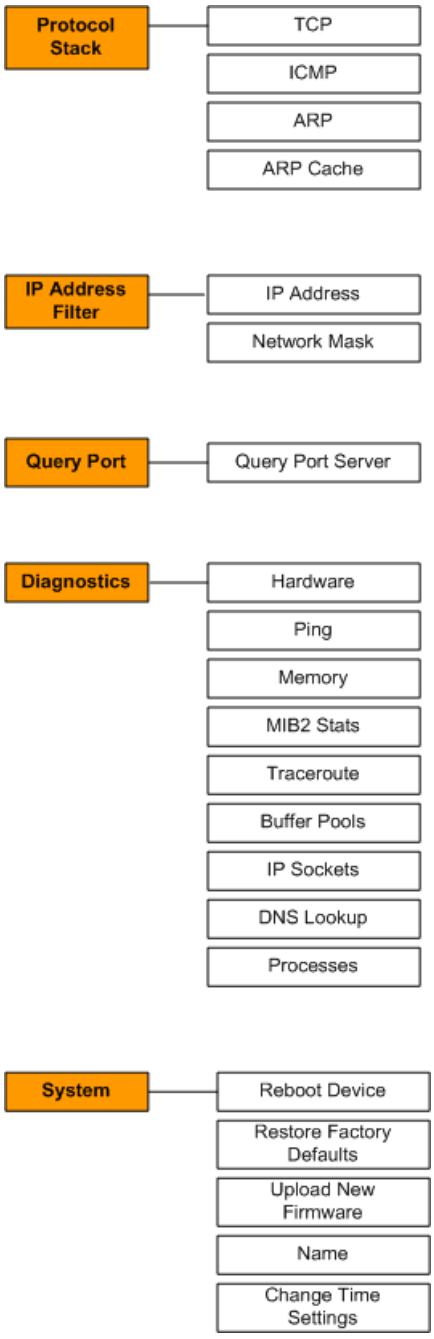
(continued on next page)

Figure 6-6 Web Manager Menu Structure (4 of 5))



(continued on next page)

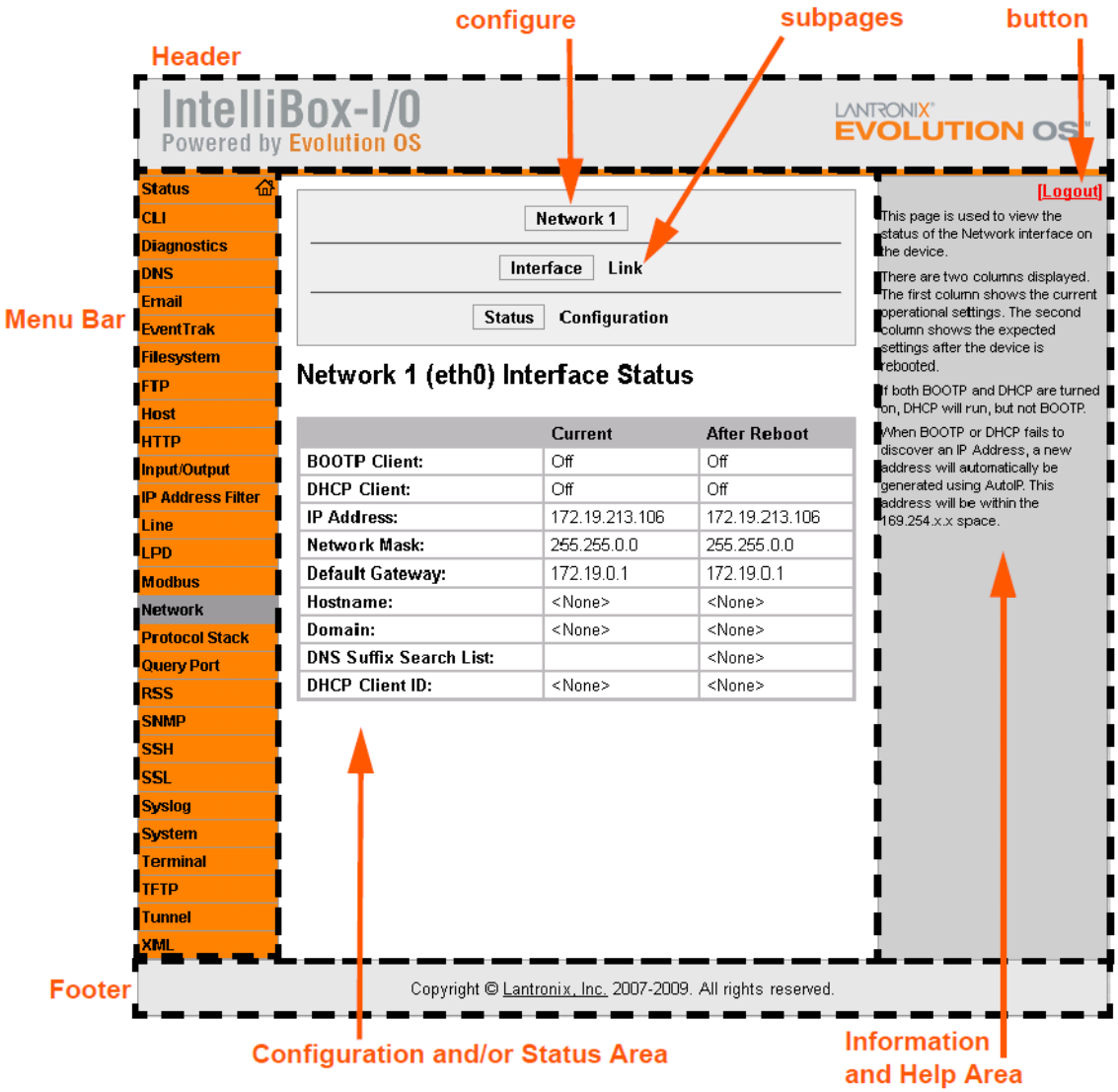
Figure 6-7 Web Manager Menu Structure (5 of 5)



Understanding the Web Manager Pages

Figure 6-8 shows the areas of the Web Manager page.

Figure 6-8 Components of the Web Manager Page



The header always displays at the top of the page. The header information remains the same regardless of the page displayed.

The menu bar always displays at the left side of the page, regardless of the page displayed. The menu bar lists the names of the pages available in the Web Manager. To display a page, click it in the menu bar.

When you click the name of a page in the menu bar, the page displays in the main area. The main area of most pages contains two sections:

- The top section lets you select or enter new configuration settings. After you change settings, click the **Submit** button to apply the change. Some settings require you to reboot the IntelliBox before the settings take effect. Those settings are identified in the appropriate sections in this chapter.
- The bottom section shows the current configuration.

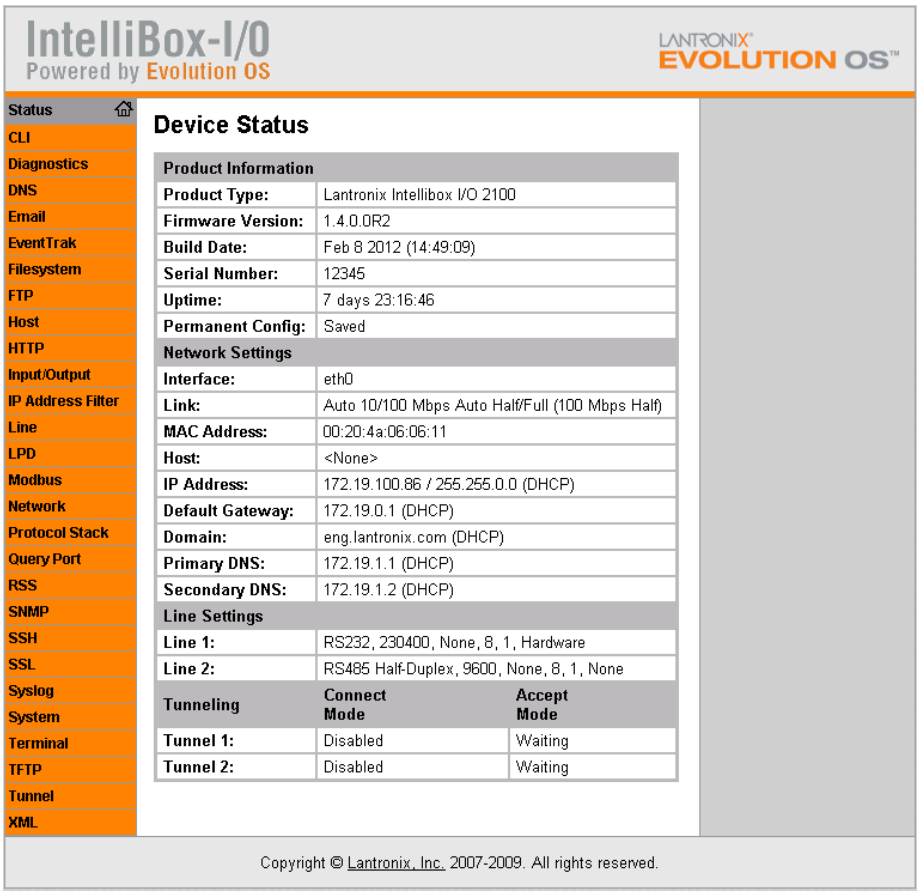
The information area shows information or instructions associated with the page.

The footer displays at the bottom of the page. It contains copyright information and a link to the Lantronix home page.

Device Status Page

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

Figure 6-9 Device Status Page (IntelliBox-I/O 2100)



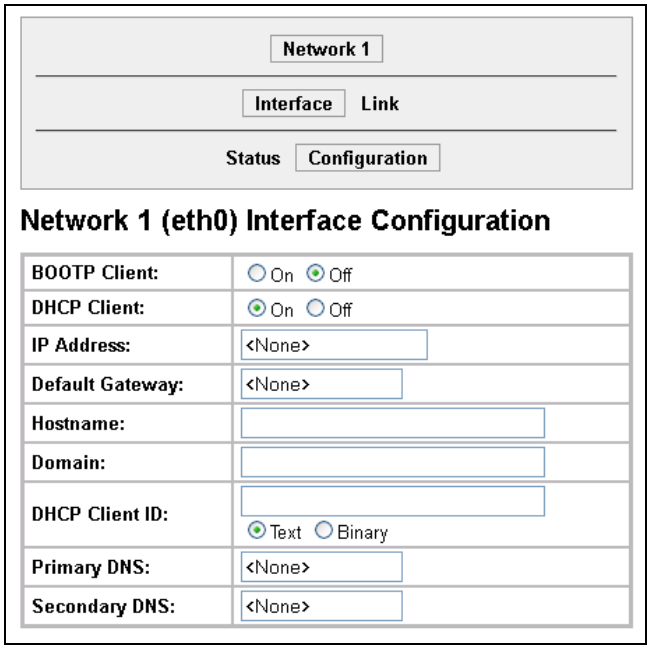
7: Network, Serial Line, Tunnel, and Modbus Settings

Network Configuration Page

Clicking the **Network** link in the menu bar displays the Network Configuration page. Here you can change the following IntelliBox network configuration settings:

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

Figure 7-1 Network Configuration



The **After Reboot** column in the **Current Configuration** section of this page shows the settings that will take effect the next time the IntelliBox reboots.

Changes to the following settings require you to reboot the IntelliBox before the new settings take effect:

- **BOOTP Client**
- **DHCP Client**
- **IP Address**
- **Network Mask**
- **DHCP Client ID**

Note: *Some settings in the **Current Configuration** section, such as **IP Address** and **Network Mask** have a **Delete** link you can click to delete the setting. If you click this link, a warning message asks whether you are sure you want to delete the setting. Click **OK** to delete the setting or **Cancel** to keep it.*

Table 7-1 Network Configuration Page Settings

Network Configuration Page Settings	Description
BOOTP Client	Select whether the IntelliBox should send BOOTP requests. Changing this value requires the IntelliBox to be rebooted. Choices are: **On** = IntelliBox sends BOOTP requests on a DHCP-managed network. This setting overrides the configured IP address, network mask, gateway, host name, and domain settings. If DHCP is set to On, the IntelliBox automatically uses DHCP, regardless of whether BOOTP Client is set to On. **Off** = IntelliBox does not send BOOTP requests.
DHCP Client	Select whether the IntelliBox IP address is automatically assigned by a DHCP server. Changing this value requires you to reboot the IntelliBox. Choices are: **On** = IntelliBox receives its IP address automatically from a DHCP server, regardless of the BOOTP Client setting. This setting overrides the configured IP address, network mask, gateway, host name, and domain settings. **Off** = IntelliBox does not receive its IP address automatically.
IP Address	Enter the IntelliBox static IP address. The IP address consists of four octets separated by a period and is used if BOOTP and DHCP are both set to Off. Changing this value requires you to reboot the IntelliBox. ***Note:*** *When DHCP is enabled, the IntelliBox tries to obtain an IP address from DHCP. If it cannot, the IntelliBox uses an Auto IP address in the range of 169.254.xxx.xxx.*
Network Mask	Enter the IntelliBox subnet mask. The subnet mask consists of four octets separated by a period. Changing this value requires you to reboot the IntelliBox. ***Note:*** *When DHCP is enabled, the IntelliBox tries to obtain a network mask from DHCP. If it cannot, the IntelliBox uses a network mask of 255.255.0.0.*

Network Configuration Page Settings	Description
Gateway	Enter the router IP address from the local LAN the IntelliBox is on. The address consists of four octets separated by a period.
Hostname	Enter the IntelliBox host name. The host name can be up to 31 characters with no spaces.
Domain	Enter the IntelliBox domain name.
DHCP Client ID	Enter a DHCP ID if used by the DHCP server. Changing this value requires the IntelliBox to be rebooted.
Primary DNS	IP address of the primary name server. This entry is required if you choose to configure the DNS (Domain Name Server) servers.
Secondary DNS	IP address of the secondary name server.

Line Settings Pages

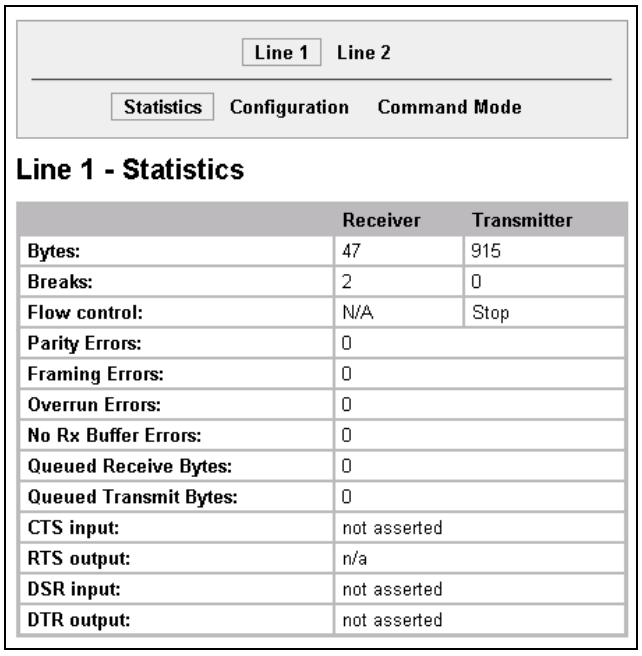
The Line Settings page displays the status and statistics for each of the serial lines (ports). This page also lets you change the character format and command mode settings for the serial lines.

To select a line, click **Line 1** or **Line 2** at the top of the page.

After you select a serial line, you can click **Statistics**, **Configuration**, or **Command Mode** to view and change the settings of the selected serial line. Because all serial lines operate independently, you can specify different configuration settings for each line.Line – Statistics Page

The Line – Statistics page displays when you click **Line** in the menu bar. It also displays when you click **Statistics** at the top of one of the other Line Settings pages. This read-only page shows the status and statistics for the serial line selected at the top of this page.

Figure 7-2 Line – Statistics Page



	Receiver	Transmitter
Bytes:	47	915
Breaks:	2	0
Flow control:	N/A	Stop
Parity Errors:	0	
Framing Errors:	0	
Overrun Errors:	0	
No Rx Buffer Errors:	0	
Queued Receive Bytes:	0	
Queued Transmit Bytes:	0	
CTS input:	not asserted	
RTS output:	n/a	
DSR input:	not asserted	
DTR output:	not asserted	

Line - Configuration Page

If you click **Configuration** at the top of one of the Line Settings pages, the Line – Configuration page displays. This page shows the configuration settings for the serial line selected at the top of the page and lets you change the settings for that serial line.

Figure 7-3 Line – Configuration Page

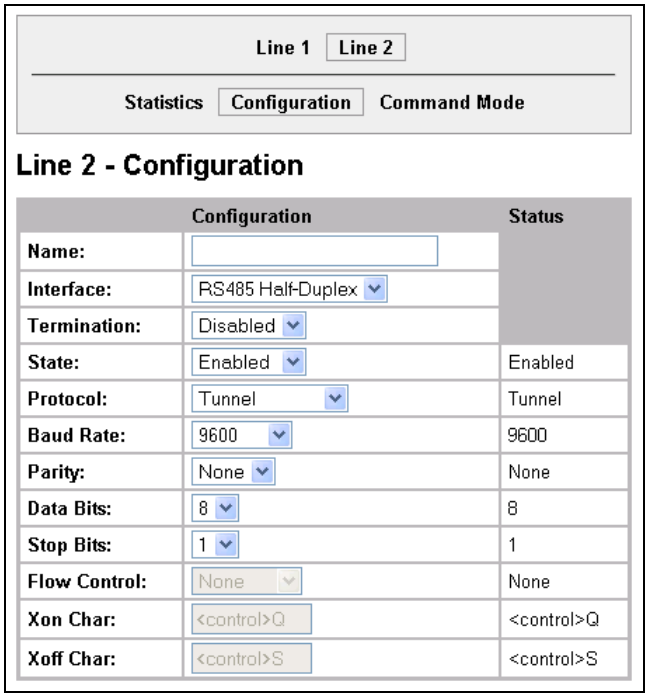


Table 7-2 Configuration Page

Line – Configuration Page Settings	Description
Name (optional)	Enter a name for the serial port. The name may have up to 25 characters.
Interface	Line 1 is always RS232. For Line 2, select the RS485 duplex mode. Choices are: **RS485 Half Duplex** (default) **RS485 Full-Duplex**
Termination (line 2 only)	Select to enable or disable RS-485 termination.
State	Select to enable or disable the current line.
Protocol	Select the protocol used on the current serial line. Choices are: **None** **Tunnel** (default) **Modbus RTU** **Modbus ASCII** **LPD** **LPD or Tunnel** ***Note:*** *Modbus protocols change the display in several fields below.*
Baud Rate	Select the baud rate for the currently selected serial port. Choices are: **300** baud to **230,400** baud. (Default is 9600 baud.) **Custom** = lets you enter in the **Custom** text box a speed other than those shown. ***Note:*** *Any baud rate over 19200, Lantronix requests flow control usage.*
Parity	Select the parity used by the currently selected serial line. Choices are: **None** (default) **Even** (default for Modbus RTU and Modbus ASCII) **Odd**
Data Bits	Select the number of data bits used by the currently selected serial line. Choices are: **7** **8** (default) For the Modbus protocols, this setting cannot be changed. For Modbus RTU, the setting is 8. For Modbus ASCII, the setting is 7.

Line – Configuration Page Settings	Description
Stop Bits	Select the number of stop bits used by the currently selected serial line. Choices are: **1** (default) **2** For the Modbus protocols, the default is 1; this setting automatically changes to 2 if parity is None.
Flow Control	Select the flow control method used by the currently selected serial line. Choices are: **None** (default for Tunnel protocol) **Hardware** (commonly called CTS/RTS) **Software** (commonly called Xon/Xoff) On Line 1, for the Modbus protocols, **Flow Control** defaults to None; this setting cannot be changed. On Line 2, **Flow Control** is unavailable for all protocols.
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.

Line – Command Mode Page

If you click **Command Mode** at the top of one of the Line Settings pages, the Line – Command Mode page displays. This page shows the command mode settings for the serial line selected at the top of the page and lets you change the settings for that serial line.

Figure 7-4 Line – Command Mode Page

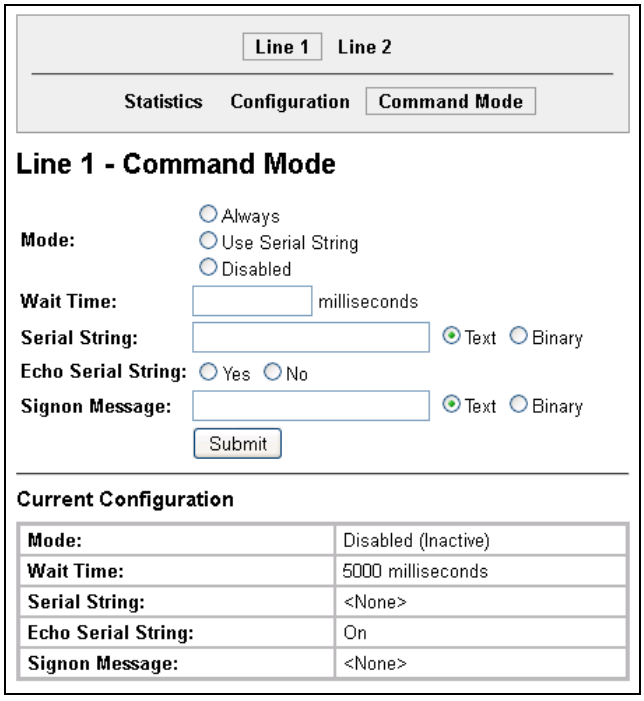


Table 7-3 Line – Command Mode Page

Line – Command Mode Page Settings	Description
Mode	Select the method of enabling command mode or choose to disable command mode. Choices are: **Always** = immediately enables command mode for the serial line. **Use Serial String** = enables command mode when the serial string is read on the serial line during boot time. **Disabled** = Disables command mode.
Wait Time	Enter the maximum number of milliseconds the selected serial line waits to receive the specific serial string at boot time to enter command mode. Default is 5000 milliseconds.
Serial String	Enter the serial string that places the serial line into command mode. After entering a string, use the buttons to indicate whether the string is a text or binary value.
Echo Serial String	Select whether the serial line echoes the specified serial string at boot time. Choices are: **Yes** = echoes the characters specified in the **Serial String** text box. **No** = does not echo the characters specified in the **Serial String** text box.
Signon Message	Enter a message to send on the serial line at bootup. Select **Text** or **Binary** to indicate the form of the entry.

Tunnel Pages

The Tunnel pages let you view and configure settings for tunnels. (For more information, see *Tunneling*.)

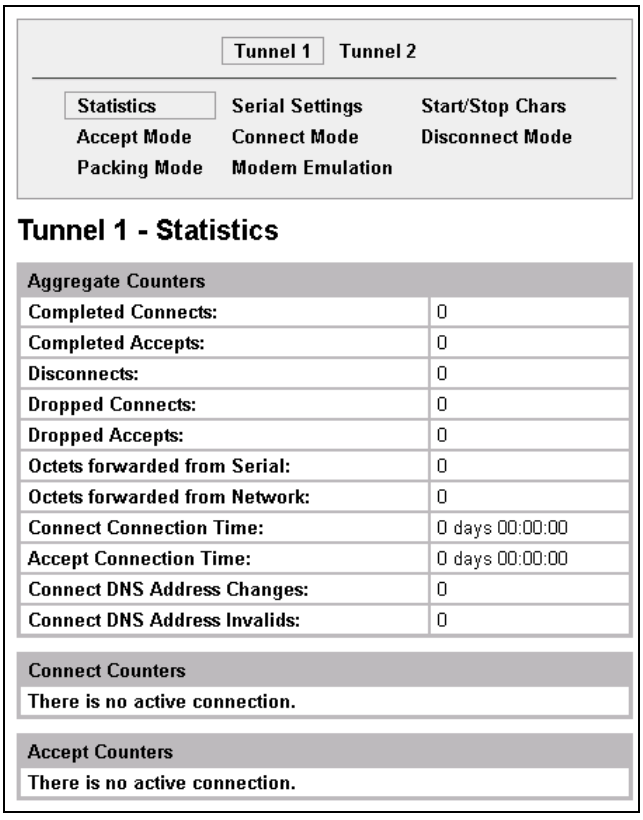
To select a tunnel, click **Tunnel 1** or **Tunnel 2** at the top of the page.

After you select a tunnel, you can click **Statistics**, **Serial Settings**, **Start/Stop Chars**, **Accept Mode**, **Connect Mode**, **Disconnect Mode**, **Packing Mode**, or **Modem Emulation** to view and change the settings of the selected tunnel. Because all tunnels operate independently, you can specify different configuration settings for each tunnel.

Tunnel – Statistics Page

The Tunnel – Statistics page displays when you click **Tunnel** in the menu bar. It also displays when you click **Statistics** at the top of one of the other Tunnel pages. This read-only page shows the status and statistics for the tunnel currently selected at the top of this page.

Figure 7-5 Tunnel - Statistics Page



Tunnel – Serial Settings Page

If you click **Serial Settings** at the top of one of the Tunnel pages, the Tunnel – Serial Settings page displays. This page shows the settings for the tunnel selected at the top of the page and lets you change the settings. If you change the **Buffer Size** value, you must reboot the IntelliBox for the change to take effect. Changing the other values does not require a reboot.

Under **Current Configuration**, **Buffer Size** has a **Reset** link that lets you reset the buffer size to its default value. If you click this link, a message tells you that you will have to reboot the IntelliBox. Click **OK** to proceed or **Cancel** to cancel the operation.

Note: *The default protocol is Tunnel. The protocol on the line 1 page must be* ***Tunnel*** *for tunneling to operate.*

Figure 7-6 Tunnel – Serial Settings Page

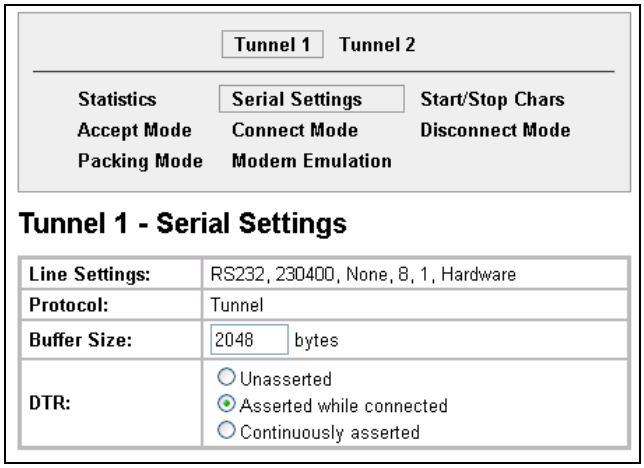


Table 7-4 Tunnel – Serial Settings Page

Tunnel – Serial Settings Page	Description
Line Settings	Lists current serial settings for the line.
Protocol	Lists the protocol being used on the line.
Buffer Size	Enter the size of the buffer used to receive data on the serial line. Range = 1 to 4096 bytes. Default is 2048 bytes. Changing this value requires you to reboot the IntelliBox.
DTR	Select **Asserted while connected** to assert DTR whenever a connect or an accept mode tunnel connection is active. Select **Continuously Asserted** (default) to assert DTR regardless of the status of a tunnel connection. **Unasserted** sets DTR off always.

Tunnel – Start/Stop Characters Page

If you click **Start/Stop Chars** at the top of one of the Tunnel pages, the Tunnel – Start/Stop Chars page displays. This page shows the start and stop characters used for the tunnel selected at the top of the page and lets you change the settings for that tunnel.

Figure 7-7 Tunnel – Start/Stop Chars Page

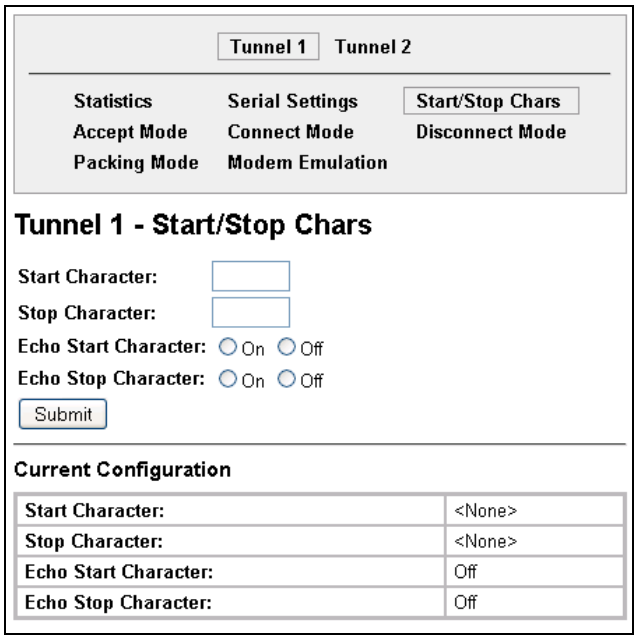


Table 7-5 Tunnel – Start/Stop Chars Page

Tunnel – Start/Stop Chars Page Settings	Description
Start Character	Enter the start character. When this character is read on the serial line, it either initiates a new connection (for a tunnel in Connect Mode) or enables a tunnel in Accept Mode to start listening for connections. Default is <none>.
Stop Character	Enter the stop character. When this character is read on the serial line, it disconnects an active tunnel connection. Default is <none>.
Echo Start Character	Select whether the start character is forwarded (or "echoed') through the selected tunnel when the serial line is read. Choices are: **On** = echo the start character on the selected tunnel when the serial line is read. **Off** = do not echo the start character. (default)
Echo Stop Character	Select whether the stop character is echoed through the selected tunnel when the serial line is read. Choices are: **On** = echo the stop character on the selected tunnel when the serial line is read. **Off** = do not echo the stop character. (default)

Tunnel – Accept Mode Page

Accept Mode determines how the IntelliBox "listens" for an incoming connection. If you click **Accept Mode** at the top of one of the Tunnel pages, the Tunnel – Accept Mode page displays. Here you can select the method for starting a tunnel in Accept Mode and select other settings for the tunnel selected at the top of the page.

For more information about Accept Mode, see *Accept Mode*.

Figure 7-8 Tunnel – Accept Mode Page

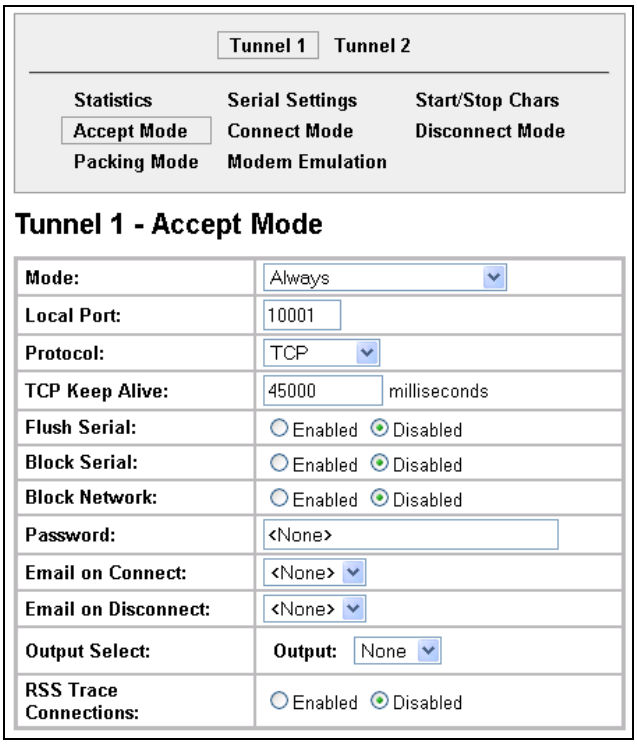


Table 7-6 Tunnel – Accept Mode Page

Tunnel – Accept Mode Page Settings	Description
Mode	Select the method used to start a tunnel in Accept Mode. Choices are: **Disable** = do not accept an incoming connection. **Always** = accept an incoming connection. (default) **Any Character** = start waiting for an incoming connection when any character is read on the serial line. **Start Character** = start waiting for an incoming connection when the start character for the selected tunnel is read on the serial line. **Modem Control Asserted** = start waiting for an incoming connection as long as the Modem Control pin (DSR) is asserted on the serial line until a connection is made. **Modem Emulation** = start waiting for an incoming connection when triggered by modem emulation AT commands. Connect Mode must also be set to **Modem Emulation**.
Local Port	Enter the number of the local port used to receive (or listen for) packets. Default is 10001 for Tunnel 1, 10002 for Tunnel 2, and so forth.
Protocol	Select the protocol to be used on the connection. Choices are: **TCP** (default) **SSH** **SSL** **TCP** **TCP/AES** **Telnet**
TCP Keep Alive	Specify the number of milliseconds the IntelliBox waits during an inactive connection before checking the status of the connection. If the IntelliBox does not receive a response from the remote host, it drops that connection.
AES Encrypt Key	Specify the Advanced Encryption Standard (AES) key string to be used for encrypting outgoing data in Accept Mode tunneling. Then, select the key form: **Text** **Hexadecimal**
AES Decrypt Key	Specify the Advanced Encryption Standard (AES) key string to be used for decrypting incoming data in Accept Mode tunneling. Then, select the key form: **Text Hexadecimal**
Flush Serial	Select whether the serial line is flushed when a connection is made. Choices are: **Enabled** = flush the serial line when a connection is made. **Disabled** = do not flush the serial line. (default)

Tunnel – Accept Mode Page Settings	Description
Block Serial	Select whether incoming serial data should be discarded. This setting is used for debugging purposes. Choices are: **On** = discard all incoming serial data on the respective interface. **Off** = do not discard all incoming serial data. (default)
Block Network	Select whether incoming network data should be discarded. This setting is used for debugging purposes. Choices are: **On** = discard all incoming network data on the respective interface. **Off** = do not discard all incoming network data. (default)
Password	Enter a password that clients must send to the IntelliBox 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 IntelliBox 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. **Enabled** = prompt for a password upon connection. **Disabled** = do not prompt for a password upon connection.
Email on Connect	Select whether an email is sent when a connection is made. **None** = do not send an email. **Email #** = send an email corresponding to the tunnel number.
Email on Disconnect	Select whether an email corresponding to the tunnel number is sent when a connection is closed. **None** = do not send an email. **Email #** = send an email corresponding to the tunnel number.
Output Selection	Select the output to be closed while a connection is active. **None** **XI01** = output from digital port 1 **XI02** = output from digital port 2 **Relay** = output from the relay
Mode	Select whether the same output may also be closed by another condition (e.g. Connect Mode settings from Tunnel 1 and Tunnel 2 for the same digital port.) **Exclusive Control** = same output may not be closed by another condition. **Logical-Or** = same output may be closed by another condition.
RSS Trace Connections	Select to enable or disable RSS Trace Connections.

Tunnel – Connect Mode Page

Connect Mode determines how the IntelliBox initiates a connection to a remote host or device. If you click **Connect Mode** at the top of one of the Tunnel pages, the Tunnel – Connect Mode page displays. Here you can select the method for starting a tunnel in Connect Mode and select other settings for the tunnel selected at the top of the page. A tunnel, like an LPD is directed to a single serial port.

Any configuration changes you make on the displayed page apply to the tunnel you selected at the top of this page. For example, if **Tunnel 1** is selected, any configuration changes you make apply to tunnel 1.

Under **Current Configuration**, **Remote Address** has a **Delete** link that lets you delete the remote address shown. If you click this link, a message tells you that your action may stop an active connection. Click **OK** to proceed or **Cancel** to cancel the operation.

Remote Port defaults to Random. If you have configured a specific port number, a **Random** link displays that enables you to restore the default. For more information about Connect Mode, see *Connect Mode*.

Figure 7-9 Tunnel -- Connect Mode Page

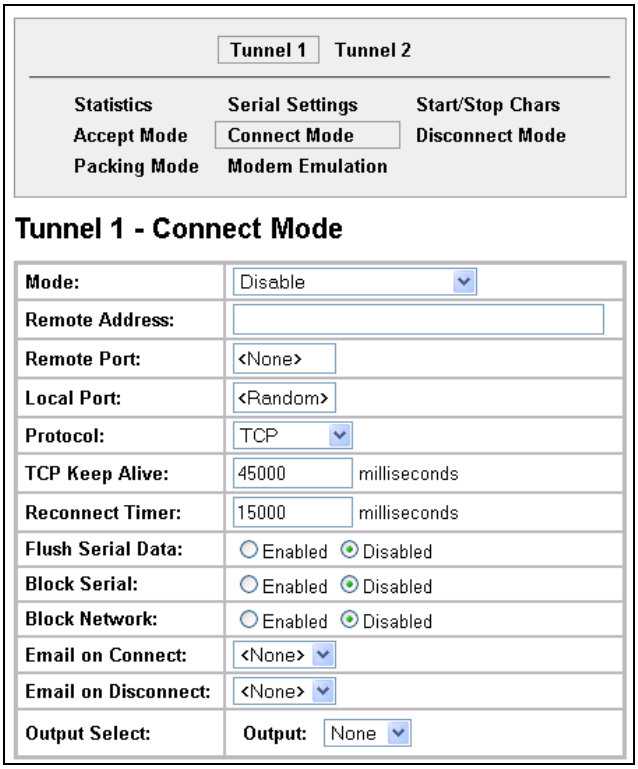


Table 7-7 Tunnel -- Connect Mode Settings

Tunnel – Connect Mode Page Settings	Description
Mode	Select the method used to start a tunnel in Accept Mode. Choices are: **Disable** = do not accept an incoming connection. **Always** = accept an incoming connection. (default) **Any Character** = start waiting for an incoming connection when any character is read on the serial line. **Start Character** = start waiting for an incoming connection when the start character for the selected tunnel is read on the serial line. **Modem Control Asserted** = start waiting for an incoming connection as long as the Modem Control pin (DSR) is asserted on the serial line until a connection is made. **Modem Emulation** = start waiting for an incoming connection when triggered by modem emulation AT commands. Connect Mode must also be set to *Modem Emulation*.
Remote Address	Enter the address of the remote host to which the selected tunnel will connect. Default is <none>.
Remote Port	Enter the number of the remote port to which the selected tunnel will connect. Default is <none>.
Local Port	Enter the number of the local port used to receive (or listen for) packets. Random by default, but can be overridden.
Protocol	Select the protocol to be used on the connection. Choices are: **TCP** (default) **SSH SSL** **TCP** **TCP/AES** **Telnet** **UDP** **UDP/AES**
TCP Keep Alive	Specifies the number of milliseconds the IntelliBox waits during an inactive connection before checking the status of the connection. If the IntelliBox does not receive a response from the remote host, it drops that connection.
AES Encrypt Key	Specify the Advanced Encryption Standard (AES) key string to be used for encrypting outgoing data in Connect Mode tunneling. Then, select the key form: **Text** **Hexadecimal**
AES Decrypt Key	Specify the Advanced Encryption Standard (AES) key string to be used for decrypting incoming data in Connect Mode tunneling. Then, select the key form: **Text** **Hexadecimal**

Tunnel – Connect Mode Page Settings	Description
Reconnect Timer	Enter the maximum number of milliseconds to wait before trying to reconnect to the remote host after a previous attempt failed or the connection was closed. Default is 15000 milliseconds.
Flush Serial Data	Select whether to flush the serial line when a connection is made. Choices are: **Enabled** = flush the serial line when a connection is made. **Disabled** = do not flush the serial line. (default)
SSH Username	If you selected SSH as the protocol for this tunnel, enter the SSH client user that is to be used for the SSH connection. Default is <none>.
Block Serial	Select whether incoming block serial data should be discarded. This setting is used for debugging purposes. Choices are: **On** = discard all incoming serial data on the respective interface. **Off** = do not discard all incoming serial data. (default)
Block Network	Select whether incoming block network data should be discarded. This setting is used for debugging purposes. Choices are: **On** = discard all incoming network data on the respective interface. **Off** = do not discard all incoming network data. (default)
Email on Connect	Select whether email should be sent when a connection is made. **None** = do not send an email. **Email #** = send an email corresponding to the tunnel number.
Email on Disconnect	Select whether email should be sent when a connection is closed. **None** = do not send an email. **Email #** = send an email corresponding to the tunnel number.
Output Select	Select the output to be closed while a connection is active. **XI01 =** Output from digital port 1 **XI02 =** Output from digital port 2 **Relay =** Output from the relay
Mode	Select whether the same output may also be closed by another condition, (e.g. Connect Mode settings from Tunnel 1 and Tunnel 2 for the same digital port.) **Exclusive Control** = The same output may not be closed by another condition. **Logical-Or** = The same output may be closed by another condition.

Tunnel – Disconnect Mode Page

If you click **Disconnect Mode** at the top of one of the Tunnel pages, the Tunnel – Disconnect Mode page displays. Here you can select the disconnect method for the tunnel selected at the top of the page. For more information about Disconnect Mode, see *Disconnect Mode*.

Figure 7-10 Tunnel – Disconnect Mode Page

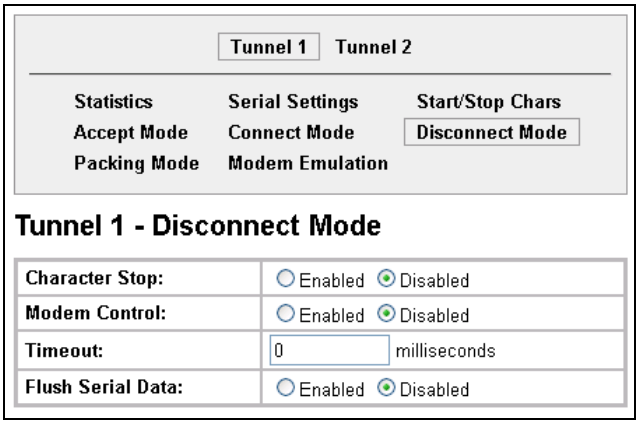


Table 7-8 Tunnel – Disconnect Mode Page

Tunnel – Disconnect Mode Page Settings	Description
Character Stop	Select whether to enable disconnect when the "Stop Character" (configured on the "Start/Stop Chars" page) is read on the serial line. Choices are: **Enabled** **Disabled**
Modem Control	Select whether to enable disconnect when the modem control pin is not asserted on the serial line. Choices are: **Enabled** **Disabled**
Timeout	Enter the idle time, in milliseconds, that must elapse for a connection before it is disconnected. Default is 60000 milliseconds. The value 0 (zero) disables the idle timeout.
Flush Serial Data	Select whether the serial line should be flushed when a connection is disconnected. Choices are: **Enabled** = flush the serial line when a connection is disconnected. **Disabled** = do not flush the serial line. (default)

Tunnel – Packing Mode Page

When tunneling, data can be packed (queued) and sent in large chunks on the network instead of being sent immediately after being read on the serial line. If you click **Packing Mode** at the top of one of the Tunnel pages, the Tunnel – Packing Mode page displays. Here you can select packing settings for the tunnel selected at the top of the page. For more information about Packing Mode, see *Packing Mode*.

Figure 7-11 Tunnel – Packing Mode Page

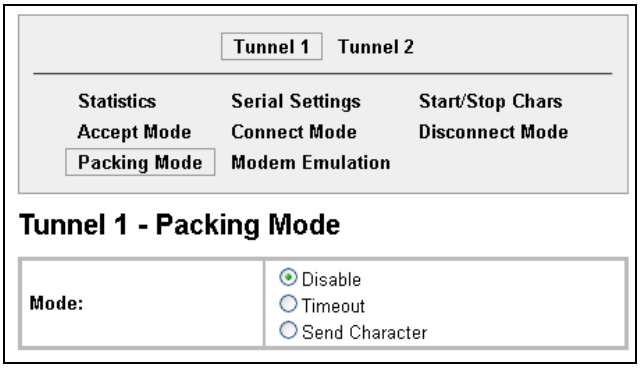


Table 7-9 Tunnel – Packing Mode Page

Tunnel – Packing Mode Page Settings	Description
Mode	Select the method used to pack data. Choices are: **Disabled** = data is never packed. (default) **Timeout** = data is sent after the timeout elapses. **Send Character** = data is sent when the send character is read on the serial line.
Timeout	Enter the maximum number of milliseconds to wait before sending queued data across the network. Default is 1000 milliseconds.
Threshold	Enter the queued data limit that, when reached, immediately sends queued data to the network. Default is 512 bytes.
Send Character	Enter the send character. When this character is read on the serial line, it forces the queued data to be sent immediately. Default is <none>.
Trailing Character	Enter the trailing character. This character is inserted into the outgoing data stream immediately after the send character. Default is <none>.

Tunnel – Modem Emulation Page

A tunnel in Connect Mode can be initiated using modem commands incoming from the serial line. If you click **Modem Emulation** at the top of one of the Tunnel pages, the Tunnel – Modem Emulation page displays. Here you can select modem emulation settings for the tunnel selected at the top of the page. For more information about modem emulation, see *Modem Emulation*.

Tunnel – Modem Emulation Page

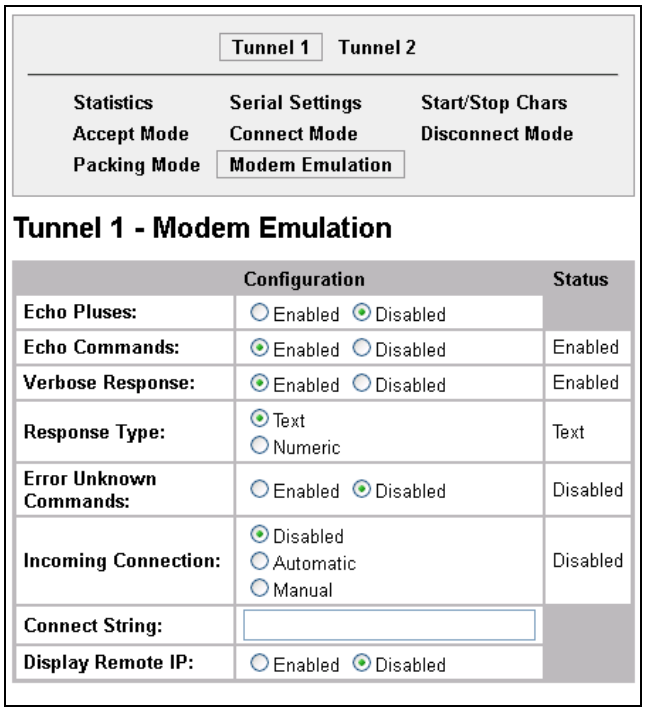


Table 7-10 Tunnel – Modem Emulation Page

Tunnel – Modem Emulation Page Settings	Description
Echo Pluses	Select whether the modem +++ escape sequence is echoed (sent). Choices are: **On** = modem pluses are sent into the network. **Off** = modem pluses are suppressed. (default).
Echo Commands	Select whether modem commands are echoed on the serial line. Choices are: **On** = modem commands are echoed. (default) **Off** = modem commands are not echoed.
Verbose Response Codes	Select whether modem response (result) codes are sent on the serial line. Choices are: **Text** = modem responses are sent on the serial line. (default) **Numeric** = modem responses are not sent.
Response Codes	Select whether modem response (result) codes sent on the serial line take the form of words or numbers. Choices are: **Text** = modem responses are sent as words. (default) **Numeric** = modem responses are sent as numbers.
Error Unknown Commands	Select whether an ERROR or OK response is sent in reply to unrecognized AT commands. Choices are: **On** = ERROR is returned for unrecognized AT commands. **Off** = OK is returned for unrecognized AT commands. (default)
Incoming Connection	Select how to manage incoming requests. Choices are: **Disabled** = disable requests (ATS0=0) **Automatic** = automatically answer requests (ATS0=1) **Manual** = manually answer requests via the ATA command after an incoming RING (ATS0=2)
Connect String	If required, enter a customized string that is sent along with the CONNECT response code. Default is <none>.
Display Remote IP	Select whether to enable an incoming RING followed by the IP address of the caller. Choices are: **Enabled** **Disabled**

Modbus Pages

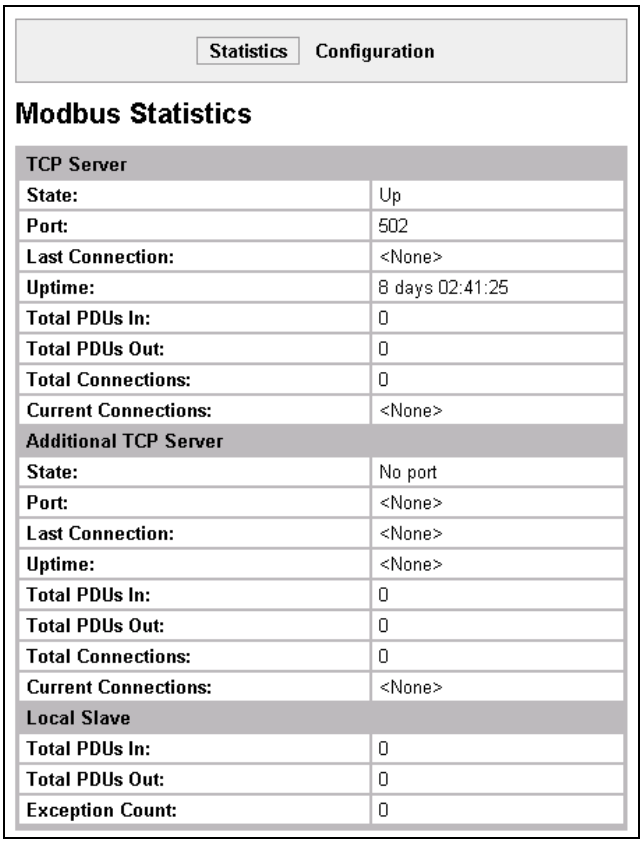
The Modbus pages let you view and configure settings for Modbus servers listening on the TCP ports. (For more information, see the appendix, *C: Modbus*.)

Modbus – Statistics Page

The Modbus – Statistics page displays when you click **Modbus** in the menu bar. It also displays when you click **Statistics** at the top of the Modbus - Configuration page. This page shows the status and statistics for up to two Modbus servers. The standard TCP server port number is 502.

When a connection is active, the remote client information displays as well as the number of Protocol Data Units (PDUs) that have been sent and received. This is a count of messages, not bytes. If a connection is active, a **Kill** link (at its right)) enables you to close the connection.

Figure 7-12 Modbus – Statistics Page



Modbus – Configuration Page

If you click **Configuration** at the top of one of the Modbus – Statistics page, the Modbus Configuration page displays. **Modbus Configuration** enables you to add a Modbus server.

The Modbus server, if enabled, is active on TCP port 502. You have the option of using an additional port.

Figure 7-13 Modbus – Configuration Page

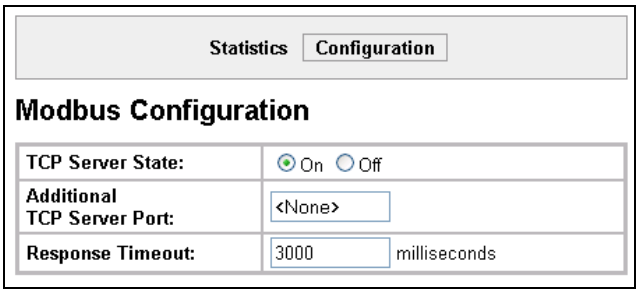


Table 7-11 Modbus – Configuration Page

Modbus – Configuration Page Settings	Description
TCP Server State	Select whether to enable a second Modbus server to have access. Choices are: **On** = Modbus server is enabled. (default) **Off** = Modbus server is disabled.
Additional TCP Server Port	Enter the number of the TCP port on which the IntelliBox additional server listens for connections.
Response Timeout	Indicate the response timeout in milliseconds. Must be a minimum of 10 msec.

8: Terminal and Host Settings

This chapter describes how to view and configure the Terminal Login Connect Menu and associated Host configuration. The Terminal Login Connect Menu feature allows the IntelliBox device to present a menu of predefined connections when the device is accessed via telnet, ssh, or a serial port. From the menu, a user can choose one of the presented options and the device automatically makes the predefined connection.

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

Terminal Settings

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

Figure 8-1 Terminal on Network and Line

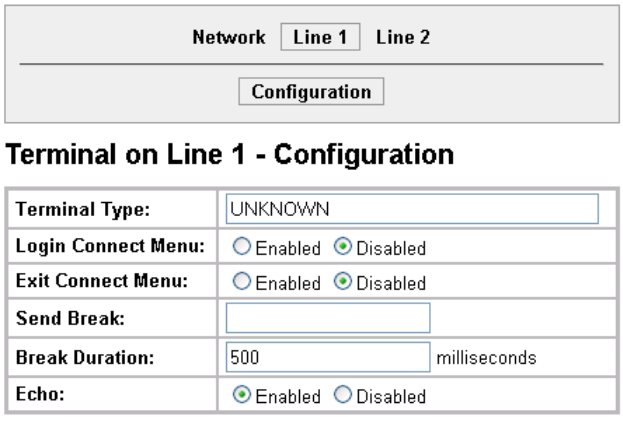


Table 8-1 Terminal on Network and Line Settings

Terminal on Network and Line Settings	Description
Terminal Type	Enter the Terminal Type to be sent from the host via IAC. ***Note:*** *IAC means "interpret as command". It is a way to send commands over the networks such as* **send break** *or* **start echoing**.
Login Connect Menu	Select the interface to display when the user logs in. Choices are: **Enabled** = shows the Login Connect menu **Disabled** = shows the CLI (default)
Exit Connect Menu	Select whether to display a choice for the user to exit the Login Connect menu and reach the CLI. Choices are: **Enabled** = a choice allows the user to exit to the CLI **Disabled** = there is no exit to the CLI (default)
Send Break	Enter a Send Break control character, e.g., <control> Y, or keep blank to disable. When the Send Break control character is received from the network on its way to a Serial Line, it will not be sent to the Line; instead, the line output will be forced inactive. ***Note:*** *This configuration option is only available for Line Terminals.*
Break Duration	Specify, in milliseconds, how long the "spacing"condition will be placed on the line when a break is sent. May enter a value up to 10000. Default is 500. ***Note:*** *This configuration option is only available for Line Terminals.*
Echo	Select whether to enable echo. Choices are: **Enabled** **Disabled** ***Note:*** *Applies only to Connect Mode Telnet connections, not to Accept Mode. Only disable* ***Echo*** *if your terminal echoes, in which case you will see double of each character typed. Default is enabled.*

Host Configuration

The Host page is where you view and configure settings for a remote host.

Figure 8-3 Host Configuration

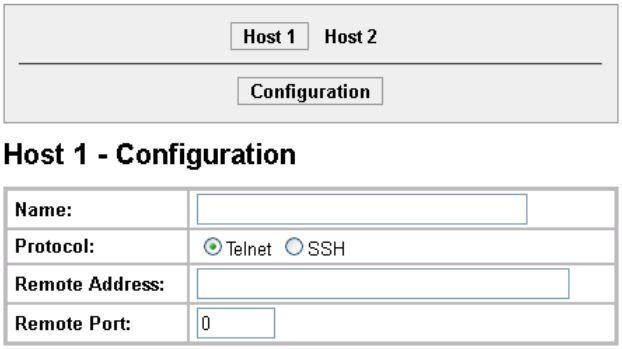


Table 8-2 Host Configuration

Host Settings	Description
Name	Enter a name for the host. This name appears on the Login Connect Menu. The maximum length of the host name is 63 characters. To leave a host out of the menu, leave this field blank.
Protocol	Select the protocol to use to connect to the host. Choices are: **Telnet** **SSH** ***Note:*** *SSH Keys must be loaded or created in SSH for the SSH protocol to work.*
SSH Username	Enter a username to select a pre-configured Username/Password/ Key (configured on the SSH: Client Users), or leave it blank to be prompted for a username and password at connect time. ***Note:*** *This field appears if you selected SSH as the protocol.*
Remote Address	Enter an IP address for the host to which the device will connect.
Remote Port	Enter the port on the host to which the device will connect.

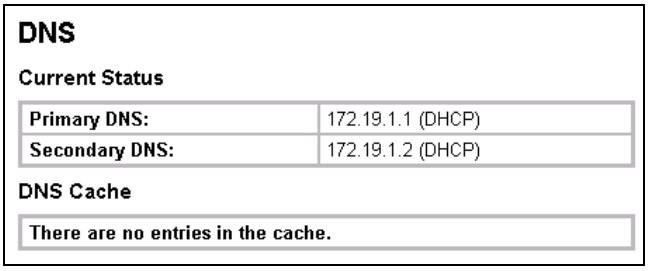
9: Services Settings

DNS Page

Clicking the **DNS** link in the menu bar displays the DNS page. This page displays and allows changes to configuration settings for the domain name system (DNS).

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

Figure 9-1 DNS Page



Note: *If the current configuration shows an address comes from DHCP or BOOTP, the new static address overrides it until you reboot the device.*

Table 9-1 DNS Page

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

SNMP Page

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

Under **Current Configuration**, several settings have a **Delete** link that lets you delete these settings. If you click these links, a message asks whether you are sure you want to delete this information. Click **OK** to proceed or **Cancel** to cancel the operation.

Figure 9-2 SNMP Page

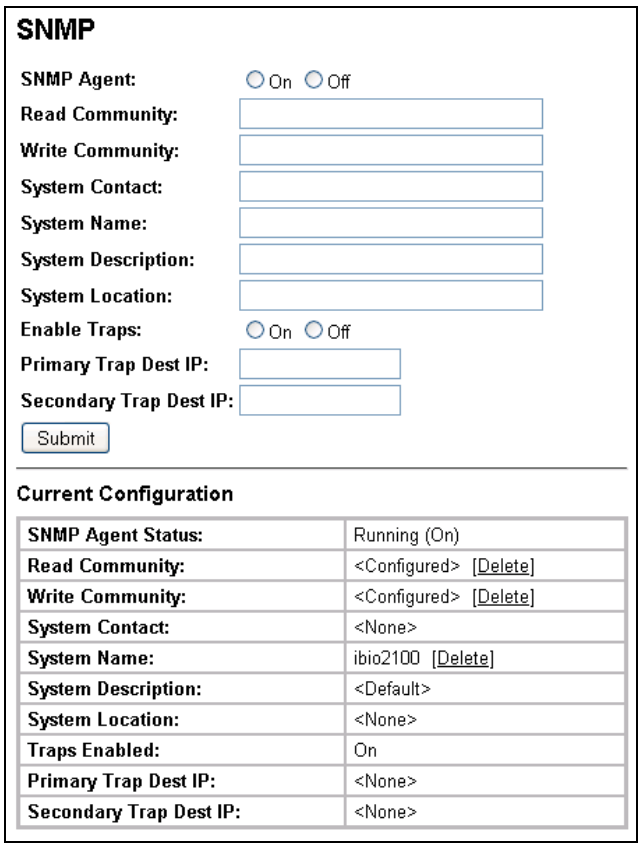


Table 9-2 SNMP Page

SNMP Page Settings	Description
SNMP Agent	Select whether SNMP is enabled. Choices are: **On** = SNMP is enabled. (default) **Off** = SNMP is disabled.
Read Community	Enter the case-sensitive community name from which the IntelliBox will receive trap messages. Default is public. For security, the read community name displays as <Configured> to show that one is enabled.
Write Community	Enter the case-sensitive community name to which the IntelliBox will send trap messages. Default is private. For security, the write community name displays as <Configured> to show that one is enabled.
System Contact	Enter the name of the system contact. Default is <None>.
System Name	Enter the IntelliBox's name.
System Description	Enter a system description for the IntelliBox.
System Location	Enter the geographic location of the IntelliBox. Default is <None>.
Enable Traps	Select whether SNMP cold start trap messages are enabled at boot. Choices are: **On** = SNMP cold start trap messages are enabled at boot time. (default) **Off** = SNMP traps are disabled.
Primary Trap Dest IP	Enter the primary SNMP trap host. Default is <None>.
Secondary Trap Dest IP	Enter the secondary SNMP trap host. Default is <None>.

FTP Page

Clicking the **FTP** link in the menu bar displays the FTP page. This page displays the current File Transfer Protocol (FTP) connection status and various statistics about the FTP server.

Under **Current FTP Configuration and Statistics**, **FTP Password** has a **Reset** link that lets you reset the FTP password. If you click this link, a message asks whether you are sure you want to reset this information. Click **OK** to proceed or **Cancel** to cancel the operation.

Figure 9-3 FTP Page

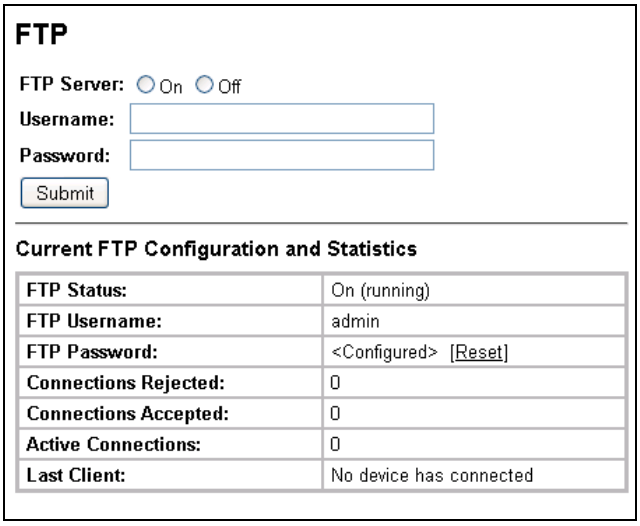


Table 9-3 FTP Page

FTP Page Settings	Description
FTP Server	Select whether the FTP server is enabled. Choices are: **On** = FTP server is enabled. (default) **Off** = FTP server is disabled.
FTP Username	Enter the username required to gain FTP access. Default is admin.
FTP Password	Enter the password associated with the username. Default is PASS.

TFTP Page

Clicking the **TFTP** link in the menu bar displays the TFTP page. This page displays the status and various statistics about the Trivial File Transfer Protocol (TFTP) server.

Figure 9-4 TFTP Page

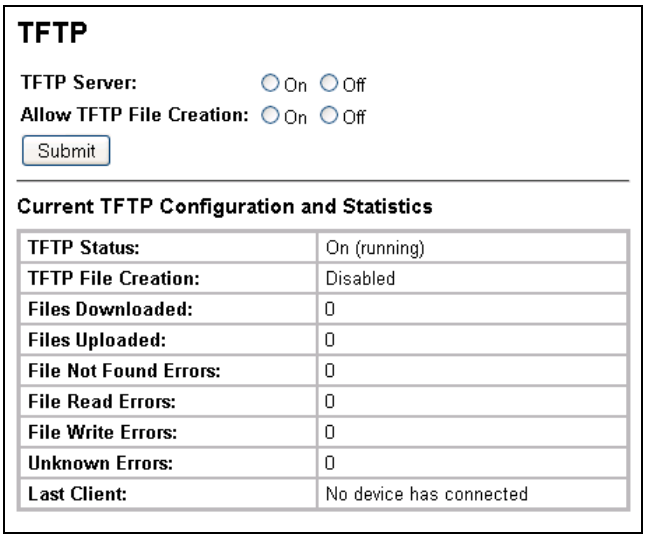


Table 9-4 TFTP Page

TFTP Page Settings	Description
TFTP Server	Select whether the TFTP server is enabled. Choices are: **On** = TFTP server is enabled. (default) **Off** = TFTP server is disabled.
Allow TFTP File Creation	Select whether the TFTP server can create a file if it does not already exist. If you enable this feature, it exposes the IntelliBox to possible Denial-of-Service (DoS) attacks against the filesystem. Choices are: **On** = files can be created by the TFTP server. **Off** = files cannot be created by the TFTP server. (default)

Syslog Page

Clicking the **Syslog** link in the menu bar displays the Syslog page. This 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.

Figure 9-5 Syslog Page

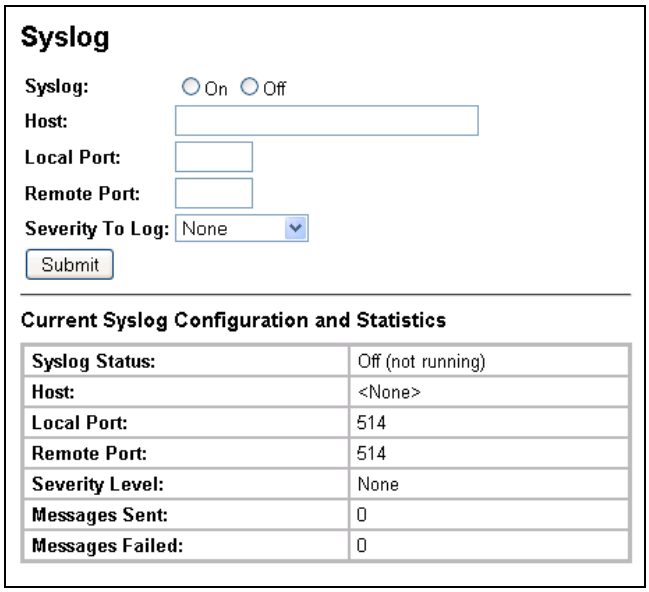


Table 9-5 Syslog Page

Syslog Page Settings	Description
Host	Enter the IP address of the remote server from which system logs are sent for storage.
Local Port	Enter the number for the local port on the IntelliBox from which system logs are sent. The default is 514. 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) enables the administrator to save the complete system log history.
Remote Port	Enter the number for 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 IntelliBox 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 Pages

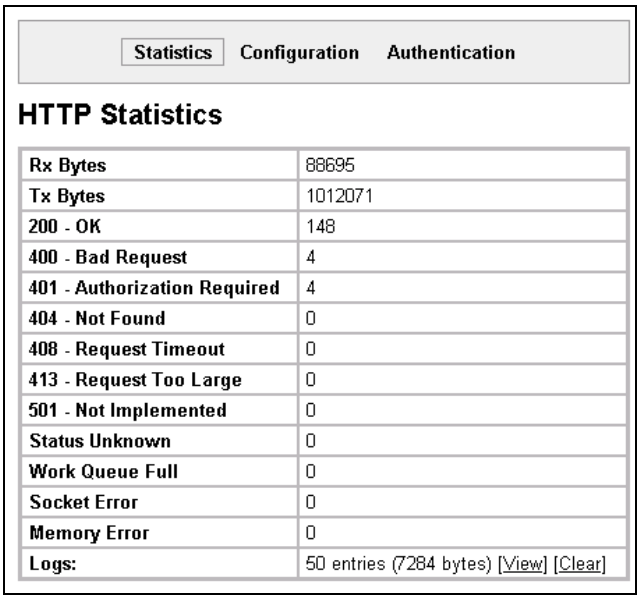
Clicking the **HTTP** link in the menu bar displays the HTTP Statistics page. This page has three links at the top for viewing statistics and for viewing and changing configuration and authentication settings.

HTTP Statistics Page

The HTTP Statistics page displays when you click **HTTP** in the menu bar. It also displays when you click **Statistics** at the top of one of the other HTTP pages. This read-only page shows various statistics about the Hyper Text Transfer Protocol (HTTP) server.

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

Figure 9-6 HTTP Statistics Page



HTTP Configuration Page

If you click **Configuration** at the top of one of the HTTP pages, the HTTP Configuration page displays. Here you can change HTTP configuration settings.

Under **Current Configuration**, **Logs** has **View** and **Clear** links that let you view or clear the log. If you click **View**, the log displays. If you click **Clear**, a message asks whether you are sure you want to delete this information. Click **OK** to proceed or **Cancel** to cancel the operation.

Note: *For help changing the format of the log, see Log Format Directives.*

Figure 9-7 HTTP Configuration Page

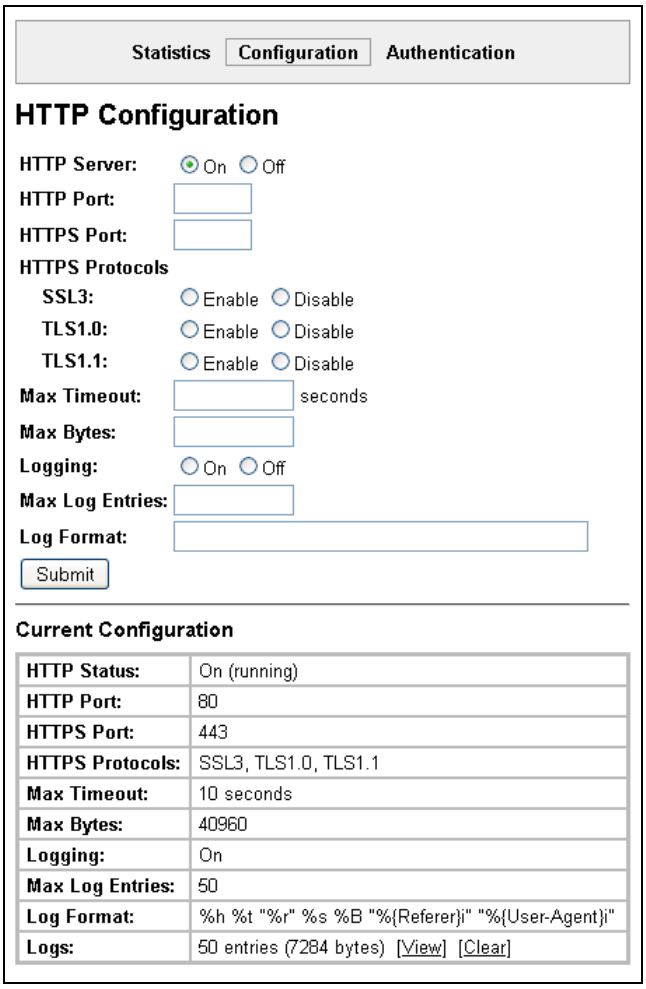


Table 9-6 HTTP Configuration Page

HTTP Configuration Page Settings	Description
HTTP Server	Select whether the HTTP server is enabled. Choices are: **On** = HTTP server is enabled. (default) **Off** = HTTP server is disabled.
HTTP Port	Enter the number of the port on which the IntelliBox listens for incoming HTTP connections from a web browser. Default is 80.
HTTPS Port	Enter the number of the port on which the IntelliBox listens for incoming HTTPS connections from a web browser. Default is 443. The IntelliBox listens on the HTTPS port only when an SSL certificate has been configured for the device (see *SSL*).
HTTPS Protocols	Select whether to enable or disable the following protocols: **SSL3** **TLS1.0** **TLS1.1**
Max Timeout	Enter the maximum number of seconds that the IntelliBox waits for a request from a client. This value helps prevent Denial of Service (DoS) attacks against the HTTP Server. Default is 10 seconds.
Max Bytes	Enter the maximum number of bytes allowed in a client request. This value helps prevent Denial of Service (DoS) attacks against the HTTP Server. Default is 40960 bytes.
Logging	Select whether the HTTP log is enabled. Choices are: **On** = HTTP log is enabled. (default) **Off** = HTTP log is disabled.
Max Log Entries	Enter the maximum number of entries that can be cached and viewed in the HTTP log. The HTTP log is a scrolling log, with only the last Max Log Entries cached and viewable. Default is 50.

Log Format	Enter the format of the HTTP log. The **log format directives**:
	`%a remote IP address (could be a proxy)`
	`%b bytes sent excluding headers`
	`%B bytes sent excluding headers (0 = '-')`
	`%h remote host (same as '%a')`
	`%{h}i header contents from request (h = header string)`
	`%m request method`
	`%p ephemeral local port value used for request`
	`%q query string (prepend with '?' or empty '-')`
	`%t timestamp HH:MM:SS (same as Apache '%(%H:%M:%S)t' or '%(%T)t')`
	`%u remote user (could be bogus for 401 status)`
	`%U URL path info`
	`%r first line of request (same as '%m %U%q <version>')`
	`%s return status`
	The maximum length for each directive is 64 bytes. The exception is '%r' where each element is limited to 64 bytes (i.e. method, URL path info, and query string). The default log format string is: `%h %t "%r" %s %B "%{Referer}i" "%{User-Agent}i"`

HTTP Authentication Page

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

For example, to add web pages to the IntelliBox to control or monitor of a device attached to a port on the IntelliBox, you can specify the user and password that can access that web page.

If you click **Authentication** at the top of one of the HTTP pages, the HTTP Authentication page displays. Here you can change HTTP authentication settings.

Under **Current Configuration**, **URI** and **Users** have a **Delete** link. If you click **Delete**, a message asks whether you are sure you want to delete this information. Click **OK** to proceed or **Cancel** to cancel the operation.

Example:

The following example shows how to add authentication to user-loaded web pages in a directory called port1control.

1. Create a directory called **port1control** in the IntelliBox's file system (using an FTP client, Windows Explorer, or the IntelliBox Web Manager).
2. Copy the custom web pages to this directory.
3. On the HTTP Authentication page of the IntelliBox Web Manager, add:

- A **URI** of **Location where to store the user**
- A **Realm** of **Monitor**
- An **AuthType** of **Digest**
- A **Username** and **Password**

4. Click the **Submit** button. The IntelliBox creates a username and password to allow the user to access all web pages located in the directory **port1control** in the IntelliBox file system.

Note: *The URI, realm, username, and password are user-specified, free-form fields. The URI must match the directory created on the IntelliBox file system. The URI and realm used in the example above are only examples and would typically be different as specified by the user.*

Figure 9-8 HTTP Authentication Page

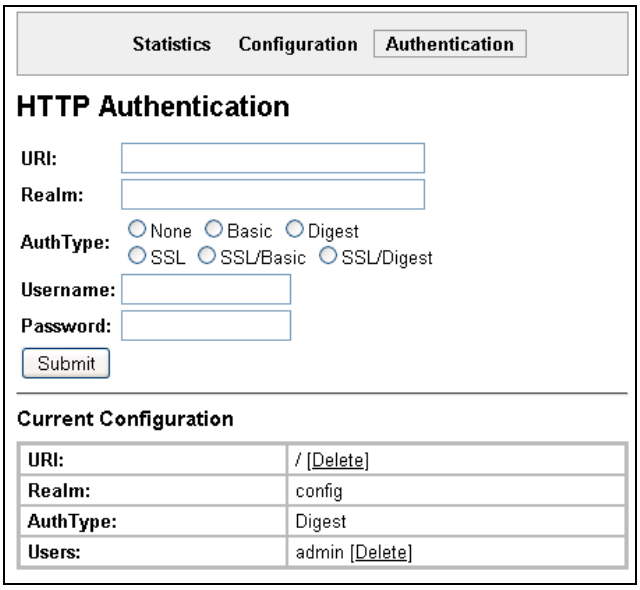


Table 9-7 HTTP Authentication Page

HTTP Authentication Page Settings	Description
URI	Enter the Uniform Resource Identifier (URI) of the resource that will participate in the authentication process. Default is /.
Realm	Enter the domain, or realm, used for HTTP operations. Default is <config>.
AuthType	Select an authorization type. Different types of authorization offer varying levels of security. Choices are (from least to most secure): **None** = no authentication necessary. **Basic** = encodes passwords using Base64. **Digest** = encodes passwords using MD5. (default) **SSL** = page can only be accessed over SSL (no password). **SSL/Basic** = page can only be accessed over SSL (encodes passwords using Base64). **SSL/Digest** = page can only be accessed over SSL (encodes passwords using MD5). SSL alone does not require a password, but all data transferred to and from the HTTP Server is encrypted. There is no reason to create an authentication directive using None, unless you want to override a parent directive that uses some other **AuthType**. Multiple users can be configured within a single authentication directive.
Username	Enter the name of the user who will participate in the authentication. Default is admin.
Password	Enter the password that will be associated with the username. Default is PASS.

RSS Page

f you click **RSS** on the menu, the RSS page displays. Here you can specify RDF Site Summary (RSS) information. RSS is a way of feeding online content to web users. Instead of actively searching for IntelliBox configuration changes, RSS displays only relevant and new information regarding changes made to the IntelliBox via an RSS publisher.

Under **Current Configuration**, **Data** has **View** and **Clear** links. If you click **View**, the data displays. If you click **Clear**, a message asks whether you are sure you want to delete this information. Click **OK** to proceed or **Cancel** to cancel the operation.

Figure 9-9 RSS Page

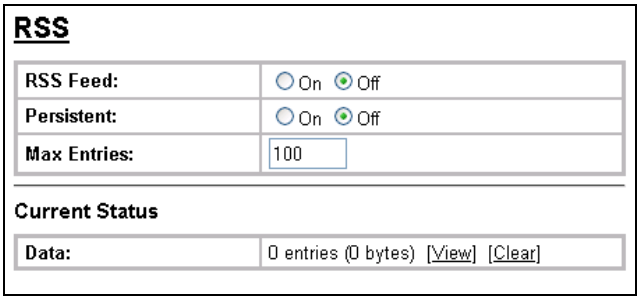


Table 9-8 HTTP RSS Page

HTTP RSS Page Settings	Description
RSS Feed	Select whether an RSS feed is enabled or disabled. An RSS syndication feed is served by the HTTP server. This feed contains up-to-date information about configuration changes that occur on the IntelliBox. Choices are: **On** = RSS feed is enabled. **Off** = RSS feed is disabled. (default)
Persistent	Select whether the RSS feed is persistent. Choices are: **On** = data is stored on the filesystem, in the file **/cfg_log.txt**. This allows feed data to be available across reboots or until the factory defaults are set. **Off** = data is not stored on the filesystem. (default) ***Note:*** *If you select* ***On****, only configuration entries corresponding to configuration changes become persistent.*
Max Entries	Enter the maximum number of log entries. The RSS feed is a scrolling feed, with only the last Max **Entries** cached and viewable. To be notified automatically about any configuration changes that occur, register the RSS feed within your favorite RSS aggregator. Default is 100. Each RSS feed entry is prefixed with a timestamp [BC:HH:MM:SS]. BC is the Boot Cycle value and indicates the number of times the IntelliBox has rebooted since factory defaults were last loaded. The resulting "HH:MM:SS" is the time since the IntelliBox booted.

LPD Pages

The IntelliBox device acts as a print server ifa printer gets connecte3d to one of its serial ports. Clicking the Line Printer Daemon (LPD) link in the Main Menu displays the LPD web page. The LPD web page has three sub-menus for viewing print queue statistics, changing print queue configuration, and printing a test page. Because the LPD lines operate independently, you can specify different configuration settings for each.

Figure 9-12 LPD Statistics

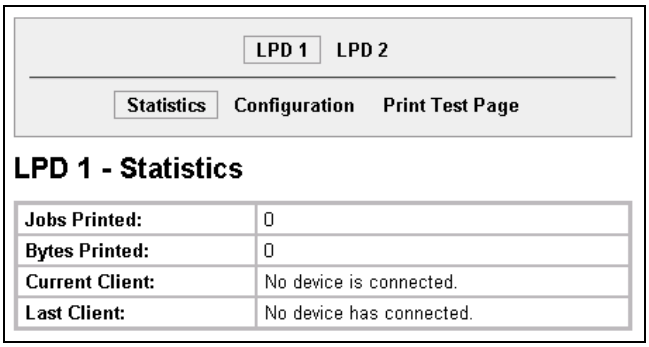


Figure 9-13 LPD Configuration

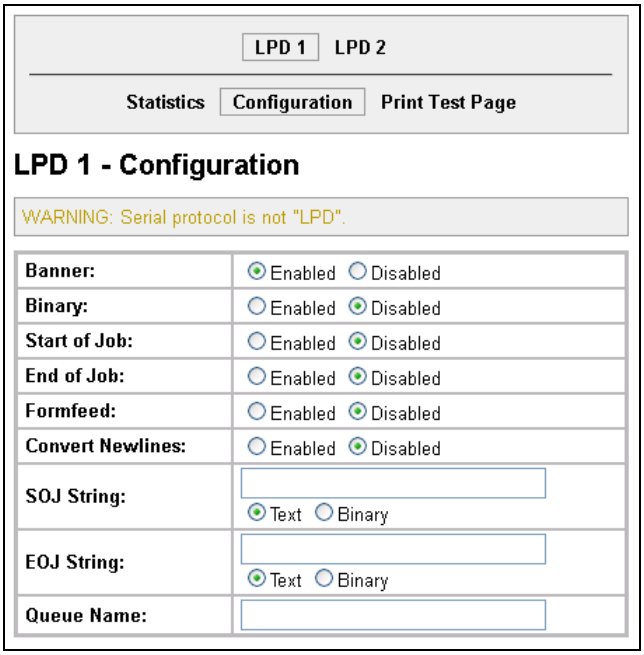
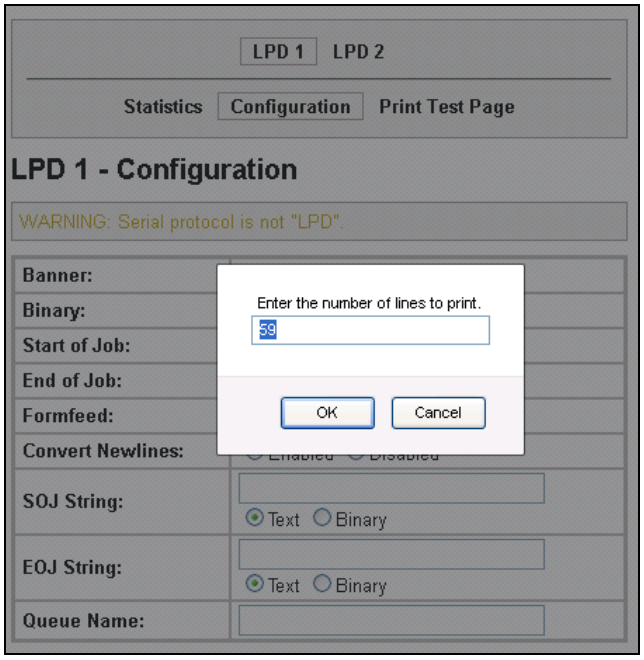


Table 9-9 LPD Configuration

LPD Page Settings	Description
Banner	Select **Enabled** to print the banner even if the print job does not specify to do so. Selected by default.
Binary	Select **Enabled** for the device to pass the entire file to the printer unchanged. Otherwise, the device passes only valid ASCII and valid control characters to the printer. Valid control characters include the tab, linefeed, formfeed, backspace, and newline characters. All others are stripped. Disabled by default.
Start of Job	Select **Enabled** to print a "start of job" string before sending the print data.
End of Job	Select **Enabled** to send an "end of job" string.
Formfeed	Select **Enabled** to force the printer to advance to the next page at the end of each print job.
Convert Newlines	Select **Enabled** to convert single newlines and carriage returns to DOS-style line endings. .
SOJ String	If **Start of Job** (above) is enabled, enter the string to be sent to the printer at the beginning of a print job. The limit is 100 characters. Indicate whether the string is in text or binary format.
EOJ String	If **End of Job** (above) is enabled, enter the string to send at the end of a print job. The limit is 100 characters. Indicate whether the string is in text or binary format.
Queue Name	To change the name of the print queue, enter a new name. The name cannot have white space in it and is limited to 31 characters. The default is **LPDQueueX** (for line number X).

Figure 9-15 LPD Print Test Page



To print an LPD test page

1. Enter the number of lines to print.
2. Click the **OK** button.

10: Security Settings

SSH Pages

Clicking the **SSH** link in the menu bar displays the SSH Server: Host Keys page. This page has four links at the top for viewing and changing SSH server host keys, SSH *server authorized keys, SSH client known hosts, and SSH client users.*

Note: *For more information, see SSH.*

SSH Server: Host Keys Page

The SSH Server: Host Keys page displays when you click **SSH** in the menu bar. It also displays when you click **SSH Server: Host Keys** at the top of one of the other SSH pages. Here you can create new keys and upload them to an SSH server.

SSH server private and public host keys are used by all applications that play the role of an SSH server, specifically the CLI and tunneling in Accept Mode. These keys can be created elsewhere and uploaded to the device, or automatically generated on the device.

Under **Current Configuration**, **Public RSA Key** and **Public DSA Key** have **View** and **Delete** links if these keys have been created. If you click **View**, the key displays. If you click **Delete**, a message asks whether you are sure you want to delete this information. Click **OK** to proceed or **Cancel** to cancel the operation.

Figure 10-1 SSH Server: Host Keys Page

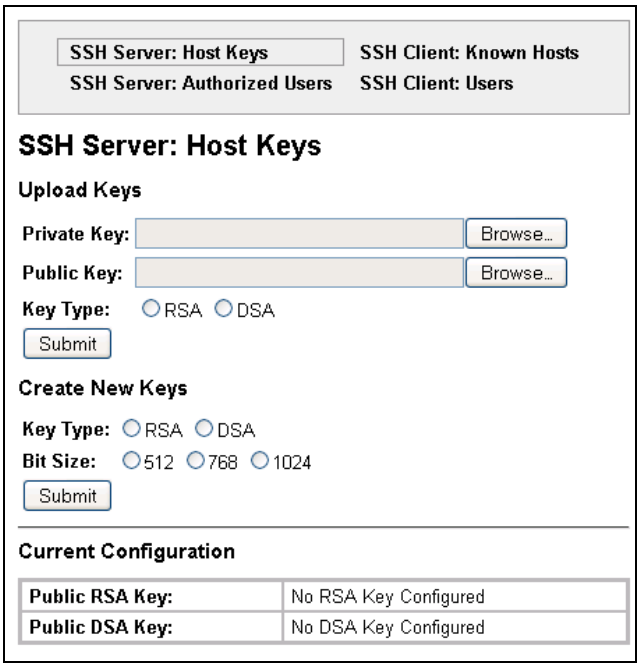


Table 10-1 SSH Server: Host Keys Page

SSH Server: Host Keys Page Settings	Description
Upload Keys	
Private Key	Enter the path and name of the existing private key you want to upload or use the **Browse** button to select the key. Be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.
Public Key	Enter the path and name of the existing public key you want to upload or use the **Browse** button to select the key.
Key Type	Select a key type to be used. Choices are: **RSA** = use this key with SSH1 and SSH2 protocols. **DSA** = use this key with the SSH2 protocol.
Create New Keys	
Key Type	Select a key type to be used for the new key. Choices are: **RSA** = use this key with the SSH1 and SSH2 protocols. **DSA** = use this key with the SSH2 protocol.
Bit Size	Select a bit length for the new key. Choices are: **512** **768** **1024** Using a larger bit size takes more time to generate the key. Approximate times are: 10 seconds for a 512-bit RSA key 1 minute for a 768-bit RSA key 2 minutes for a 1024-bit RSA key 2 minutes for a 512-bit DSA key 10 minutes for a 768-bit DSA key 15 minutes for a 1024-bit DSA key Some SSH clients require RSA host keys to be at least 1024 bits long.

SSH Client: Known Hosts Page

If you click **SSH Client: Known Hosts** at the top of one of the SSH pages, the SSH Client: Known Hosts page displays. Here you can change SSH client settings for known hosts.

Note: *You do not have to complete the fields on this page for communication to occur. However, completing them adds another layer of security that protects against Man-In-The-Middle (MITM) attacks.*

Figure 10-2 SSH Client: Known Hosts Page

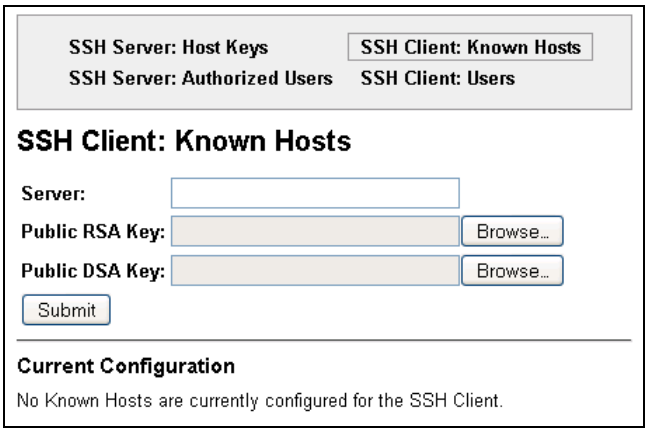


Table 10-2 SSH Client: Known Hosts Page

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

SSH Server: Authorized Users Page

If you click **SSH Server: Authorized Users** at the top of one of the SSH pages, the SSH Server: Authorized Users page displays. Here you can change SSH server settings for authorized users.

SSH Server Authorized Users are accounts on the IntelliBox that can be used to log into the IntelliBox via SSH. For instance, these accounts can be used to SSH into the CLI or open an SSH connection to a device port. Every account must have a password.

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

Under **Current Configuration**, **User** has a **Delete User** link, and **Public RSA Key** and **Public DSA Key** have **View Key** and **Delete Key** links. If you click a **Delete** link, a message asks whether you are sure you want to delete this information. Click **OK** to proceed or **Cancel** to cancel the operation.

Figure 10-3 SSH Server: Authorized Users Page

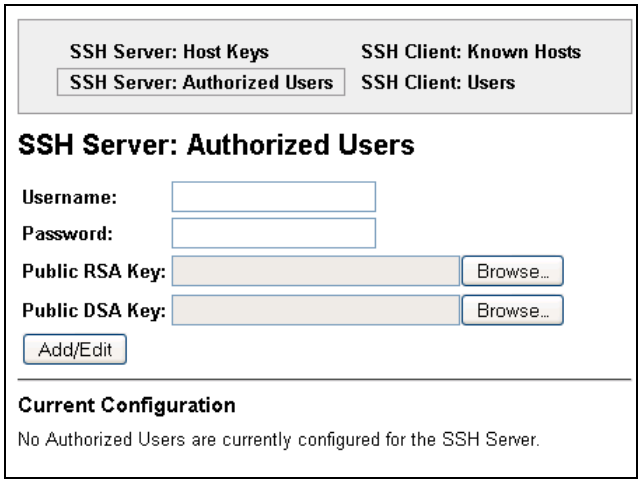


Table 10-3 SSH Server: Authorized Users Page

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

SSH Client: Users Page

If you click **SSH Client: Users** at the top of one of the SSH pages, the SSH Client: Users page displays. Here you can change SSH client settings for users.

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

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

Figure 10-4 SSH Client: Users Page

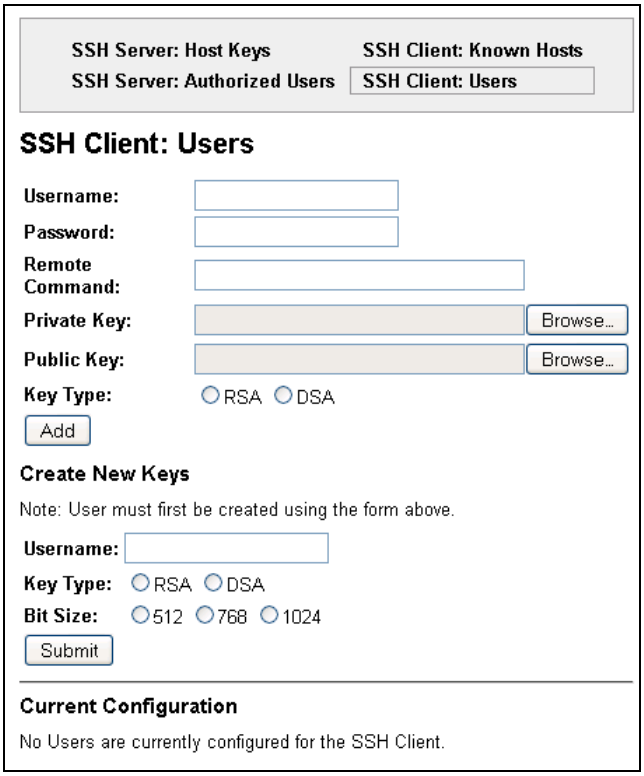


Table 10-4 SSH Client: Users Page

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

SSL Page

Clicking the **SSL** link in the menu bar displays the SSL page. Here you can upload an existing SSL certificate or create a new self-signed one.

Note: *For more information about SSL, see SSL.*

An SSL certificate must be configured for the HTTP server to listen on the HTTPS port. This certificate can be created elsewhere and uploaded to the device or automatically generated on the device. A certificate generated on the device will be self-signed. If uploading an existing SSL certificate, be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.

At the bottom of this page is the current SSL certificate, if any. Under **Current SSL Certificate**, there is a **Delete** link. If you click **Delete**, a message asks whether you are sure you want to delete the current certificate. Click **OK** to proceed or **Cancel** to cancel the operation.

Figure 10-5 SSL Page

Table 10-5 SSL Page

SSL Page Settings	Description
Upload Certificate	
New Certificate	Enter the path and name of the existing certificate you want to upload, or use the **Browse** button to select the certificate.
New Private Key	Enter the path and name of the existing private key you want to upload, or use the **Browse** button to select the private key.
Upload Authority Certificate	
Authority	Enter the path and name of the authority certificate you want to upload, or use the **Browse** button to select the authority certificate.
Create New Self-Signed Certificate	
Country (2 Letter Code)	Enter the 2-letter country code to be assigned to the new self-signed certificate. Examples: US for United States and CA for Canada
State/Province	Enter the state or province to be assigned to the new self-signed certificate.
Locality (City)	Enter the city or locality to be assigned to the new self-signed certificate.
Organization	Enter the organization to be associated with the new self-signed certificate. **Example:** If your company is called Widgets, and you are setting up a web server for the Sales department, enter Widgets for the Organization.
Organization Unit	Enter the organizational unit to be associated with the new self-signed certificate. **Example:** If your company is setting up a web server for the Sales department, enter Sales for your Organizational Unit.
Common Name	Enter the same name that the user will enter when requesting your web site. **Example:** If a user enters http://www.widgets.abccompany.com to access your web site, the **Common Name** would be www.widgets.abccompany.com.
Expires	Enter the expiration date, in mm/dd/yyyy format, for the new self-signed certificate. **Example:** An expiration date of May 9, 2007 is entered as 05/05/2007.

SSL Page Settings	Description
Key length	Select the bit size of the new self-signed certificate. Choices are: **512 bit** **768 bit** **1024 bit** Using a larger bit size takes more time to generate the key. Approximate times are: 2 minutes for a 512 bit RSA Key 5 minutes for a 768 bit RSA Key 15 minutes for a 1024 bit RSA Key 8 minutes for a 512 bit DSA Key 20 minutes for a 768 bit DSA Key 60 minutes for a 1024 bit DSA Key
Type	Select the type of key: **RSA** **DSA**

11: Maintenance and Diagnostics Settings

Filesystem Pages

Clicking the **Filesystem** link in the menu bar displays the Filesystem Statistics page. This page has two links at the top for viewing filesystem statistics and browsing and manipulating the entire filesystem.

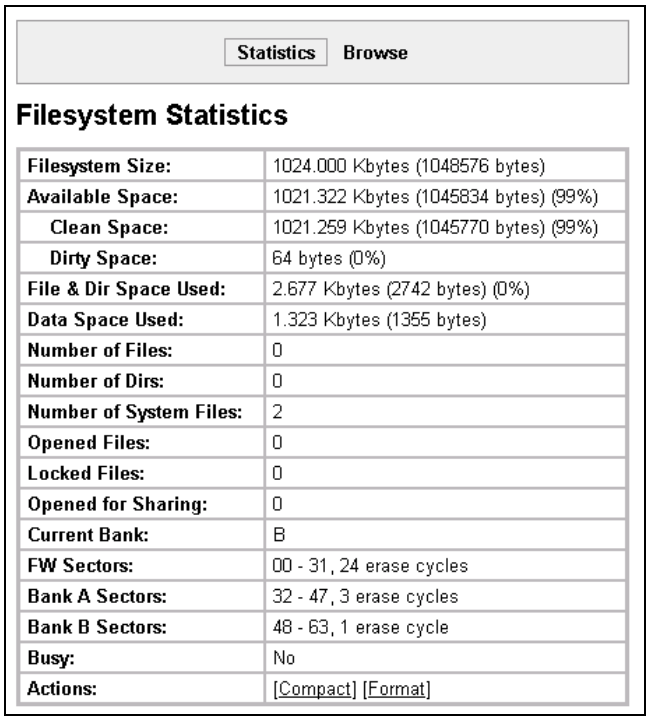
Filesystem Statistics Page

The Filesystem Statistics page displays when you click **Filesystem** in the menu bar. It also displays when you click **Statistics** at the top of the Filesystem Browser page. This page displays various statistics and current usage information of the flash filesystem.

The **Actions** row provides **Compact** and **Format** links for compacting or formatting the filesystem. Only a system administrator should perform these tasks.

Note: ***Compact*** *preserves data and eliminates dirty space by making a new copy.* ***Format*** *destroys all of the data in the filesystem.*

Figure 11-1 Filesystem Statistics Page



Filesystem Browser Page

If you click **Browse** at the top of a Filesystem page, the Filesystem Browser page displays. Here you can browse and manipulate the entire filesystem. For example, you can:

- Browse the filesystem.
- Create files and directories.
- Upload files via HTTP.
- Copy and move files.
- Transfer files to and from a TFTP server.

Figure 11-2 Filesystem Browser Page

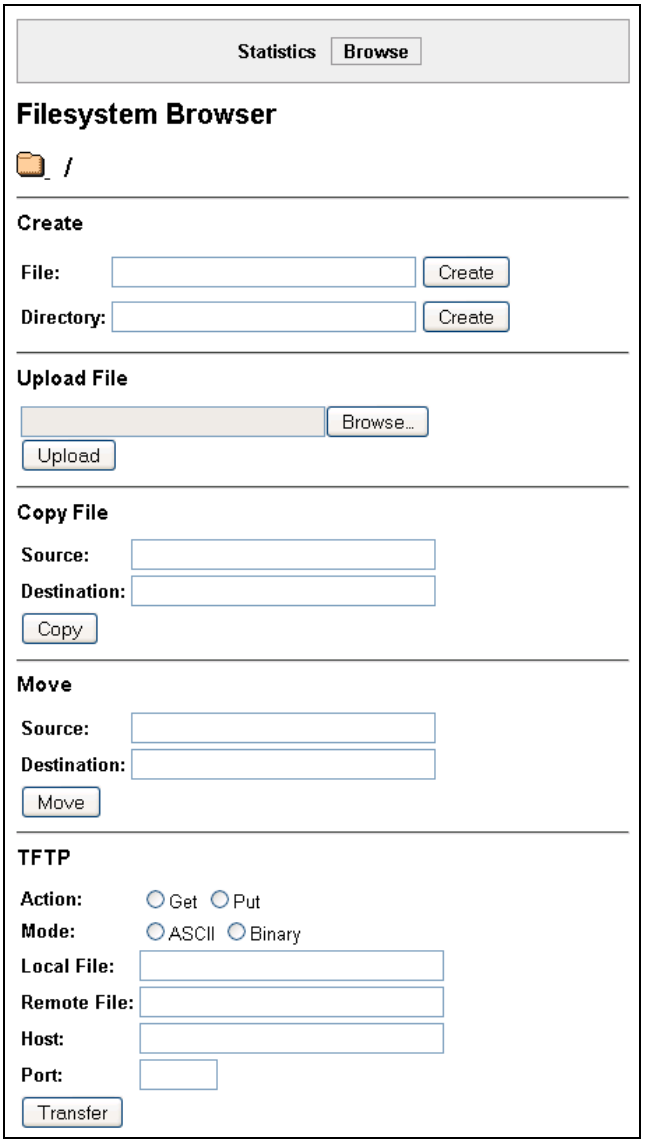


Table 11-1 Filesystem Browser Page

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

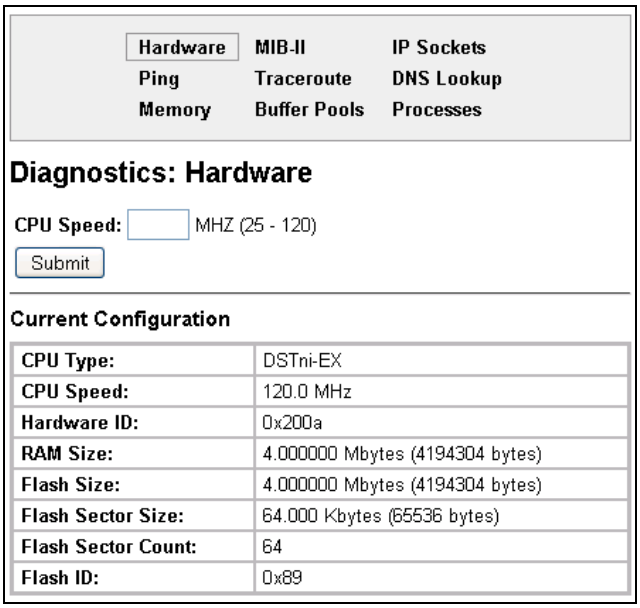
Diagnostics Pages

The IntelliBox has several tools for performing diagnostics. To view these diagnostic tools, click the **Diagnostics** link in the menu bar to display the Diagnostics: Hardware page. The available diagnostic tools appear at the top of the page.

Diagnostics: Hardware Page

The Diagnostics: Hardware page displays when you click **Diagnostics** in the menu bar. It also displays when you click **Hardware** at the top of one of the other Diagnostic pages. This read-only page displays the current hardware configuration.

Figure 11-3 Diagnostics: Hardware Page

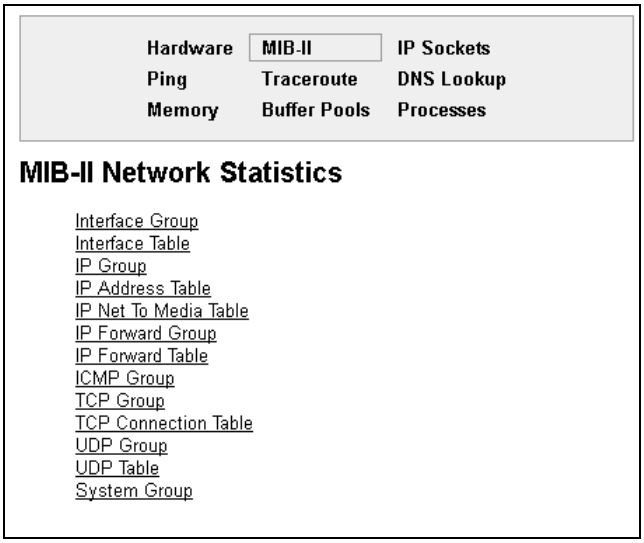


MIB-II Network Statistics Page

Clicking **MIB-II Stats** from one of the Diagnostics pages displays the MIB-II Network Statistics page. This page displays the various SNMP-served Management Information Bases (MIBs) available on the IntelliBox. Information about these MIBs can be found in the following Request for Comments (RFCs):

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

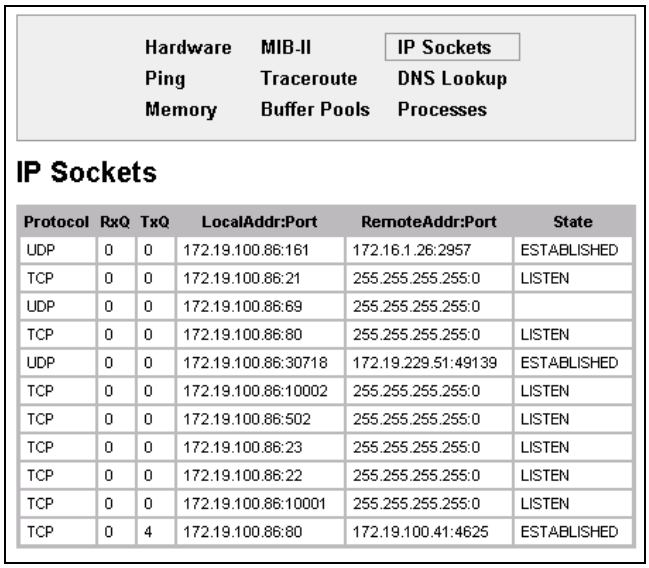
Figure 11-4 Diagnostics: MIB-II Network Statistics Page



IP Sockets Page

Clicking **IP Sockets** from one of the Diagnostics pages displays the IP Sockets page. This read-only page lists all the network sockets on the IntelliBox that are currently open.

Figure 11-5 Diagnostics: IP Sockets Page



Diagnostics: Ping Page

Figure 11-6 Diagnostics: Ping Page

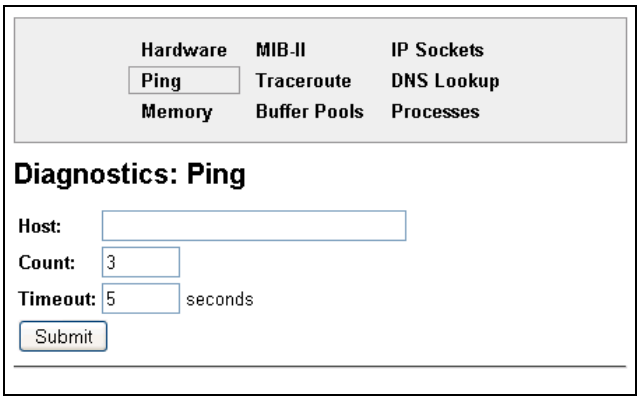


Table 11-2 Diagnostics: Ping Page

Diagnostics: Ping Page Settings	Description
Host	Enter the IP address you want the IntelliBox to ping.
Count	Enter the number of ping packets that the IntelliBox should try to send to the Host. Default is 3.
Timeout	Enter the maximum number of seconds that the IntelliBox should wait for a response from the host before timing out. Default is 5 seconds.

Diagnostics: Traceroute Page

Clicking **Traceroute** from one of the Diagnostics pages displays the Diagnostics: Traceroute page. Here you can trace a packet from the IntelliBox to an Internet host, showing how many hops the packet requires to reach the host and how long each hop takes. If you visit a web site whose pages appear slowly, you can use traceroute to determine where the longest delays are occurring.

Figure 11-7 Diagnostics: Traceroute Page

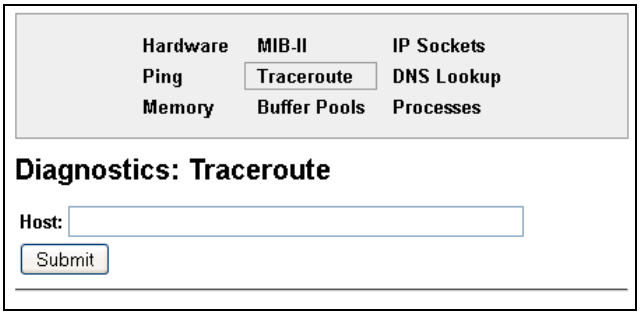


Table 11-3 Diagnostics: Traceroute Page

Diagnostics: Traceroute Page Settings	Description
Host	Enter the IP address or DNS host name of the remote host that you want to traceroute from the IntelliBox.

Diagnostics: DNS Lookup Page

Clicking **DNS Lookup** from one of the Diagnostics pages displays the Diagnostics: DNS Lookup page. Here you can specify a DNS Hostname for a forward lookup or an IP address for a reverse lookup. You can also perform a lookup for a Mail (MX) record by prefixing a DNS Hostname with @.

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

Figure 11-8 Diagnostics: DNS Lookup Page

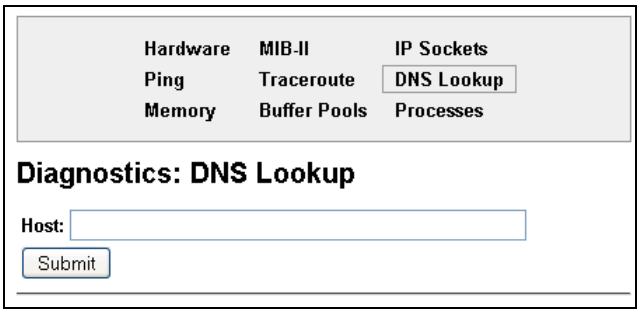


Table 11-4 Diagnostics: DNS Lookup Page

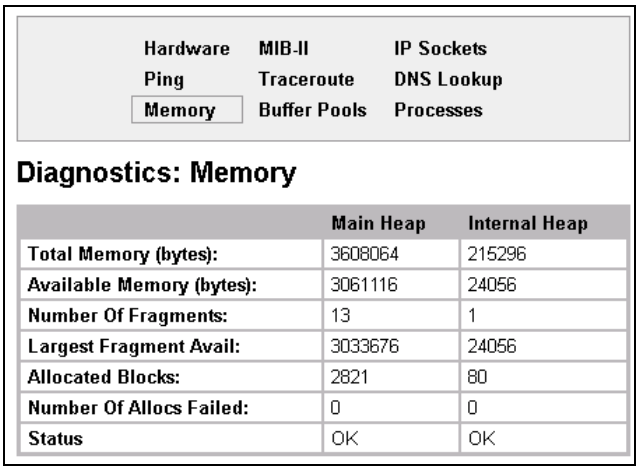
Diagnostics: DNS Lookup Page Settings	Description
Host	Perform one of the following: For reverse lookup to locate the hostname for that IP address, enter an IP address. For forward lookup to locate the corresponding IP address, enter a hostname. To look up the Mail Exchange (MX) record IP address, enter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

Diagnostics: Memory Page

Clicking **Memory** from one of the Diagnostics pages displays the Diagnostics: Memory. This read-only page shows the total memory and available memory (in bytes), along with the number of fragments, allocated blocks, and memory status.

The Diagnostics: Memory page also shows the current amount of available memory.

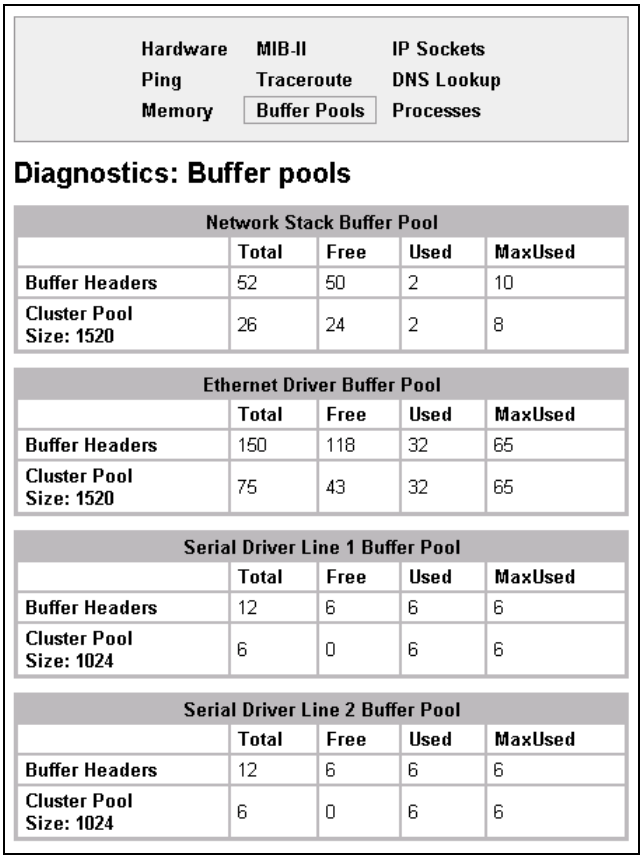
Figure 11-9 Diagnostics: Memory Page



Diagnostics: Buffer Pool

Clicking **Buffer Pools** from one of the diagnostics page displays a read-only screen that shows the current usage of the private buffer pools. Private buffer pools are used in various parts of the system to ensure deterministic memory management, thus eliminating any contention for memory from the generic heap space.

Figure 11-10 Diagnostics: Buffer Pools Page

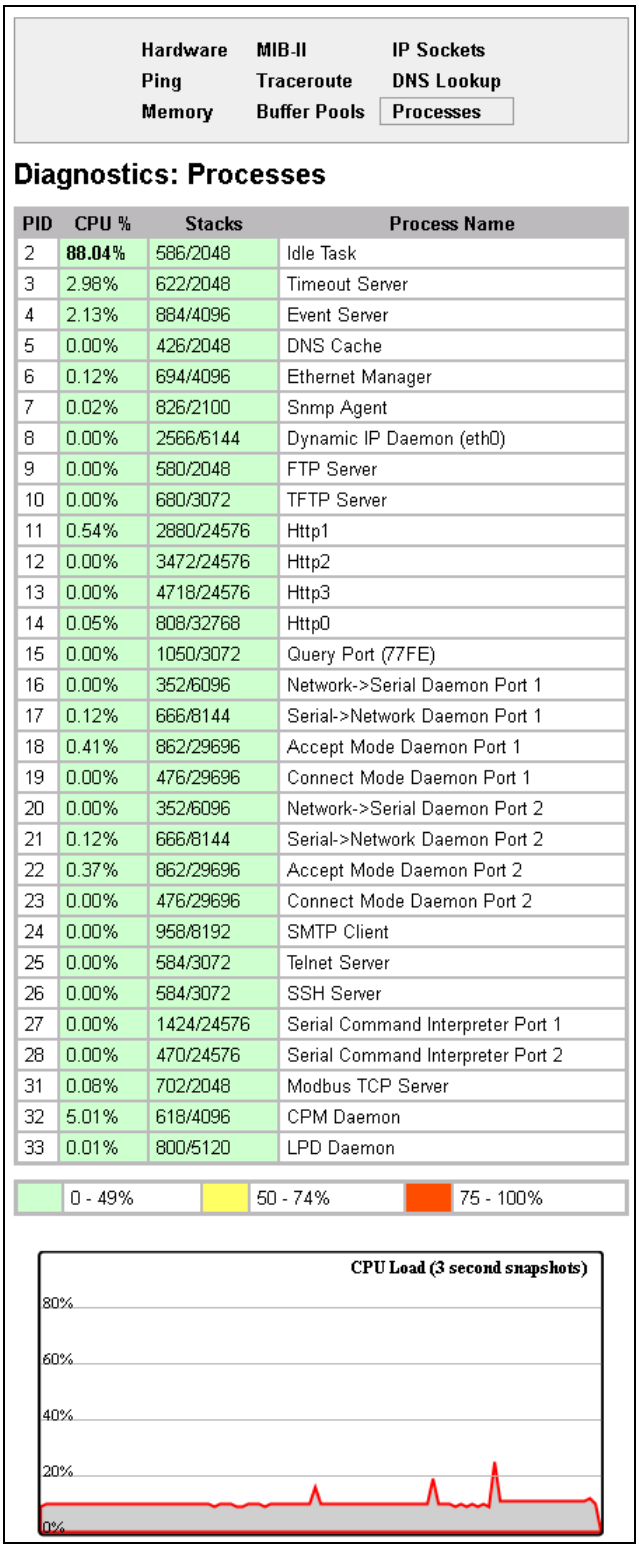


Diagnostics: Processes Page

Clicking **Processes** from one of the diagnostics page displays a read-only screen that lists all processes running on the IntelliBox.

- The **CPU %** column displays the percentage of total CPU cycles a process used in the last two seconds.
- The **Stacks** column displays the total stack space available to the process and the maximum amount of the stack space the process used since it was started.

Figure 11-11 Diagnostics: Processes Page



Below the process chart is a CPU Load Graph that shows the CPU load over the last five minutes. The IntelliBox generates the graph using the Scalable Vector Graphics (SVG)

modularized XML language and updates every two seconds. The information area contains a link for viewing the raw SVG XML.

Note: *The SVG plug-in is available on the Internet.*

System Page

Clicking the **System** link in the menu bar displays the System page. Here you can:

- Reboot the IntelliBox.
- Restore factory defaults.
- Upload new firmware.
- Assign short and long names to the IntelliBox.
- Change time settings.

Figure 11-12 System Page

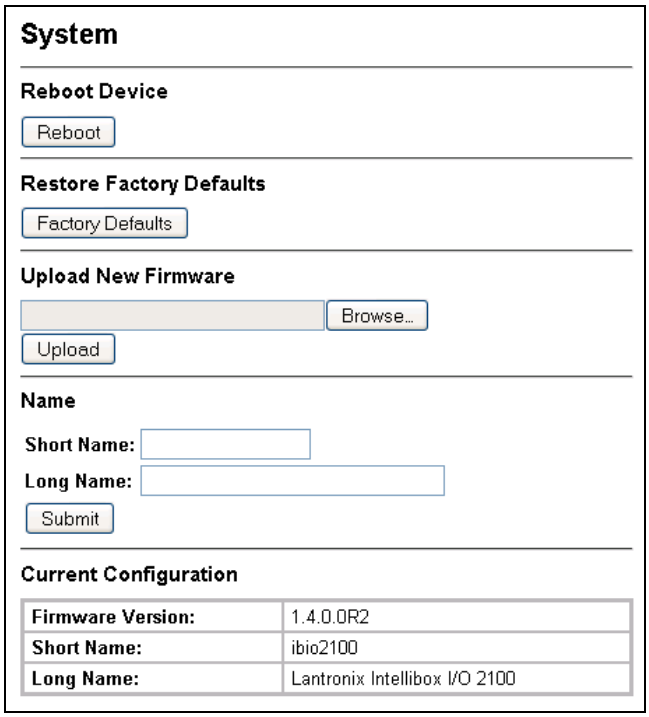


Table 11-5 System Page

System Page Settings	Description
Reboot Device	Click the **Reboot** button to reboot the IntelliBox. When the IntelliBox reboots, refresh your web browser and redirect it to the IP address for the IntelliBox.
Restore Factory Defaults	Click the **Factory Defaults** button to return the IntelliBox to its factory-default configuration. *A: Factory Default Configuration* identifies the factory-default configuration. If you restore the factory default configuration, the IntelliBox reboots automatically. Using this function also erases the IP address, subnet and gateway of the IntelliBox.
Upload New Firmware	Lets you update the IntelliBox firmware. Do not power off or reset the IntelliBox while uploading new firmware. Once the upload has completed and the new firmware has been verified and flashed, the IntelliBox reboots automatically. For instructions about upgrading firmware, see *14: Updating Firmware*.
Name	Enter the short name and long name for the IntelliBox. Default short name is IntelliBoxio and default long name is Lantronix IntelliBox.

Query Port Page

Clicking the **Query Port** link in the menu bar displays the Query Port page. This page displays statistics and current usage information about the query port server. The query port server is an application that only responds to auto-discovery messages on port 0x77FE. It is used when DeviceInstaller is used to discover the IntelliBox automatically.

Figure 11-13 Query Port Page

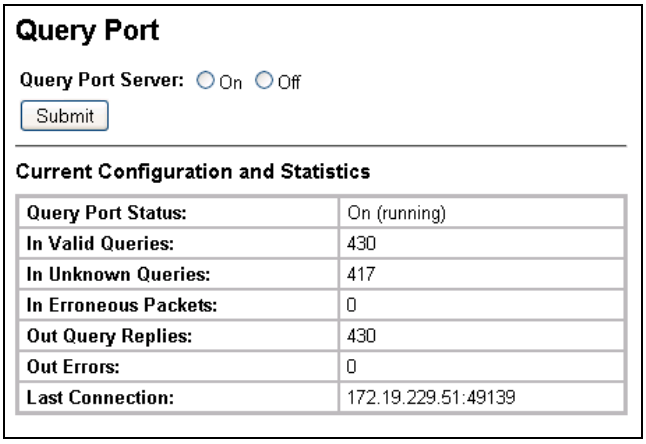


Table 11-6 Query Port Page

Query Port Page Settings	Description
Query Port Server	Select whether the query port server is enabled or disabled. Choices are: **On** = query port server is enabled. (default) **Off** = query port server is disabled.

12: Advanced Settings

Input/Output Page

The IntelliBox has two digital input/outputs (I/Os) and a relay. This page allows you to manage the digital I/Os on the IntelliBox. Inputs can monitor external devices that have digital outputs for use with EventTrak or for sending an email message. EventTrak or Tunnel connections can use outputs to control external devices.

You can monitor or control digital I/Os on the Tunnel Connect, Tunnel Accept, and EventTrak pages. The Input/Output page enables you to manually control the digital output and relay.

Input/Output Page

The Input/Output page displays when you click **Input/Output** in the menu bar. A **Submit** button displays if you modify either a direction or a control. Clicking **Submit** applies changes immediately to the IntelliBox.

Figure 12-1 Input Output Page

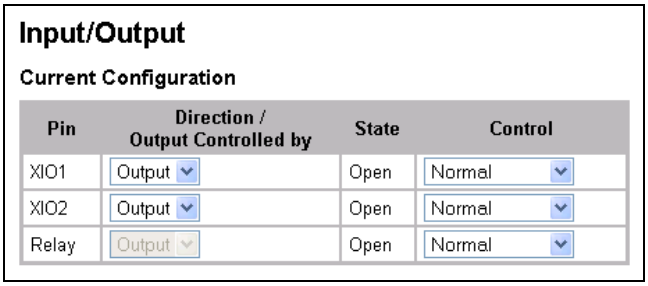


Table 12-1 Input/Output Page

Input/Output Page Settings	Description
Pin	Identifies the digital switch port and the relay.
Direction	Select the direction of data flow. Choices are: **Input** = pin is set to read input **Output** = pin is set to drive data out of the IntelliBox .
Output Controlled by	The functions that control an output display in rows below the output.
State	Displays the state of an input or output pin. The state of an input pin, **High** or **Low**, depends on the external voltage sensed. When a pin is configured as ouput, it acts as a solid state switch and has a state of either **Open** or **Closed**. Initially the output is **Open**. The Output is **Closed** if just one controlling function is asserted **Closed**, such as in Tunnel1 Connect Mode.
Control	Select the output controls. Choices are: **Normal** = allows an output to be controlled normally by the configured device functions **Force Closed** = asserts the output as **Closed** regardless of the state of the device functions. For example, even if other functions within the IntelliBox have not changed the pin state, you can still force the output state closed manually. **Force Open**: asserts the output as **Open** regardless of the state of the device functions. For example, even if other functions within the IntelliBox have not changed the pin state, you can still force the output state closed manually.
RSS Trace transitions	A change in the state of a pin triggers the IntelliBox to send an RSS feed. Primarily used for troubleshooting. RSS Trace transitions are visible when XI01/XI02 are set to the Input option.

Note: *The Relay is an output port only.*

Email Pages

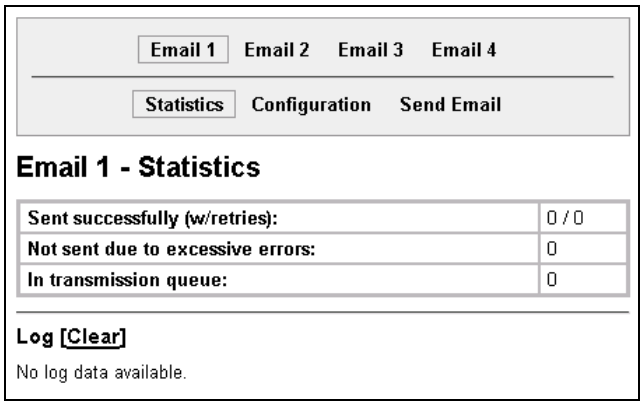
Clicking the **Email** link in the menu bar displays the Email Statistics page. This page has links at the top for displaying the email configuration and for sending an email. You can configure the email subsystem for delivering email notifications and send an email.

Email Statistics Page

The Email Statistics page displays when you click **Email** in the menu bar. It also displays when you click **Statistics** at the top of one of the Configuration page. This read-only page shows various statistics and current usage information about the email subsystem. Click the desired email at the top of the page to view its statistics.

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

Figure 12-2 Email Statistics Page



Email Configuration Page

If you click **Configuration** at the top of one of the Email pages, the Email Configuration page displays. Here you can change email configuration settings.

From the **Select Email** drop-down list at the top of the page, select the email whose configuration you want to view. The number of emails is the number of email configurations available. For example, if the highest email number available is four, then four different email addresses can be used.

Figure 12-3 Email Configuration Page

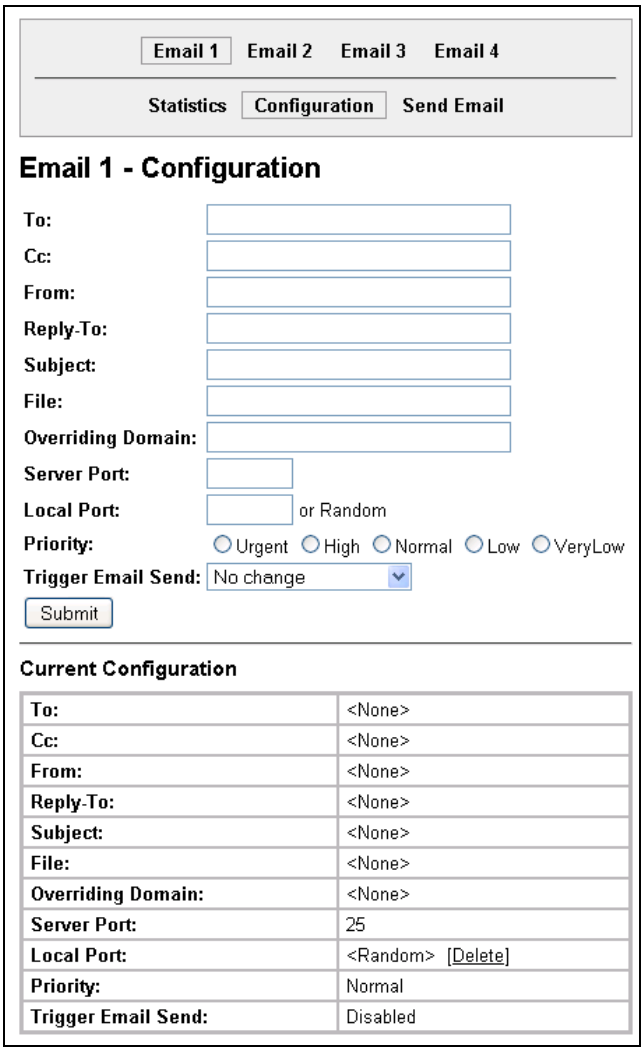


Table 12-2 Email Configuration Page

Email Configuration Page Settings	Description
To (Required)	Enter the email address of the recipient of this message. Separate multiple email addresses with semi-colons.
Cc	Enter the email address to receive a copy of this message. Separate multiple email addresses with semi-colons.
From (Required)	Enter the email address of the sender of this type of email.
Reply –To	Enter the email address to which replies should be sent.
Subject	Enter the subject of the email.
File	Enter the file on the filesystem that will be sent with each notification email message. The file is inserted as the message text, not as an attachment.
Overriding Domain	Enter the sender's domain name that will be forged in the outgoing email message. This domain name may be needed if this device is located behind a firewall whose IP address resolves to a different domain name than this device. For SPAM protection, many SMTP servers perform reverse lookups on the sender IP address to ensure the email message is really from whom it says it is from.
Server Port	Enter the SMTP server port number. The default is 25.
Local Port or Random	Enter the local port to use for email alerts. The default is a random port number.
Priority	Select the priority level for the email alert.
Trigger Email Send	Select the condition that serves as a trigger for sending an email.

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

CLI Pages

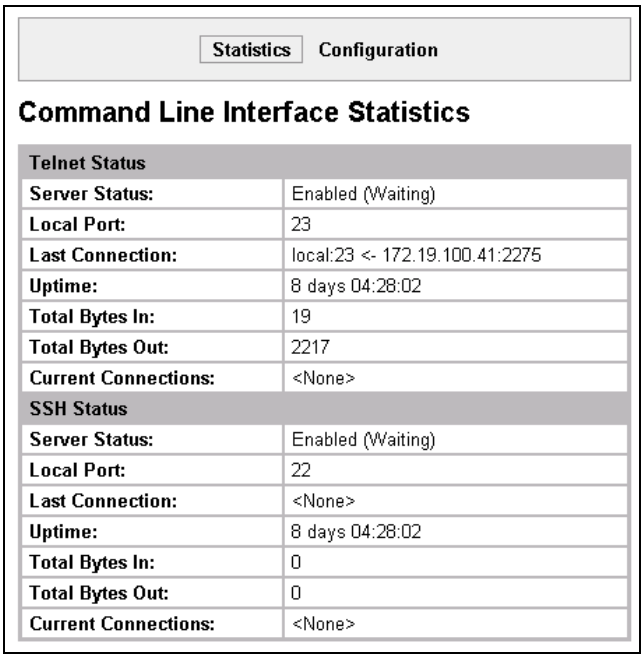
Clicking the **CLI** link in the menu bar displays the Command Line Interface Statistics page. This page has two links at the top for viewing statistics and for viewing and changing configuration settings.

Command Line Interface Statistics Page

The Command Line Interface Statistics page displays when you click **CLI** in the menu bar. It also displays when you click **Statistics** at the top of the CLI Configuration page. This read-only page shows the current connection status of the CLI servers listening on the Telnet and SSH ports. When a connection is active:

- The remote client information displays.
- The number of bytes that have been sent and received displays.
- A **Kill** link can be used to terminate the connection.

Figure 12-4 Command Line Interface Statistics Page



Command Line Interface Configuration Page

If you click **Configuration** at the top of the Command Line Interface Statistics page, the Command Line Interface Configuration page displays. Here you can change CLI configuration settings.

Under **Current Configuration**, **Password** has a **Delete** link at its right. If you click **Delete**, a message asks whether you are sure you want to delete this information. Click **OK** to proceed or **Cancel** to cancel the operation.

Figure 12-5 Command Line Interface Configuration Page

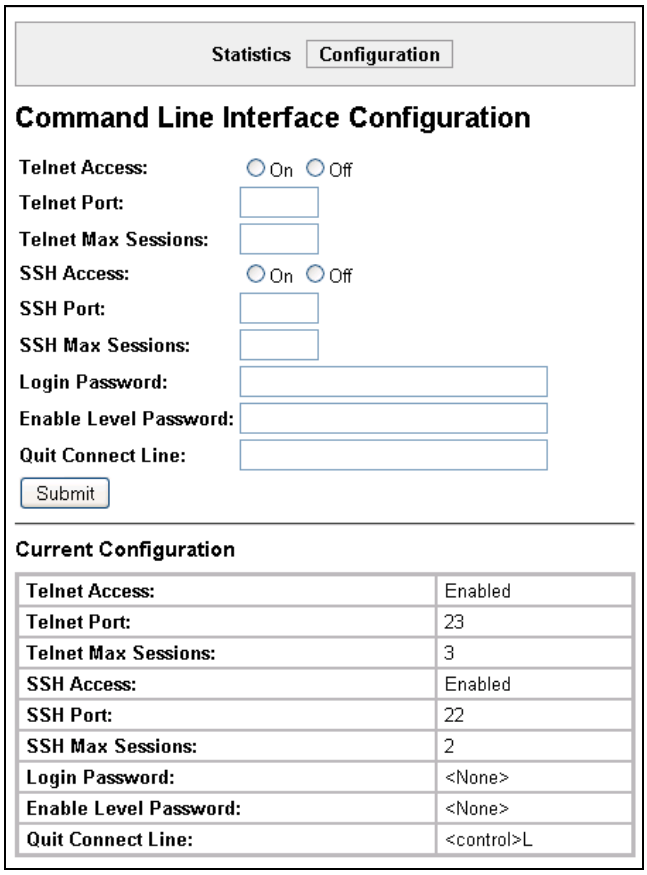


Table 12-3 Command Line Interface Configuration Page

Command Line Interface Configuration Page Settings	Description
Telnet Access	Select whether Telnet access is enabled. Choices are: **On** = Telnet access is enabled. (default) **Off** = Telnet access is disabled.
Telnet Port	Enter the number of the port on which the IntelliBox listens for incoming Telnet connections. Default is 23.
Telnet Max Sessions	Specify the maximum number of simultaneous telnet sessions that will be allowed. Maximum is 10.
SSH Access	Select whether Secure Shell (SSH) access is enabled. Choices are: **On** = SSH access is enabled. (default) **Off** = SSH access is disabled. ***Note:*** *The SSH Server Authorized Users are used for initial login access. See SSH Server: Authorized Users Page.*
SSH Port	Enter the number of the port on which the IntelliBox listens for incoming SSH connections. Default is 22.

Command Line Interface Configuration Page Settings	Description
SSH Max Sessions	Specify the maximum number of simultaneous SSH sessions that will be allowed.
Login Password	Enter the password that must be specified for the initial Telnet login session. Default is PASS.
Enable Level Password	Enter the password that must be specified to access the “enable” level in the CLI. Disabled by default.
Quit connect line	Enter a string to terminate a connect line session and resume the CLI. Type **<control>** before any key the user must press when holding down the **Ctrl** key. An example of such a string is **<control>L.** ***Note:*** *A connect line session is a CLI-only feature. Type* `connect <line>` *and subsequent characters go out the selected line and a subsequent display comes from characters received on the line. This mode ends after you type this string (e.g.,* `<control>L`*). The CLI command mode returns.*

XML Pages

The IntelliBox can be configured using an XML configuration record. Clicking the **XML** link in the menu bar displays the XML page. This page has three links at the top for exporting an XML configuration record, exporting an XML status record, and importing an XML configuration record.

XML Configuration Record: Export System Configuration Page

The XML Configuration Record: Export System Configuration page displays when you click **XML** in the menu bar. It also displays when you click **Export XML Configuration Record** at the top of one of the other XML pages. Here you can export the current system configuration in XML format. The generated XML file can be imported later to restore a configuration. It can also be modified and imported to update the configuration on this IntelliBox unit or another. The XML data can be exported to the browser window or to a file on the filesystem.

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

Figure 12-6 XML Configuration Record: Export System Configuration Page

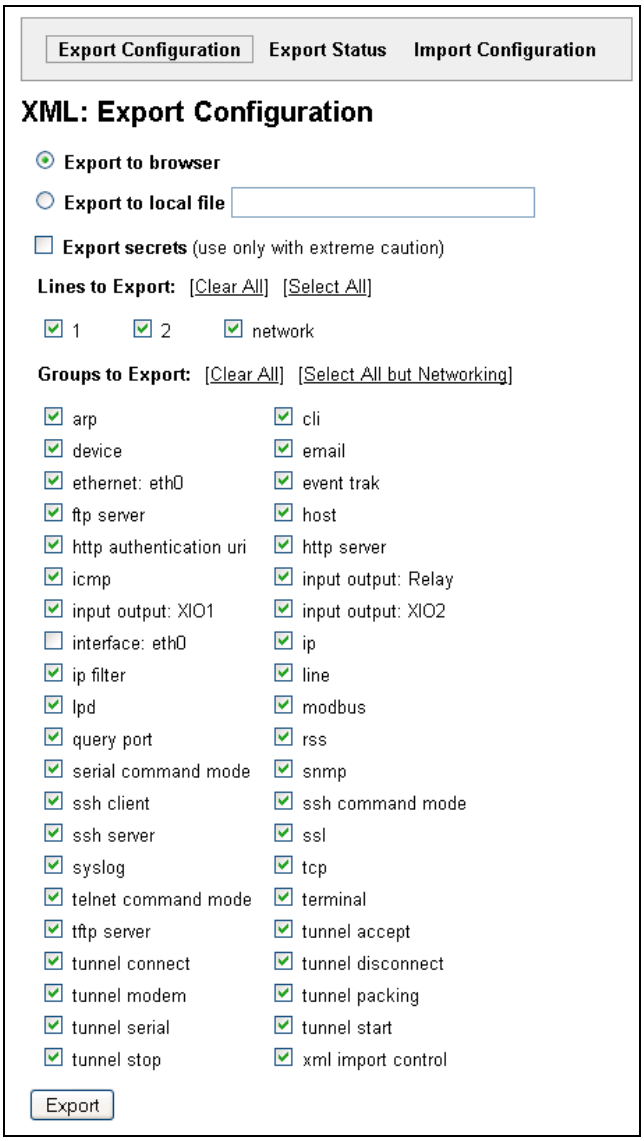


Table 12-4 Configuration Record: Export System Configuration Page

XML Configuration Record: Export System Configuration Page Settings	Description
Export to browser	Select this option to export the XCR data in the selected fields to a web browser.
Export to local file	Select this option to export the XCR data to the filesystem on the IntelliBox filesystem. If you select this option, enter a file name for the XML configuration record.
Export secrets	Check to export secrets when exporting and http authentication uri groups, SSH and SSL certificates so that the configuration may later be restored.
Lines to Export	Check the instances to be exported in the event trak, line, lpd, serial, tunnel and terminal groups.
Groups to Export	Check the configuration groups that are to be exported to the XML configuration record. If no groups are checked, all groups will be exported.

XML Status Record: Export System Status

If you click **XML Status Record** at the top of an XML page, the XML Status Record: Export System Status page displays. Here you can export the current system status in XML format. The XML data can be exported to the browser window or to a file on the filesystem.

Figure 12-7 XML Status Record: Export System Status Page

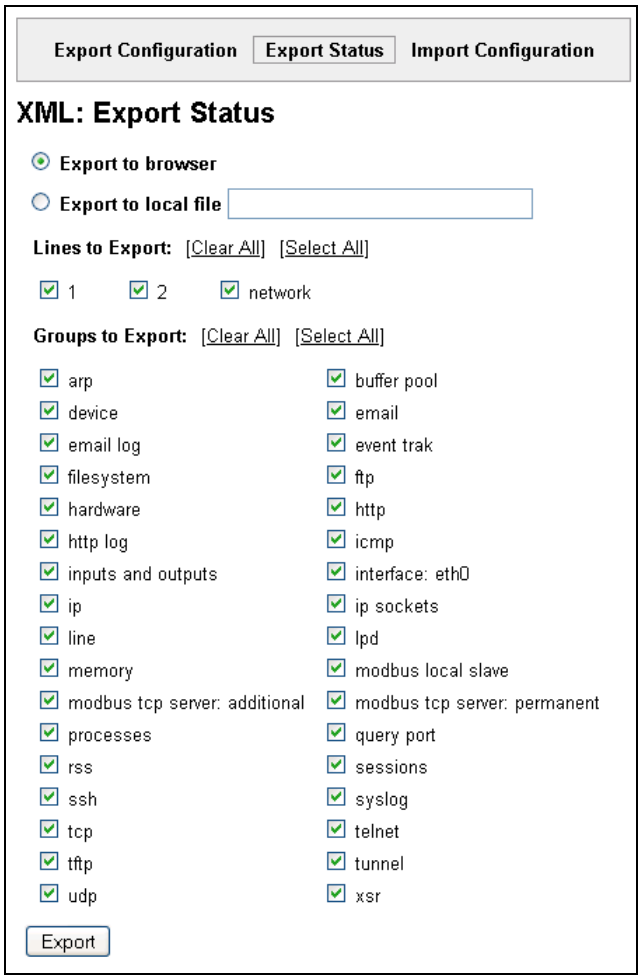


Table 12-5 XML Status Record: Export System Status Page

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

XML: Import System Configuration Page

If you click **Import XML Configuration Record** at the top of an XML page, the XML: Import System Configuration page displays. Here you can import a system configuration from an XML file.

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

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

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

Figure 12-8 XML: Import System Configuration Page

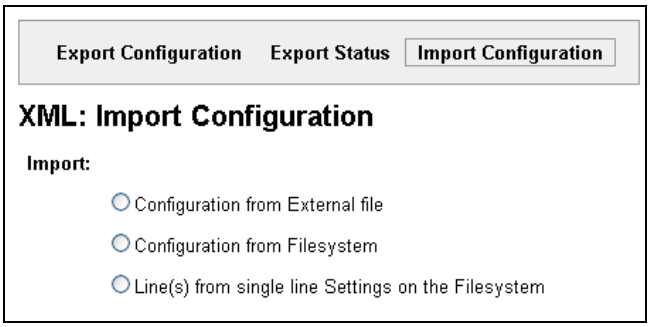


Table 12-6 XML: Import System Configuration Page

XML: Import System Configuration Page Settings	Description
Import > Configuration from External file	Click the **Configuration from External file** radio button. Then, enter the path and file name of the entire external XCR file you want to import or use the **Browse** button to select the XCR file.
Import > Configuration from Filesystem	Click the **Configuration from Filesystem** radio button. Then, complete the following fields: Enter the **Filename** of the XCR file that has certain groups you want to import. Check the **Lines to Import** to indicate the instances to be imported in the event trak, line, lpd, serial, tunnel and terminal groups. Check or uncheck the **Whole Groups to Import**. Enter content in the **Text List**. Click the **Import** button.
Import > Line(s) from single line Settings on the Filesystem	Click the **Line(s) from single line Settings on the Filesystem** radio button. Then, complete the following fields: Enter the **Filename** of the XCR file that has certain groups you want to import. Check the **Lines to Import** to indicate the instances to be imported in the event trak, line, lpd, serial, tunnel and terminal groups. Check or uncheck the **Whole Groups to Import**. Click the **Import** button.
Groups and Instances to Import	If required, enter the filter string for importing specific instances of a group.
Whole Groups to Import	Check the configuration groups that are to be imported into the XML configuration record. If no groups are checked, all groups will be imported.

Protocol Stack Page

Clicking the **Protocol Stack** link in the menu bar displays the Protocol Stack page. Here you can configure lower level network stack-specific configuration settings.

Under **Current State**, there is a **Clear** link to remove all addresses and a **Remove** link to remove the individual address shown. If you click **Clear** or **Remove**, a message asks whether you are sure you want to perform the operation. Click **OK** to proceed or **Cancel** to cancel the operation.

Figure 12-9 Protocol Stack Page (TCP)

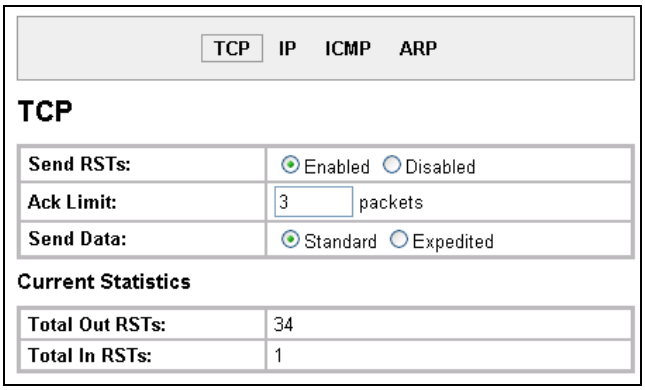


Table 12-7 TCP Protocol Stack Page

Protocol Stack Page Settings	Description
Send RSTs	RST is a TCP control bit that informs the receiving TCP stack to end a connection immediately. However, sending this bit may pose a security risk. Select whether you want the RST control bit sent to end a connection immediately. Choices are: **Enabled** = the RST bit is sent. (default) **Disabled** = the RST bit is not sent.
Ack Limit	Specify a value indicating the number of packets which must be received before an ACK is forced. If there is a large amount of data to acknowledge, an ACK will be forced before this. If the sender TCP implementation waits for an ACK before sending more data even though the window is open, setting Ack Limit to "1" packet will improve performance by forcing immediate acknowledgements.
Send Data	Determine when data may be sent to the network. Choices are: **Standard** = waits for an ACK before sending a packet less than the maximum length. **Expedited** = sends data whenever the window allows it.

Figure 12-10 Protocol Stack Page (IP)

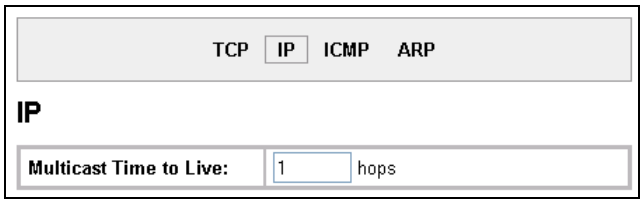


Table 12-8 IP Protocol Stack Page

Protocol Stack Page Settings	Description
Multicast Time to Live	Enter the **Multicast Time to Live** value in the IP header. Normally this value will be one so the packet will be blocked at the first router. Set this value to greater than one to intentionally propogate multicast packets to additional routers.

Figure 12-11 Protocol Stack Page (ICMP)

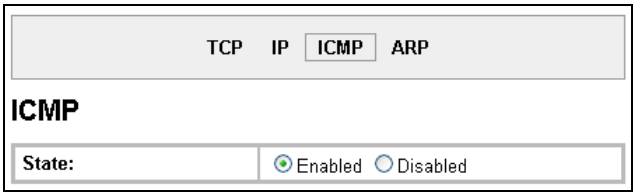


Table 12-9 ICMP Protocol Stack Page

Protocol Stack Page Settings	Description
ICMP	Internet Control Message Protocol (ICMP) can be used as an error-reporting protocol between two hosts. This setting specifies whether incoming and outgoing ICMP messages are processed. Choices are: **Enabled** = ICMP messages are processed. (default) **Disabled** = ICMP messages are not processed.

Figure 12-12 Protocol Stack Page (ARP)

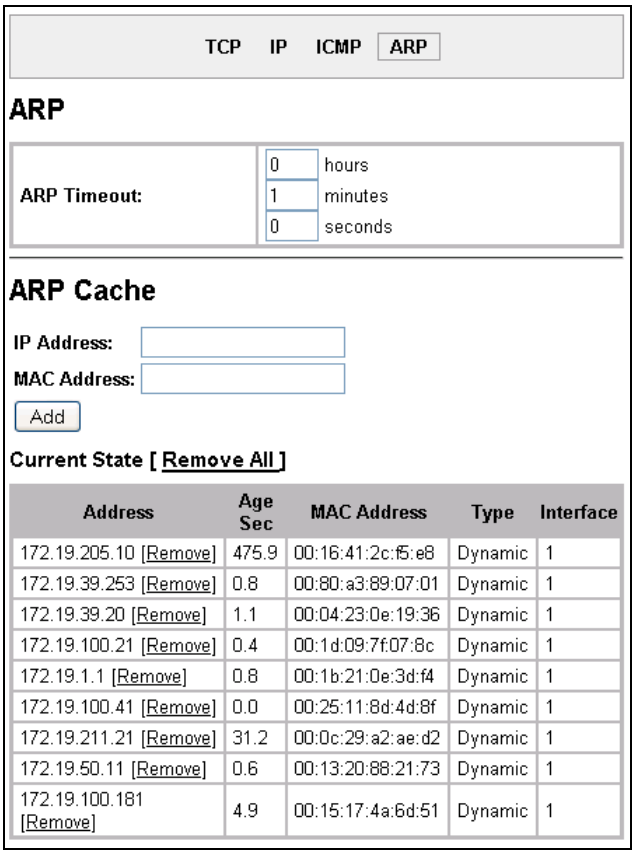


Table 12-10 ARP Protocol Stack Page

Protocol Stack Page Settings	Description
ARP Timeout	Enter the maximum number of hours, minutes and seconds that a MAC address will remain in cache before being removed. Default is 00:01:00. (one minute).
ARP Cache	
IP Address	Enter the IP address of the entry to be added to the Address Resolution Protocol (ARP) cache.
MAC Address	Enter the MAC address of the entry to be added to the ARP cache.

IP Address Filter Page

Clicking the **IP Address Filter** link in the menu bar displays the IP Address Filter page. Here you can specify the IP addresses and subnets allowed to send data to the IntelliBox. All packets sent from IP addresses not on this list are ignored and discarded. By default, the IP address list is empty, so all addresses are allowed.

The network mask and IP address settings you specify on this page determine the range of IP addresses that can access the IntelliBox. For example:

- An IP address of 10.0.0.0 and a network mask of 255.0.0.0 allow any device with an IP address in the 10.x.x.x range to access the IntelliBox.
- An IP address of 192.168.1.1 with a network mask of 255.0.0.0 causes the IntelliBox to allow all IP addresses in the range of 192.x.x.x.
- An IP address of 192.168.1.1 with a network mask of 255.255.255.0 only allows IP addresses in the range of 192.168.1.x to access the IntelliBox.

Figure 12-13 IP Address Filter Page

Table 12-11 IP Address Filter Page

IP Address Filter Page Settings	Description
IP Address	Enter the IP address that is allowed to send packets to the IntelliBox. If using DHCP with BOOTP, enter the IP address of the DHCP/BOOTP server.
Network Mask	Enter the network mask associated with the IP address that is allowed to send packets to the IntelliBox.

13: EventTrak Pages

The user can monitor different types of devices and respond to specified events that occur. The IntelliBox provides this capability through EventTrak™, its event monitoring firmware. Additionally, the IntelliBox provides automatic reporting and RSS feeds.

On the IntelliBox-I/O 2100, there is one EventTrak for each of the two serial lines. After you select an EventTrak, you can click **Status**, **Monitoring**, or **Control** to view and change the settings of the selected EventTrak.

Notes:

- For more explanation about the IntelliBox's ability to monitor and respond to events, see *3: EventTrak*.
- For detailed application examples, please go to the Lantronix web site (*www.lantronix.com*).

Clicking **Submit** applies changes immediately to the IntelliBox.

EventTrak – Status Page

The EventTrak Status page displays when you click **EventTrak** in the menu bar. It also displays when you click **Status** at the top of one of the other EventTrak pages. This read-only page shows the status of monitored events and actions for the EventTrak selected at the top of this page.

Figure 13-1 EventTrak Status Page

Table 13-1 EventTrak -- Status Page

EventTrak Status Page	Description
Task Description	Text identifying the task.
Current Step	Letter identifying the currently active step.
Step Name	Text identifying the step.
Duration	Length of time the IntelliBox has been performing the step.

EventTrak – Monitoring Page

EventTrak scans incoming data to trigger an event when the IntelliBox receives specific data. The user defines the data that triggers an event on the Monitoring page of each EventTrak. You can configure three match strings per EventTrak to enable EventTrak to run multiple tasks to monitor for different events

The EventTrak Monitoring page displays when you click **Monitoring** at the top of one of the other EventTrak pages. This page contains the configuration settings for match strings for the EventTrak selected at the top of this page.

At the top of the page, select **Match 1**, **Match 2**, or **Match 3** to display a Monitoring page for each match you want to configure.

Figure 13-2 EventTrak Monitoring Page

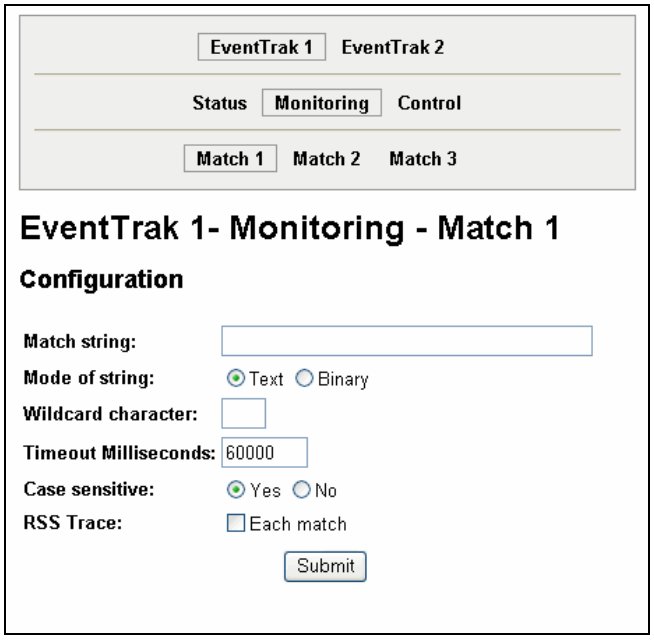


Table 13-2 EventTrak Monitoring Page

EventTrak Monitoring Page Settings	Description
Match string	EventTrak monitors activity on each line, comparing to the match string at all times. Enter the match string you want the IntelliBox to use to monitor the line. You can use text or binary format.

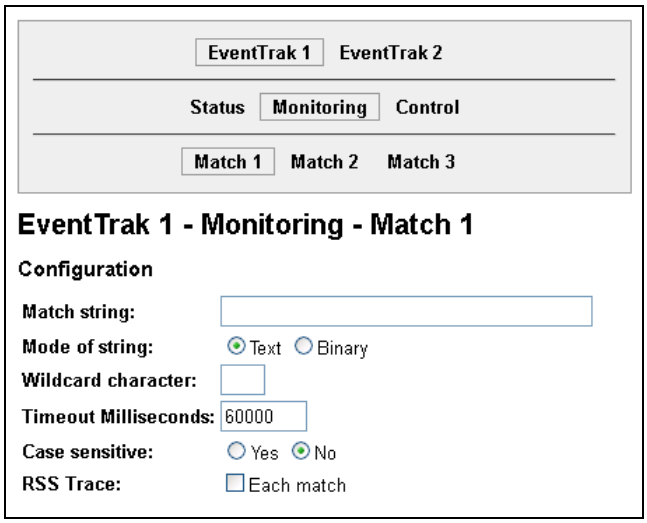
EventTrak Monitoring Page Settings	Description
Mode of string	Select the type of string entered in **Match string**. Choices are: **Text** = standard readable text. **Binary** = any combination of text, hexadecimal, decimal, or control characters. Allows square brackets [ ] to enclose one or more special character designations separated by spaces. Use straight decimal numbers up to 255, hexadecimal numbers prefixed with 0x up to 0xFF, or control characters prefixed by **^**. To specify an open bracket in binary mode, use two open brackets in a row ([[).
Wildcard character	Enter a character that will indicate any character is a match. For example, if you set a question mark as a wildcard and set your match string to **error???**, the word **error** and any three characters would trigger a match.
Timeout Milliseconds	Enter how long (in milliseconds) EventTrak will wait before clearing the buffer of partial matches.
Case sensitive	Select the option that indicates whether the match must be case sensitive.
RSS Trace	Select the checkbox to cause EventTrak to send information by means of RSS when it encounters a string match. This function is primarily for troubleshooting.

Match String Examples

Following are examples of how to set up the EventTrak Monitoring page for one or more match strings.

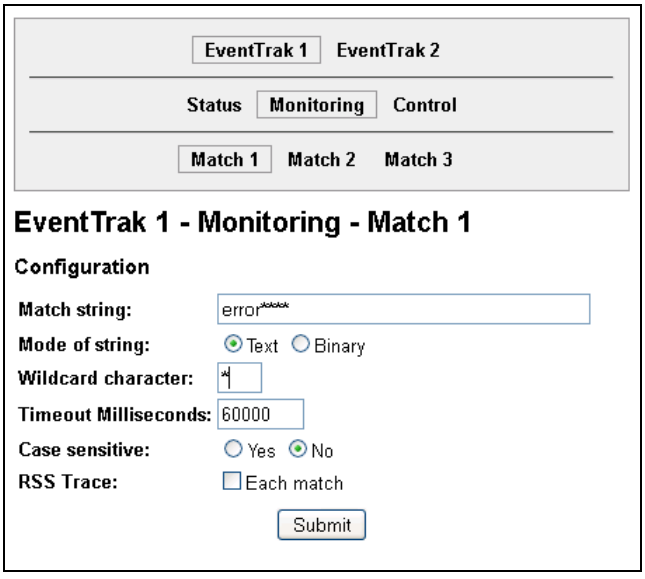
Match String Example 1 – Simple Text String

In this example of a simple text-based match string, EventTrak will monitor for any string that contains the term **error 123**. The timeout of 60000 milliseconds (60 seconds) means that if EventTrak finds the string **error**, it will wait 60 seconds for the remaining data to determine a match before discarding the partially matched data.



Match String Example 2 – Simple Text Strings with Wild Cards

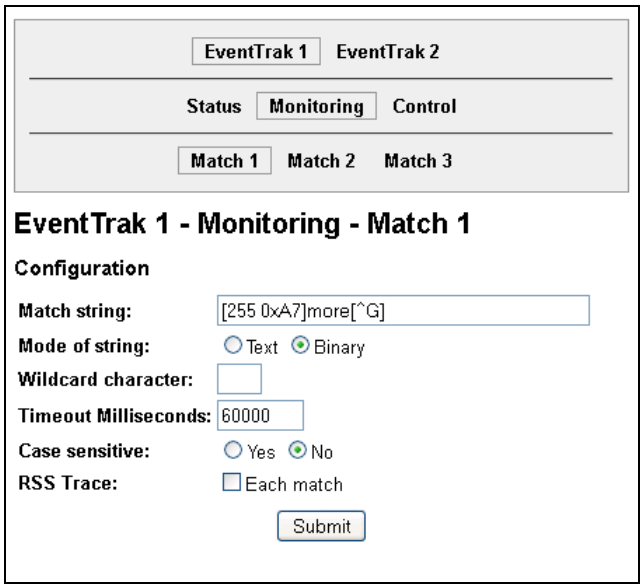
In this example, the match string is set to allow EventTrak to monitor for any string that contains the word **error** followed by any 4 characters. This is an example of a simple text-based match string with an asterisk as a wild card character.



Match String Example 3 – Mixing Text and Special Characters

In this example, the match string contains a combination of decimal, hexadecimal, text, and control characters. Users can configure EventTrak to monitor specific protocols that the attached device requires.

Note: ***Mode of string*** *must be* ***Binary*** *to support hexadecimal, decimal, and control characters.*



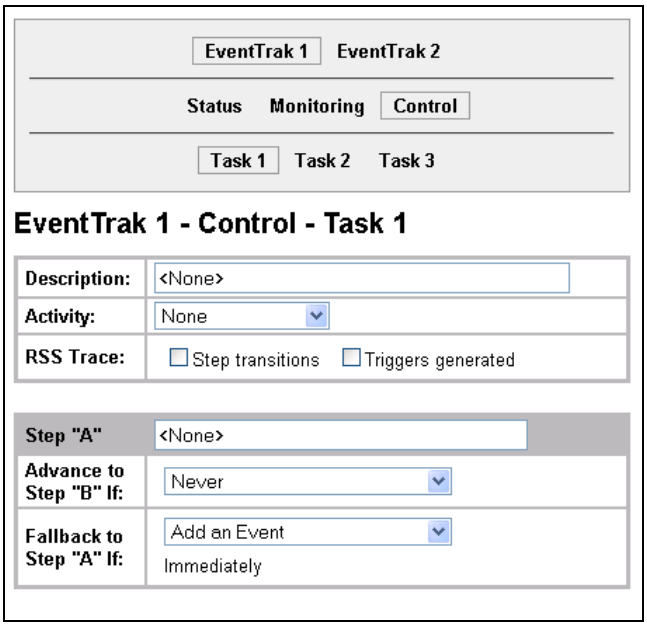
EventTrak – Control Page

The EventTrak Control page displays when you click **Control** at the top of one of the other EventTrak pages. Each EventTrak has three tasks. Each task can monitor for different events simultaneously. This page enables you to set up EventTrak to monitor and take action in response to events. Additionally, a detected event on one task can trigger an event on another task. Two triggers (Trigger A and Trigger B) are supported for sending and and receiving local triggers. This provides flexibility for configuring definitions of events and actions in response to a detected event. An externally triggered option is also available to trigger from one eventtrak to another.

The Task configuration page uses a dynamically changing interface. As you make changes, only applicable settings display. As a result, the IntelliBox interface remains easy to use while also allowing for highly advanced configurable event detection with multiple actions.

At the top of the page, select **Task 1**, **Task 2**, or **Task 3** to display a Control page for each task you want to configure.

Figure 12-3 EventTrak Control Page



Note: *To remove an action or an event with a checkbox, clear the checkbox. In other cases select* ***No action*** *or* ***Never****.*

Initial Settings

The first section on the Control page has three initial settings.

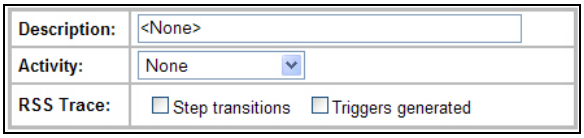


Table 13-3 EventTrak Control Settings

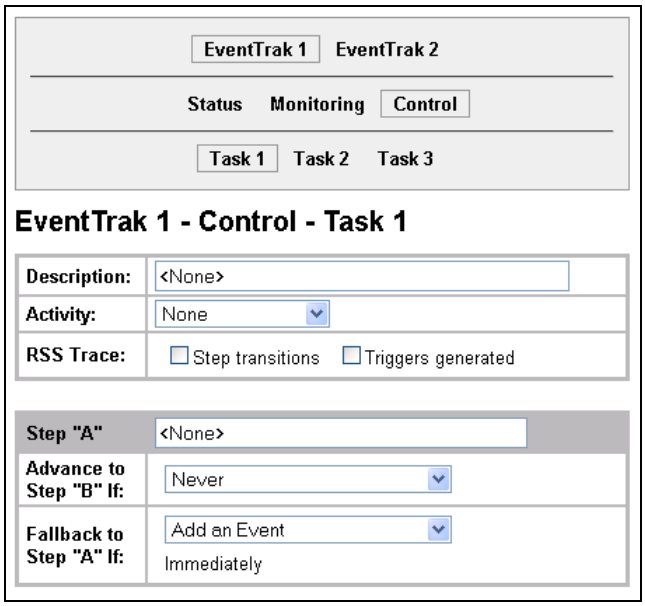
EventTrak Control Page Initial Settings	Description
Description	Enter the function of the initial activities. The default is **None**.
Activity	From the drop-down list, leave **None** or select an activity for the task to control. Choices are: **None** = no activity is assigned to the task (default). **Ping per second** = when selected, enter the IP address of the device you want to ping. **XIO1 & XIO2** = assigns an I/O to a task to be controlled. This option only displays if the digital I/O is set as an output. The **Output Control** options display (See description in this table.) **Relay** = assigns the relay to a task to be controlled. The **Output Control** options display. (See description in this table.)

EventTrak Control Page Initial Settings	Description
RSS Trace	Enables recording on RSS each time EventTrak takes a step or generates a trigger. Select one or more of the following criteria for initiating an RSS trace. This function is primarily for troubleshooting. Choices are: **Step transitions** = sends a trace whenever EventTrak moves forward or back from one step to another. **Triggers generated** = sends a trace whenever EventTrak generates a trigger for an event to take place. **Ping responses** = sends a trace whenever the IntelliBox successfully pings a device.
Output Control	If you selected XIO1, XIO2, or Relay, select an output control option in the field that displays. Choices are: **Exclusive** = Only one task can control the I/O pin or relay. **Logical-Or (shared):** = Multiple tasks can control the I/O pin or relay.

Step "A"

EventTrak consists of multiple steps that determine the events EventTrak will monitor and the actions it will take in response to them. A simple EventTrak configuration may only use one step, while a more complex configuration can use multiple steps in multiple tasks or even multiple EventTraks. The EventTrak user interface is dynamic; for example, Step “B” only displays if it can advance to it.

Each step consists of two to four configurable items, depending on the options selected. For example, if you select **Relay** as the initial activity, you must select the initial relay setting at the beginning of Step “A” as shown in the example below.



The additional settings are described below:

Table 13-4 EventTrak Control Step Settings

EventTrak Control Step A Settings	Description
Advance to Step "B" if	This setting defines the event that will cause EventTrak to move to the next step. When you use an option, the **Upon Advance** setting displays. ***Note:*** *In Step "B", this is entitled Advance to Step "C" if. In Step "C", this is entitled Advance to Step "D".* Choices are: **Never** = there is no event that advances to the next step. **Match String "x"** = tells EventTrak to monitor the serial port and advance if it detects a specific string. The choices are **Match String 1**, **Match String 2** or **Match String 3**. (See EventTrak – Monitoring Page for instructions on defining match strings.) **Line outputs data** = advances if data is sent out the serial port. **Tunnel accepts connection** = tells EventTrak to advance if the IntelliBox accepts a TCP connection to its serial port. **Tunnel accepts disconnection** = tells EventTrak to advance if a TCP connection to its serial port is disconnected. **Ping Response** = tells EventTrak to advance if the IntelliBox receives a ping response. This setting works in conjunction with the initial action of **Ping per second**. **Timeout expires** = tells EventTrak to wait a configurable amount of time before advancing. This is useful when you want to pause EventTrak to wait for an event or gather serial data for automated reporting. You can configure the timeout as milliseconds, seconds or minutes. The maximum length of a timeout is 10080 minutes (7 days). **Triggered by task "x"** = allows EventTrak to advance when another triggers it. **Externally triggered** = Allows EventTrak to advance when another task on another EventTrak triggers it.
Upon Advance	This setting tells EventTrak what actions to take when a detected event causes EventTrak to move to the next step. ***Note:*** *Upon Advance happens at the same time as moving to the next step.* The **Upon Advance** box displays when you select **Advance to step "x"**. ***Note:*** *You can add multiple actions.* Choices are: **Send Email** = tells EventTrak to send an email when it detects an event. When you select an option, the following additional configurable items display: ◆ **No Email** removes **Send email** as an action in response

EventTrak Control Step A Settings	Description

to an event.

- **Email 1, 2, 3 or 4** are the email profiles configured on the Email page.
- **Email with buffered serial data 1, 2, 3 or 4** are the emails configured on the Email page along with the data in the serial buffer.
- **Subject line** can be changed from the configured email to be sent when this event happens.

Send on line= sends data out the serial port. When selected, the following additional configurable items display:

- **No Send** removes **Send on line** as an action in response to an event
- **Send text** adds a text box in which you can add a string.
- **Send binary** allows you to combine text, hexadecimal, and decimal characters.

  Use square brackets [ ] to enclose one or more special character designations separated by spaces. Use straight decimal numbers up to 255, hexadecimal numbers prefixed with 0x up to 0xFF, or control characters prefixed by **^**. For example, the string **test[255 0xFF ^Q** would send the word **test** followed be the additional special characters.
- **Send file** sends a file from the IntelliBox file system out the serial port. For example, a file named **example.txt** located in root directory of the file system would be typed as **/example.txt**. If the file is in a directory called **hold,** it would be entered as **/hold/example.txt.** You can add a file to the file system or a directory created on the file system using FTP or the Filesystem web page on the IntelliBox.

Send RSS = posts data by means of an RSS feed.

Note: *RSS must be enabled on the RSS page.*

If selected, the following additional configurable items display:

- **No RSS** removes the **Send RSS** option as an action in response to an event.
- **RSS** enables you to define a string to send by means of RSS.
- **RSS Rx buffer in body** enables you to define a string to send by RSS along with data in the serial buffer.
- **Title**

Clear receive buffer = clears all buffered data received on the serial port. Selecting this option causes a **Clear receive buffer** checkbox to display. Clearing the checkbox removes **Clear receive buffer** option as an action in response to an event.

Fire Trigger = fires a trigger on another task. When selected, the following additional configurable items display. Choices are:

- **No Trigger** removes the **Fire Trigger** option as an action

EventTrak Control Step A Settings	Description
	in response to an event. ◆ **Trigger task x** triggers an event on another task in the same EventTrak. ◆ **Trigger EventTrak x Task 1** triggers an event on Task 1 in a different EventTrak (e.g., serial line 1 EventTrak can trigger an event on serial line 2 EventTrak).
Fallback to Step "A" if	From the **Add an Event** drop-down list, select one or more events that will trigger EventTrak to fall back (return) to Step "A," the beginning of the task. When you select an option, **Upon Fallback** displays. ***Note:*** *You can select more than one event to trigger a fallback to step "A," but you must open the drop-down list and select one at a time.* **Timeout expires** = tells EventTrak to wait a configurable amount of time before falling back. This is useful when you want to pause EventTrak to wait for an event or gather serial data for automated reporting. Select to configure as milliseconds, seconds or minutes. The maximum length of a timeout is 7 days (10080 minutes) **Line outputs data** =falls back if data is sent out the serial port **Tunnel accepts connection** = tells EventTrak to fall back if the IntelliBox accepts a TCP connection to its serial port **Tunnel accepts disconnection** = tells EventTrak to fall back event if a TCP connection to the IntelliBox's serial port is disconnected **Ping Response** = tells EventTrak to fall back if it receives a ping response. Use this option in conjunction with the initial action of **Send a ping**. **Match String "x"** = tells EventTrak to monitor the serial port and fall back if it detects a specific string. The choices are **Match String 1**, **Match String 2** or **Match String 3.** (See *EventTrak – Monitoring Page* for instructions on defining match strings.) **Triggered by task "x"** = enables EventTrak to fall back when another task instructs it to continue.
Upon Fallback	From the drop-down list, select the action EventTrak should take when the IntelliBox detects an event that will cause EventTrak to fall back to Step "A". The **Upon Fallback** box displays when you configure **Fallback to Step "A"**. Choices are: **No Trigger** = no trigger is fired upon fallback to Step "A" **Fire Trigger to Task x** =t ells EventTrak to trigger an event on another task. For example, you can set **Upon Fallback** on Task 1 to trigger an event on Task 2. Task 2 can be triggered by setting its **Advance to** or **Fallback to** configurable to **Triggered by task 1**.

Note: *For examples of using EventTrak for event monitoring and automated reporting, please go to http://www.lantronix.com/support.*

14: Updating Firmware

Lantronix periodically releases updates to the firmware to fix problems or provide feature upgrades.

Obtaining Firmware

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

Upgrading Using DeviceInstaller

Loading New Firmware

1. Download the latest firmware and release notes for IntelliBox-I/O 2100 from the Lantronix web site http://www.lantronix.com/support/downloads.html.
2. Unzip the files and save them to a directory on your PC

Updating Firmware

1. Open DeviceInstaller. (See *Starting DeviceInstaller* .)
2. Open the IntelliBox-I/O 2100 folder in the left Window pane.
3. Select the IntelliBox-I/O 2100 that you would like to upgrade.
4. Click the **Web Configuration** tab and click **Go**.
5. Enter the **User name** and **Password**. The default user name is **admin** with a default password of **PASS** (all caps).
6. On the menu bar, click **System**. The System page displays.
3. Under **Upload New Firmware**, click **Browse** and navigate to the directory where you saved the IntelliBox-I/O 2100 firmware.
4. Select the IntelliBox-I/O firmware file, e.g. **IntelliBox-io_1_4_0_0_R2.romz** and click **Upload**.

A: Factory Default Configuration

This appendix lists the IntelliBox factory-default configuration. The types of settings are in alphabetical order.

CLI Settings

Table A-1 CLI Telnet Settings

CLI Telnet Parameters	CLI Telnet Settings
Telnet Access	Enabled
Telnet Port	23
SSH Access	Enabled
SSH Port	22
Password	<None>
Enable Password	<None>
Quit Connect Line	<control>L

Diagnostics Settings

Table A-2 Diagnostic Ping Settings

Diagnostics Ping Parameters	Diagnostic Ping Settings
Count	3
Timeout	5 seconds

Email Settings

Table A-3 Email Settings

Email Parameters	Email Settings
To	<None>
Cc	<None>
From	<None>
Reply –To	<None>
Subject	<None>
File	<None>
Overriding Domain	<None>
Server Port	25
Local Port or Random	Random
Priority	Normal
Trigger Email Send	Disabled

EventTrak Settings

Table A-4 Monitoring Settings

EventTrak Monitoring Parameters	*EventTrak Monitoring Settings*
Match String	*<None>*
Mode of string	*Text*
Wildcard character	*<None>*
Timeout Milliseconds	*60000*
Case sensitive	*No*
RSS Trace	*<None>*

Table A-5 Control – Task Settings

EventTrak Control Parameters	EventTrak Control Settings
Task Description	<None>
Activity	<None>
RSS Trace	<None>

FTP Settings

Table A-6 FTP Settings

FTP Parameters	FTP Settings
FTP Server	On
Username	admin
Password	PASS

HTTP Settings

Table A-7 HTTP Settings

HTTP Configuration Parameters	HTTP Settings
HTTP Server	On
HTTP Port	80
HTTPS Port	443
Max Timeout	10 seconds
Max Bytes	40960
Logging	On
Max Log Entries	50
Log Format	%h %t "%r" %s %B "%{Referer}i" "%{User-Agent}i"

Table A-8 HTTP Authentication Settings

HTTP Authentication Parameters	HTTP Authentication Settings
URI	/
Realm	config
AuthType	Digest
Username	admin
Password	PASS

Input/Output Settings

Table A-9 Input/Output Settings

Input/Output Parameters	Input/Output Settings
XIO1	Output
XIO1	Output
Relay	Output

IP Address Filter Settings

Table A-10 IP Address Settings

IP Address Parameters	IP Address Settings
IP Address	<None>
Network Mask	<None>

Modbus Settings

Table A-11 Modbus Settings

Modbus Parameters	Modbus Settings
TCP Server Access	Enabled

Modbus Parameters	Modbus Settings
TCP Server Port	502 (not changeable)
Additional TCP Server Port	*<None>*

Network Configuration Settings

Table A-12 Network Configuration Settings

Network Configuration Parameters	Network Configuration Settings
BOOTP Client	Off (disabled)
DHCP Client	On (enabled)
IP Address	0.0.0.0 (auto-IP if DHCP fails)
Network Mask	0.0.0.0 (auto if DHCP fails)
Gateway	0.0.0.0
MAC Address	Specified by manufacturer
Hostname	<None>
Domain	<None>
DHCP Client ID	<None>
Ethernet lINK	Auto speed, auto duplex

Query Port Settings

Table A-13 Query Port Settings

Query Port Parameters	Query Port Settings
Query Port Server	On

RSS Settings

Table A-14 RSS Settings

RSS Parameters	RSS Settings
RSS Feed	Off
Persistent	Off
Max Entries	100

Serial Port Line Settings

Table A-15 Configuration Settings

Configuration

Serial Port Line Parameters	Configuration Settings
Name	<None>
Status	Enabled
Protocol	Tunnel
Interface	Disabled
Termination	Disabled
Baud Rate	9600 baud
Parity	<None>
Data Bits	8
Stop Bits	1
Flow Control	<None>
Xon char	0x11 (\17)
Xoff char	0x13 (\19)

Command Mode

Table A-16 Command Mode Settings

Serial Port Line Parameters	Command Mode Settings
Command Mode	Disabled
Use Serial String	Off (disabled)
Echo Serial String	On (enabled)
Wait Time (milliseconds)	5000 milliseconds
Serial String (text or binary)	<None>
Signon Message	<None>

SNMP Settings

Table A-17 SNMP Settings

SNMP Parameters	SNMP Settings
SNMP Agent	Running
Read Community	Public
Write Community	Private
System Contact	<None>
System Name	ibio2100
System Description	Lantronix IntelliBox-I/O 2100
System Location	<None>
Enable Traps	On
Primary TrapDest IP	<None>
Secondary TrapDest IP	<None>

Syslog Settings

Table A-18 Syslog Settings

Syslog Parameters	Syslog Settings
Syslog Status	Off
Host	<None>
Local Port	514
Remote Port	514
Severity to Log	<None>

System Settings

Table A-19 System Settings

System Parameters	System Settings
System Name	ibio2100
System Description	Lantronix IntelliBox-I/O 2100

TFTP Settings

Table A-20 TFTP Settings

TFTP Parameters	TFTP Settings
TFTP Server	On
Allow TFTP File Creation	Disabled

Tunnel Settings

Serial Settings

Table A-21 Serial Settings

Serial Parameters	Serial Settings
Buffer Size	2048 bytes
Read Timeout (milliseconds)	200 milliseconds
Wait for Read Timeout	Disabled

Start/Stop Characters

Table A-22 Start/Stop Character Settings

Start/Stop Character Parameters	Start/Stop Character Settings
Start Character	<None>
Stop Character	<None>
Echo Start Character	Off
Echo Stop Character	Off

Accept Mode

Table A-23 Accept Mode Settings

Accept Mode Parameters	Accept Mode Settings
Accept Mode	Enabled
Local Port	Port 1 = 10001, Port 2 = 10002
Protocol	TCP
Flush Serial Data	Disabled
Block Serial Data	Off
Block Network Data	Off
TCP Keep Alive	45 seconds
Email on Connect	<None>

Accept Mode Parameters	Accept Mode Settings
Email on Disconnect	<None>
RSS Trace Connections	Disabled
Output Selection	<None>
Control	Exclusive
Password	<None>
Prompt for Password	Off

Connect Mode

Table A-24 Connect Mode Settings

Connect Mode Parameters	Connect Mode Settings
Connect Mode	Disabled
Remote Address	<None>
Remote Port	<None>
Local Port	Random
Protocol	TCP
Reconnect Timer	15000 milliseconds
Flush Serial Data	Disabled
SSH Username	<None>
Block Serial Data	Off
Block Network Data	Off
TCP Keep Alive	45 seconds
Email on Connect	<None>
Email on Disconnect	<None>
Output Selection	<None>
Control	Exclusive

Disconnect Mode

Table A-25 Disconnect Mode Settings

Disconnect Mode Parameters	Disconnect Mode Settings
Mode	Disabled
Timeout	60000 milliseconds
Flush Serial Data	Disabled

Packing Mode

Table A-26 Packing Mode Settings

Packing Mode Parameters	Packing Mode Settings
Mode	Disabled
Timeout	1000 milliseconds
Threshold	512 bytes
Send Character	<None>
Trailing Character	<None>

Modem Emulation

Table A-27 Modem Emulation Settings

Modem Emulation Parameters	Modem Emulation Settings
Echo Pluses	Off
Echo Commands	On
Verbose Response Codes	On
Response Codes	Text
Error Unknown Commands	Off
Optional Connect String	<None>

AES Keys

Table A-28 AES Key Settings

AES Key Parameters	AES Key Settings
Accept Mode AES Keys: Encrypt Key	<None>
Accept Mode AES Keys: Decrypt Key	<None>
Connect Mode AES Keys: Encrypt Key	<None>
Connect Mode AES Keys: Decrypt Key	<None>

B: Networking and Security

This chapter describes the following networking and security concepts as they relate to the IntelliBox:

SSL

Secure Sockets Layer (SSL) is an open-standard security protocol that provides privacy through encryption, server authentication, and message integrity. From its introduction in 1994, SSL has become the industry standard for securing e-commerce transactions over TCP/IP connections. And it is easy to see why.

Imagine mailing a letter in a clear envelope that anyone could see. If the envelope contained a check, credit card, or other valuable information, some nefarious individual could steal the letter or change its contents. Information traveling over networks, including the Internet, is just as vulnerable.

Prior to SSL, packets of information would travel networks in full view of anyone who could access the data. As the World Wide Web grew and gained in popularity, a solution became necessary for securing e-commerce transactions over the Internet. The solution would have to enable Internet consumers to reliably identify the Internet vendors (e-commerce servers) with whom they transact business while, at the same time, protect the confidentiality of the consumers' sensitive information as it traversed the Internet. With the advent of SSL, personal information that anyone with view access could see could now be secure.

Benefits of SSL

The following list summarizes the benefits of SSL:

- Widely implemented standard for e-commerce applications
- Reduces the complexities associated with keeping user information confidential
- Works with existing web servers and browsers
- Eliminates the need for additional software applications
- Provides high level of security
- Platform and O/S neutral
- Allows server authentication via certificates

How SSL Works

SSL uses cryptography to deliver authentication and privacy to message transmission over the Internet. SSL permits the communication of client/server applications without eavesdropping and message tampering.

SSL runs on layers between application protocols (HTTP, SMTP, etc.) and the TCP transport protocol. To set up an SSL connection, establish a TCP/IP connection first. The SSL connection sets up a secure channel within the TCP/IP connection in which all traffic between the client and server is encrypted. All the calls from the application layer to the TCP layer are replaced with calls to the SSL layer, with the SSL layer handling communication with the TCP layer.

SSL is most commonly used with HTTP (thus forming HTTPS). Web sites protected by SSL start with a URL that begins with “https” and displays a padlock icon at the bottom of the page (and for Mozilla Firefox in the address bar as well).

When a web browser accesses a domain secured by SSL, an SSL handshake authenticates the server and client, and establishes an encryption method and a unique session key. Once this handshake has been completed, the client and server can begin a secure session that guarantees message privacy and message integrity.

SSL uses Digital-Certificate technology to identify target servers reliably and uses encryption to protect the confidentiality of information passing between client and server. You can configure the IntelliBox to use an SSL certificate for the HTTP server. The certificate can be created elsewhere and uploaded to the IntelliBox, or it can be automatically generated as a self-signed certificate on the IntelliBox. For more information about uploading a new certificate or create a new self-signed certificate, see *SSL*.

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

The following steps summarize how SSL works:

1. A client contacts a server secured by SSL.
2. In response to the client request, the server sends its certificate to the client.
3. The client generates a master key, which it encrypts with the server's public key and transmits the encrypted master key back to the server.
4. The server recovers the master key and authenticates itself to the client by returning a message authenticated with the master key. Subsequent data is encrypted and authenticated with keys derived from this master key.

Digital Certificates

Authentication with SSL is achieved with a Digital Certificate issued and signed by a Certificate Authority (CA) and stored on the server. Without a certificate signed by a CA, the server cannot be reliably identified to the client, yet a connection can still proceed if allowed.

The Digital Certificate resides on a secure server and is used to encrypt data and identify the web site. The Digital Certificate verifies that a site belongs to who it claims to belong to and contains information about the certificate holder, the domain that the certificate was issued to, the name of the Certificate Authority who issued the certificate, the root and the country it was issued in. In addition to proving the veracity of a site, the Digital

Certificate provides the receiver with a way to encode a reply. Digital Certificates come in 40-bit and 128-bit versions.

There are two principal ways to obtain a Digital Certificate. It can be bought from a certificate vendor or a user can "self-sign" his or her own certificate. With the latter method, a user can use various tools, both open source and proprietary, to sign his or her own Digital Certificate, saving the time and expense of going through a certificate vendor.

SSH

Like SSL, Secure Shell (SSH) is a protocol that provides secure encrypted communications over unsecured TCP/IP networks such as the Internet. SSH allows for secure access to remote systems, eliminating potential security breaches such as spoofing and eavesdropping or hijacking of sessions. However, SSH differs significantly from SSL and, in fact, cannot communicate with SSL. The two are different protocols, though they have some overlap in how they accomplish similar goals.

How Does SSH Authenticate?

SSH authenticates using one or more of the following:

- Password (the /etc/passwd or /etc/shadow in UNIX)
- User public key (RSA or DSA, depending on the release)
- Host based (.rhosts or /etc/hosts.equiv in SSH1 or public key in SSH2)

What Does SSH Protect Against?

SSH provides strong authentication and secure communications over insecure channels. It also provides secure connections that protect a network from attacks such as:

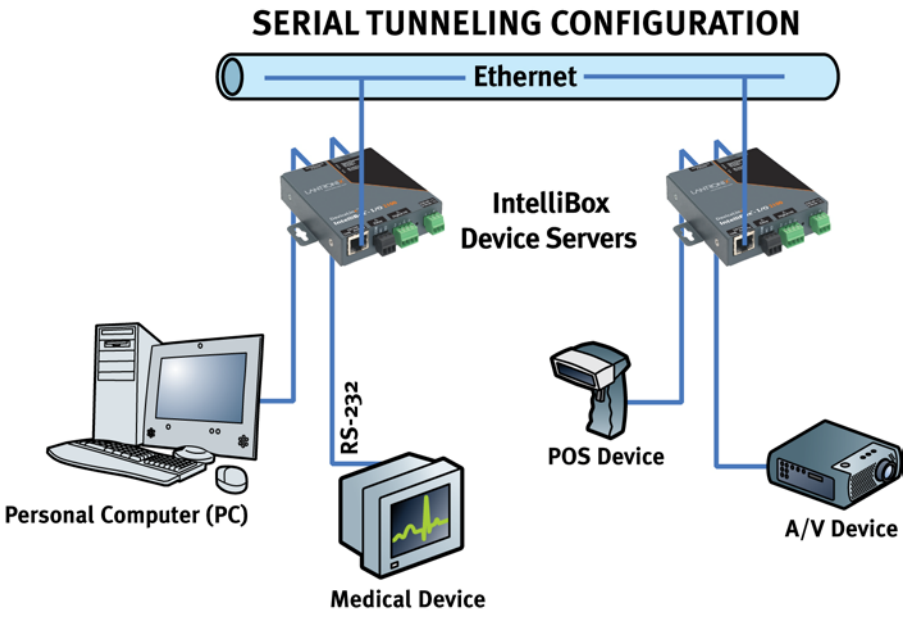
- IP spoofing, where a remote host sends packets that pretend to originate from another, trusted host. SSH even protects against a spoofer on the local network that is pretending to be a router to the outside.
- IP source routing, where a host pretends that an IP packet comes from another, trusted host.
- DNS spoofing, where an attacker forges name server records.
- Interception of cleartext passwords and other data by intermediate hosts.
- Manipulation of data by people in control of intermediate hosts.
- Attacks based on listening to authentication data and spoofed connections to the server.

Tunneling

Tunneling provides a way to create a connection between two serial devices across an untrusted network so the devices can share data. The sharing of information is achieved through a direct connection (or “serial tunnel”) between the two devices that encapsulates, authenticates, and encrypts the serial data into TCP packets and sends them across the Ethernet network. In this way, two previously isolated and non-networked devices can securely and effectively communicate and exchange information and operate with existing installed software applications or devices that are configured to run independently of an Ethernet network. And because the tunnel can be secure, anyone who tries to monitor the conversation between the two devices would see encrypted, unintelligible data.

The figure below shows how to use a pair of device servers in tandem to provide transparent serial tunneling across an Ethernet network. In this example, a POS device in a store collects data and sends it to a device server attached to a POS serial port. The device server forwards the collected data, through an encrypted tunnel established over the Ethernet network, to a device server connected to a remote PC. The data received at the remote device server is decrypted and forwarded to the PC’s serial port and received at the remote PC. In this way, serial data that goes in one end comes out at the other end.

Figure B-1 Example of an Encrypted Tunnel



Tunneling and the IntelliBox

Each IntelliBox serial port supports two concurrent tunneling connections, Connect Mode and Accept Mode . These connections operate independently of the other IntelliBox serial ports.

- In Connect Mode, the IntelliBox actively makes a connection. The receiving node on the network must listen for the Connect Mode's connection. By default, Connect Mode is disabled.
- In Accept Mode, the IntelliBox listens for a connection. A node on the network initiates the connection. By default, Accept Mode is enabled.
- Disconnect Mode defines how an active connection is disconnected. The parameters used to drop the connection are user-configurable. The IntelliBox's Disconnect Mode disconnects both Accept Mode and Connect Mode connections on a serial port when it observes the defined event occur on that port.

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

Connect Mode

For Connect Mode to work:

- Connect Mode must be enabled on the IntelliBox .
- A remote station (node) must be configured for Connect Mode.
- A remote TCP or UDP port must be configured.

When Connect Mode is enabled, it remains on until it is ended by Disconnect Mode.

Connect Mode supports the following protocols:

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

For AES encryption, both the encrypt key and the decrypt key must be specified. The encrypt key is used with data sent from the IntelliBox, while the decrypt key is used when the IntelliBox receives data. Both keys can have the same value.

If the remote address or port is not configured and Connect Mode is set to UDP, the IntelliBox accepts packets from any device on the network and sends packets to the last device that sent it packets. To ensure the IntelliBox does not accept UDP packets from all devices on the network, you must configure the remote address and port. When the remote port and station are configured, the IntelliBox ignores data from other sources.

To configure SSH, you must configure the SSH client username. In Connect Mode, the IntelliBox is the SSH client. Ensure the IntelliBox SSH client username is configured on the SSH server before using it with the IntelliBox.

Connect Mode has six variations:

- Disabled (no connection)
- Enabled (always makes a connection)
- Active if it sees any character from the serial port (makes a connection upon receiving any character)
- Active if it sees a specific (configurable) character from the serial port
- Modem emulation (controlled by modem commands)
- Modem control asserted (makes a connection when the modem central signal on the serial line becomes active)

For the “any character” or “specific character” connection states, the IntelliBox waits and retries the connection if the connection cannot be made. Once it makes a connection and then disconnects, it does not reconnect until it sees any character or the start character again (depending on the configured setting).

Accept Mode

In Accept Mode, the IntelliBox 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 (IntelliBox is the server in Accept Mode). For this protocol, the SSH server host keys and at least one SSH authorized user must be configured.
- TCP
- AES encryption over TCP

Accept Mode has the following options:

- 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 (when the modem control on the serial line corresponding to the tunnel becomes active)

Disconnect Mode

Disconnect Mode ends Accept Mode and Connect Mode connections. When disconnecting, the IntelliBox-I/O 2100 shuts down connections gracefully. Tunnel Disconnect Mode allows multiple simultaneous options.

The following three settings end a connection:

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

To clear out data from the serial buffers upon disconnecting, configure the IntelliBox to flush serial data.

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.

Note: *Packing control does not work when the line is configured for Modbus ASCII, or RTU.*

The following settings are configurable for Packing Mode:

- Enable or disable Packing Mode
- Packing Mode timeout. Data that is packed for a specified period before being sent out.
- Packing Mode threshold. When the buffer fills to a specified amount of data and the timeout has not elapsed, the IntelliBox packs the data and sends it out.
- Send character. Similar to a start or stop character, the IntelliBox packs data until it sees the send character. When it sees the send character, the IntelliBox sends the packed data and the send character in the packet.
- 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 IntelliBox supports Modem Emulation Mode for devices that transmit modem AT commands. The IntelliBox supports two different modes:

- **Command Mode:** The IntelliBox serial ports accept modem commands that instruct the IntelliBox to perform an action such as start or drop a connection.
- **Data Mode:** Serial data received in the IntelliBox serial port is sent through the active network connection.

The Tunnel – Modem Emulation page lets you configure modem emulation settings for two tunnels. Each tunnel can have different settings.

Note: *When the IntelliBox serial port is in Modem Emulation Mode, the serial port remains in Command Mode until an active tunnel starts. Once an active tunnel*

starts, the serial port remains in Data Mode until the connection is dropped or the serial port is placed in Command Mode by issuing the modem command +++.

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.
ATO	Switches to data mode if connection still exists. Vice versa to '+++'.
ATEn	Switches echo in command mode (off – n = 0, on –n = 1).
ATH	Disconnects the network session.
ATI	Displays modem information.
ATS0 = n	Accepts incoming connection. (n = 0: disable, n = 1: connect automatically, n = 2+: connect with ATA command (basically wait for the user or application to issue a command to "pick up the phone")
ATQn	Quiet mode (0 - enable results code, 1 - disable result codes)
ATVn	Verbose mode (0 - numeric result codes, 1 - text result codes)
ATZ	Restores the current state from the setup settings.
A/	Repeats last valid command.

These commands allow the IntelliBox to emulate a modem. The IntelliBox ignores valid AT commands that do not apply to the IntelliBox and sends an OK response code.

In Command Mode, the IntelliBox can make a connection to the remote host using the remote address and remote port information specified on the Tunnel – Connect Mode page.

When making a connection from the IntelliBox using an ATDT or ATDP command, full or partial IP addresses can be used. If a partial IP address is used, the IntelliBox uses the remote address and port as configured in the Connect Mode settings.

For the following examples, we assume that the remote address is 192.168.16.10 and the port is set to 10001 in the Connect Mode settings:

- Entering **ATDT** alone causes the IntelliBox to connect to the IP address and remote port configured in Connect Mode.

- Entering **ATDT 119.25.50** causes the IntelliBox to assume the first octet in the IP address and connects to the remote IP address 192.119.25.50, port 10001. (Since the remote port was not specified in the **ATDT** command, the remote port defined under Connect Mode is used.)
- Entering **ATDT 28.150** causes the IntelliBox to assume the first two octets in the IP address and connects to the remote IP address 192.168.28.150, port 10001.
- Entering **ATDT 150** causes the IntelliBox to assume the first three octets and connects to the remote IP address 192.168.16.150, port 10001.
- Entering **ATDT 28.150:10012** causes the IntelliBox to assume the first two octets in the IP address and connects to the remote IP address 192.168.28.150, port 10012.

Note: *If you add 10012 after the IP address segment, port 10012 is used instead of the port defined in Connect Mode.*

By default, the +++ characters are not passed through the connection. To pass them through the connection, enable Echo Pluses on the Tunnel - Modem Emulation page.

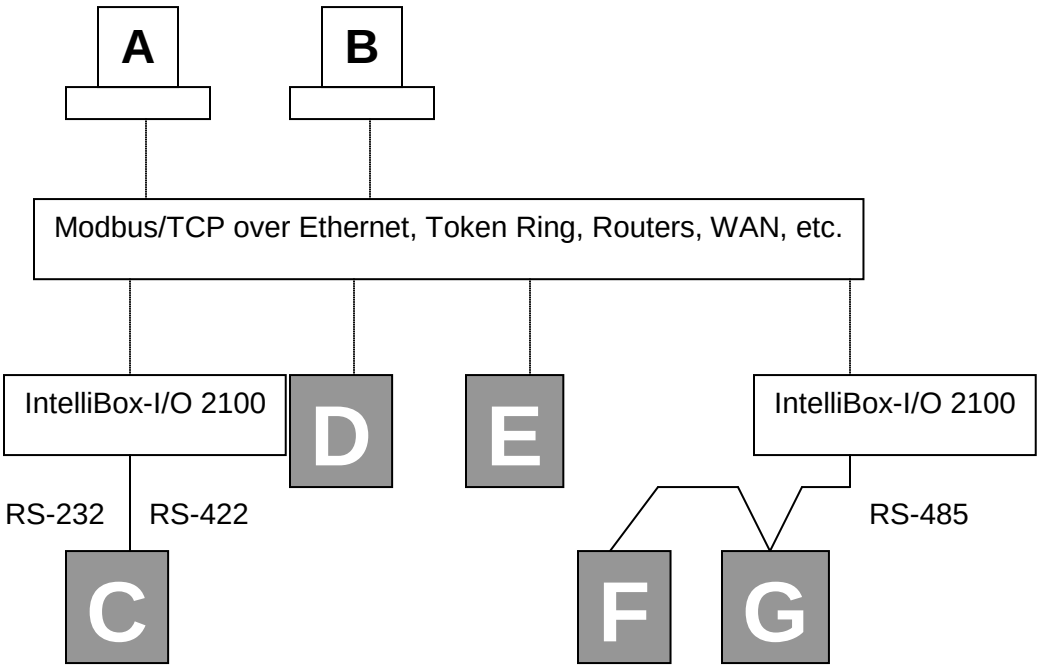
C: Modbus

Overview

When it comes to planning data communication for open, multi-vendor industrial control systems, Modbus is the first choice of end users and integrators alike. The Modbus/RTU protocol defines how a master device polls one or more slave devices to read and write data in real time by means of RS232, RS422, or RS485 serial data communication. Although not the most powerful protocol available, its rare simplicity allows not only rapid implementation but also enough flexibility to apply in virtually all industrial situations. Modbus/TCP, an extension of Modbus/RTU, defines how Modbus/RTU and Modbus/ASCII encode and transport messages over TCP/IP-based networks. Modbus/TCP is just as simple to implement and as flexible to apply as the original Modbus/RTU. You can find the specifications for both online at www.Modbus.org.

The IntelliBox enables users to integrate new and existing Modbus/RTU and Modbus/ASCII serial devices with newer TCP/IP network-based devices. This appendix describes a system that integrates three Modbus/RTU slave devices with four Modbus/TCP devices.

Table C-1 Extended Modbus System Example



The figure above shows various specific styles of Modbus operations. Traditionally, Modbus/RTU devices fall into two groups:

Modbus slave devices: These are generally the workhorse devices. They perform their tasks 24 hours a day, 365 days a year. Flow metering, temperature control, batch loading, and running entire automated assembly lines are examples of such tasks. The slave devices are called slaves because as far as data communications is concerned, they function as passive servers. Modbus slave devices passively sit and wait for a remote Modbus master device to ask them to report existing data values (read) or accept new data values (write).

Modbus master devices: These are generally higher-level computers, devices in which data and software are very important. The most common examples of Modbus master devices are the “Human-Machine-Interface” (HMI) computers, which allow human operators to monitor, adjust, and maintain the operations of field devices. Modbus master devices are clients that actively go out and read from and/or write to remote Modbus slave devices to monitor or adjust slave behavior. The IntelliBox does not support Master devices connected to the serial ports, unless the Masters are being polled like a slave device.

Examples

Modbus/TCP Master Talking to Modbus/TCP Slave

Devices A, B, D, and E are new Modbus/TCP devices, which are improved over Modbus/RTU (see more about Modbus/RTU limitations below). All four devices can function concurrently as both Modbus master and Modbus slave. Both computers A and B can treat controller D as a slave, polling data in real time. Yet controller D can also act as a master and poll data from controller E, which can in turn also act as a master to write alarm data directly up to computers A and B to alert the operators to the alarm condition. Traditional Modbus/RTU requires slave devices, even with severe alarm conditions, to sit patiently and wait for a remote master to poll the specific data that caused the alarm condition.

It is revolutionary for such a simple and flexible protocol as Modbus to offer such functionality. Therefore, Modbus/TCP offers exciting new design options for industrial users, which the IntelliBox-I/O extends to traditional Modbus/RTU serial devices.

Modbus/TCP Master Talking to Modbus/RTU Serial Slave

Devices C, F, and G are traditional Modbus/RTU slave devices. Device C uses a point-to-point electrical interface like RS232. This allows only a single Modbus/RTU master to talk to device C. However, the IntelliBox makes device C appear on the Modbus/TCP network as a full Modbus/TCP slave device. All Modbus/TCP enabled devices, A, B, D, and E, can actively share access to slave device C. A limitation in traditional Modbus/RTU implementation expects devices to be dedicated as either master or slave devices, so device C can only act as a Modbus slave.

Devices F and G are different from device C. They share a single RS485 multi-drop line that strictly limits them to act as slaves to a single Modbus/RTU master. However, all Modbus/TCP enabled devices A, B, D, and E can actively share access to both slave devices F and G. IntelliBox manages and coordinates the shared access. In fact, the IntelliBox allows up to sixteen concurrent Modbus masters (or thirty-two if an additional TCP Server is also used) to share access to the slaves.

Local Slave

The IntelliBox itself hosts a local Modbus slave role. This local slave is addressable from Modbus/TCP at Unit Identifier 255 (0xFF).The local slave provides access to the relay and digital I/Os as a single data block:

Address	Name	I/O
0	XIO1	User configurable as input or output
1	XIO2	User configurable as input or output
2	Relay	Output

The server treats broadcast (Unit Identifier 0) as a request to forward to the Modbus serial port, but does not attempt to apply the function locally.

The local slave supports the following Modbus functions:

Number	Name
1	Read Coils
2	Read Discrete Inputs
3	Read Holding Registers
4	Read Input Registers
5	Write Single Coil
6	Write Single Register
15	Write Multiple Coils
16	Write Multiple Registers
23	Read/Write Multiple Registers
43/14	Read Device Identification (Basic)

Note: *Any attempt to write to an XIO that the user has configured as an input returns exception 4 (**slave device failure**).*

D: Technical Specifications

Table D-1 Technical Specifications

Category	IntelliBox-I/O 2100 Specifications
CPU	Lantronix's DSTni-EX controller with 256 KB SRAM, 16 KB of boot ROM, and an integrated AMD 10/100B Ethernet PHY
Flash	4 MB Flash
RAM	2 MB SRAM
EEPROM	64 Kbits
Firmware	Upgradeable via the Web Manager, TFTP, or FTP; Evolution-based OS runs up to 120 MHz
Serial Interface	2 serial ports: 1 RS232, 1 RS422/485 (4-Wire/2-Wire) with terminal block connection Baud rate selectable from 300 to 230k Kbps Customizable baud rate support for non-standard serial speeds LED indicators for TXD and RXD activities
Serial Line Formats	Characters: 7 or 8 data bits Stop bits: 1 or 2 Parity: odd, even, none
Digital I/O	2 independently configurable digital I/Os, configured via Web Page, CLI, or XML Opto-isolated to eliminate grounding issues Logically compatible with 3.3V and higher voltage levels Solid state relay if configured as outputs; thus, can also be used as small signal DC/AC switches Transient voltage and polarity reversal protections built in
Relay	Contacts capable of handling up to 8A resistive load Contacts mechanically isolated to eliminate grounding issues Contacts non-latching with Normally Open (NO) or Normally Closed (NC) for simple applications such as power failure indication
Modem Control	CTS, RTS, DTR, DCD on Serial 1
Flow Control	Hardware: RTS/CTS on Serial 1 Software: XON/XOFF
Power Input	Removable screw terminal block connector 9-30 VDC or 9-24 VAC with chassis ground 2.3W maximum
Network Interface	1 RJ45 Ethernet port 10Base-T or 100Base-TX Full or half duplex Auto-negotiating or hard coded

Category	IntelliBox-I/O 2100 Specifications
	LED indicators
Dimensions (LxWxH)	115 x 109 x 23 mm (4.54 x 4.30 x .90 in), terminal blocks included
Weight	0.3 Kg (0.63 lb) (10 oz)
Temperature	-40°C to 75°C (-40°F to 167°F) Operating -40°C to +85°C (-40°F to 185°F) Storage
Relative Humidity	10 to 90%, non-condensing
Case	Metal enclosure with wall mounts
Protocols Supported	ARP, UDP/IP, TCP/IP, Telnet, ICMP, SNMP, DHCP, BOOTP, TFTP, Auto IP, SMTP, FTP, DNS, Traceroute, HTTP, Modbus TCP, Modbus ASCII/RTU
Management	Internal web server SNMP v2C (MIB-II, RS232MIB) Serial login Telnet/SSH login XML DeviceInstaller software
Security	SSL v3, SSH v2 MD5, SHA-1 Rijndael/AES 128-bit encryption 3DES encryption ARC4 128-bit encryption Password protection IP address filtering Hardened OS and stack
Internal Web Server	Serves static and dynamic CGI-based pages and Java applets Storage capacity: Limited to size of file system
System Software	Windows-based DeviceInstaller configuration software and Windows-based Com Port Redirector
LEDs	10Base-T and 100Base-TX Link Ethernet Activity Serial Transmit Data Serial Receive Data Power/Status
Isolation and Transient Voltage Protection	1.5 KVAC/2.1 KVDC galvanic isolation between power input port and Ethernet ports (except chassis ground) 1.5 KVAC / 2.1 KVDC galvanic isolation between power input port and serial ports 1.5 KVAC / 2.1 KVDC galvanic isolation between Ethernet port and serial ports 1.5 KVAC / 2.1 KVDC opto-isolation between digital I/O ports and all other ports 1.5 KVAC / 2.1 KVDC mechanical isolation between relay contacts and all other ports 8 KV direct contact, 15 KV air discharge, ESD protection on all serial ports (IEC 1000-4-2, IEC 61000-4-2) 40 A (5/50 ns) EFT protection (IEC 61000-4-4), 12 A (8/20 us) lightning protection (IEC 61000-4-5) on Ethernet port Transient voltage protection and ESD at power input with max non-repetitive surge current 800 A 8/20 us) (IEC 61000-4-2) Transient voltage protection and ESD with max non-repetitive surge power 600W peak (10/1000 us) at digital I/O ports

Category	IntelliBox-I/O 2100 Specifications
Agency Approvals	UL, CSA, FCC, CE, TUV, CTick, VCCI
EMC Standards	
ITE	FCC Part 15 Subpart B Class A ICES-003 Issue 4 February 2004 Class A AS/NZS CISPR 22: 2006 Class A EN55022: 1998 + A1: 2000 + A2: 2003 CLASS A EN61000-3-2: 2000 Class A EN61000-3-3: 1995 +A1: 2001 EN55024: 1998 +A1: 2001 +A2: 2003 IEC_61000-4-2: 1995 IEC_61000-4-3: 1995 IEC_61000-4-4: 1995 IEC_61000-4-5: 1995 IEC_61000-4-6: 1996 IEC_61000-4-8: 1993 IEC_61000-4-11: 1994
Industrial Environment	FCC Part 18 Subpart C ICES-001 Issue 4 July 2004 EN61000-6-4: 2001 and AS/NZS 4251.2: 1999 CISPR11 EN61000-6-2: 2001 and AS/NZS 61000.6.2: 2002 IEC_61000-4-2: 1995 IEC_61000-4-3: 1995 IEC_61000-4-4: 1995 IEC_61000-4-5: 1995 IEC_61000-4-6: 1996 IEC_61000-4-8: 1993 IEC_61000-4-11: 1994
Safety Standards	UL 60950-1 CSA 22.2. No 60950-1-03 EN 60950-1 TUV VCCI C-Tick
Product Label Markings	FCC Part 15 Statement Class A Device, ICES-003 Class A Device, C-Tick, VCCI, CE Marking, UL-CUL Mark, TUV-GS Mark

E: Isolated I/O Specifications

Absolute Maximum Ratings

Parameters	Symbols	Value	Units	Notes
Operating temperature	T_{OPR}	-40 to 75	C	
Output characteristics of Digital I/O ports (see note 5)				
Load current when ON	I_L	120	mA	1
Breakdown load voltage when OFF	V_L	+/-50	VDC	
Input characteristics of Digital I/O ports (see note 5)				
Input current	I_I	8	mA	2
Input voltage	V_I	10	VDC	2, 4
Input reverse voltage	V_I	-50	VDC	
Transient voltage suppression on digital I/O (see note 5)				
Peak pulse power dissipation on 10/1000 usec Waveform	P_{TVS}	600	W	
Isolation Characteristics of digital I/O ports (see note 5)				
Between primary to secondary of IO ports	V_{IOISO1}	1500	VAC	
Between adjacent IO Ports	V_{IOISO2}	300	VAC	
Isolation characteristics of relay port (see note 5)				
Between contacts and coil (inner circuit)	$V_{RLYISO1}$	1500	VAC	
Between open contacts	$V_{RLYISO2}$	300	VAC	
Between relay port and IO Ports	$V_{RLYISO3}$	1500	VAC	

Stressing the device above the rating listed in the Absolute Maximum Ratings table may cause permanent damage to the IO ports. Exposure to Absolute Maximum Rating conditions for extended periods may affect the IO port reliability.

Notes:

1. *Solid state relay output; can source or sink current. See Figure C-1.*
2. *Opto-isolator with emitter input and a series resistor to limit current. See Figure C-2.*
3. *To realize a logic high input, a typical current of I_I = 1mA is required; that translates to a minimum of V_{IH} = 3V.*
4. *For $V_I = V_{IH} > 10$ VDC an external series resistor is required as shown in Table C-1.*
5. *Connect RELAY and DIGITAL IO Ports only to Class III or Class 2 circuit.*

Electrical Characteristics

Parameters	Symbols	Min	Typ	Max	Units	Notes
Output characteristics of digital I/O ports (see note 5)						
Continuous load current	I_L			100	mA	1
On resistance (I_L = 50 mA)	R_{ON}			15	Ohm	
Load voltage when ON (I_L = 50 mA)	V_L			0.75	VDC	
Leakage current when OFF	I_L			50	uA	
Input characteristics of digital/O ports (see note 5)						
High level input voltage (I_I = 1 mA typically)	V_{IH}	3.0			VDC	2, 3
Low level input voltage	V_{IL}			0.8	VDC	2
Characteristics of relay port (see note 5)						
Switching voltage	V_{RLY}			250	VAC	5
Switching voltage	V_{RLY}			30	VDC	
Switching current (resistive load)	I_{RLY}			8	A	

Notes:

1. *Solid state relay output; can source or sink current. See Figure C-1.*
2. *Opto-isolator with emitter input and a series resistor to limit current. See Figure C-2.*
3. *To realize a high logic input, a typical current of II = 1mA is required; that translates to a minimum of VIH = 3V.*
4. *For VI = VIH > 10 VDC an external series resistor is required as shown in Table C-1.*
5. *Connect RELAY and DIGITAL IO Ports only to Class III or Class 2 circuit.*

Figure C-1 Optically Isolated I/O Configured as an Output with Solid State Relay

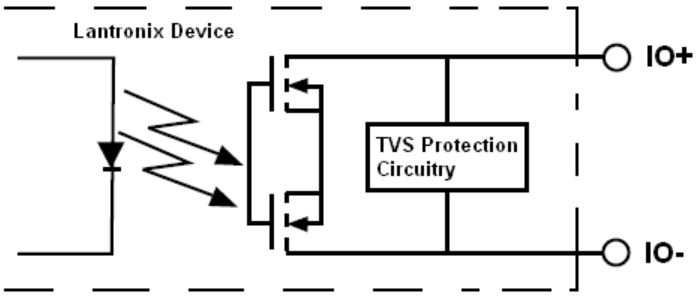


Figure C-2 Optically Isolated I/O Configured as an Input with Opto-Isolator's Emitter

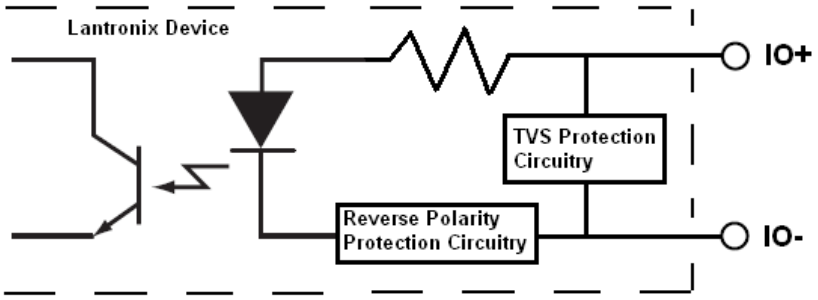


Figure C-3 Application Circuit

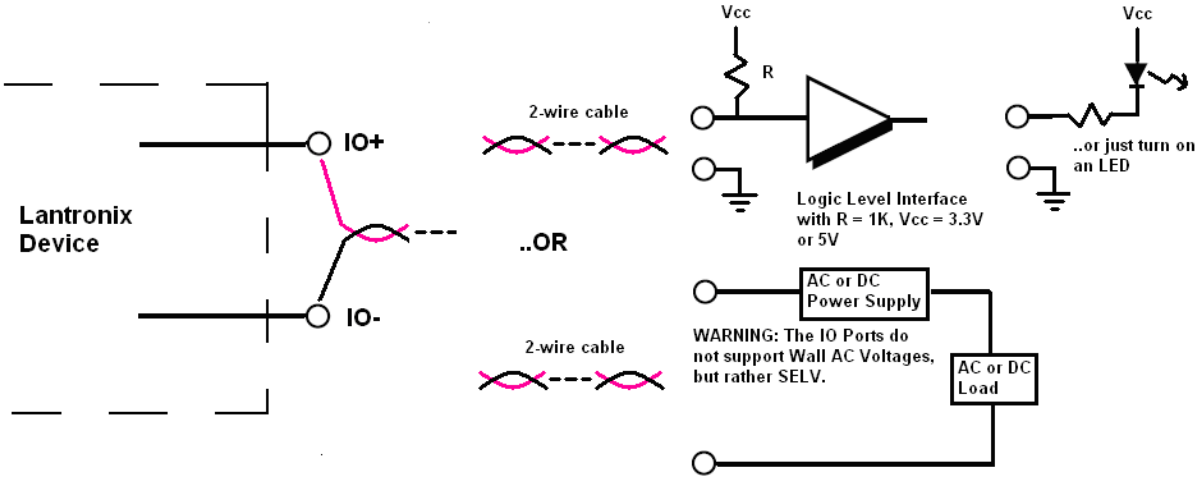
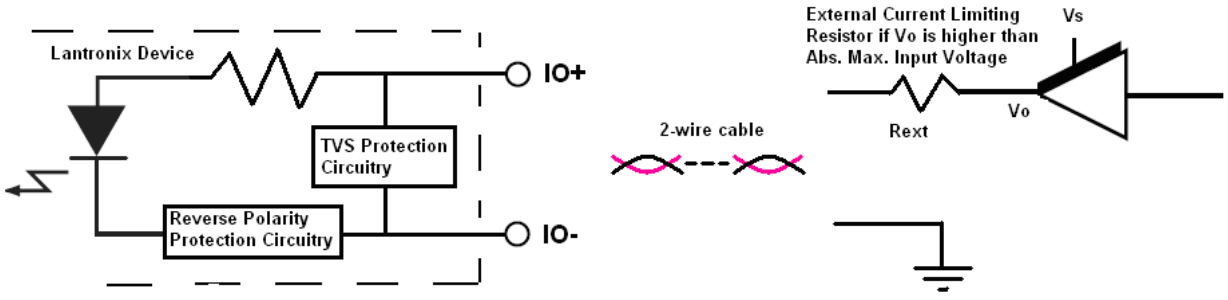


Figure C-4 Isolated General Purpose Input Application Circuit



Note: *For input close to or higher than Absolute Maximum Rating value, use a series resistor Rext as in Figure C-4. Table C-1 has the tabulated values for Rext in such cases.*

Table E-1 Rext Values

VOH (V)	REXT (K)
7	2.57
8	3.23
9	3.9
10	4.57
11	5.23
12	5.9
13	6.57
14	7.23
15	7.9
16	8.57
17	9.23
18	9.9
19	10.6
20	11.2
21	11.9
22	12.6
23	13.2
24	13.9
25	14.6
26	15.2
72	15.9
28	16.6
29	17.2
30	17.9

The Rext resistor limits the current I to about 1.5 mA, and Rext is 1/4W.

Figure C-5. Relay Contact position when not energized (power off)

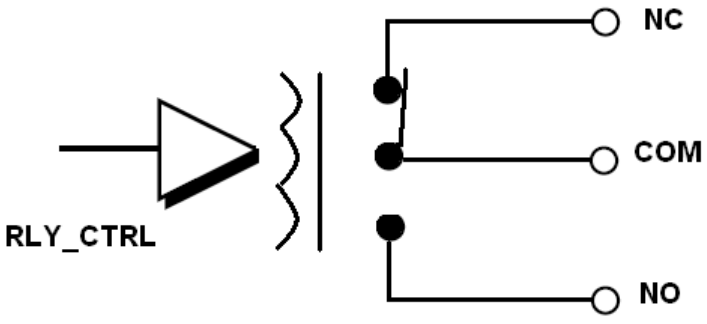
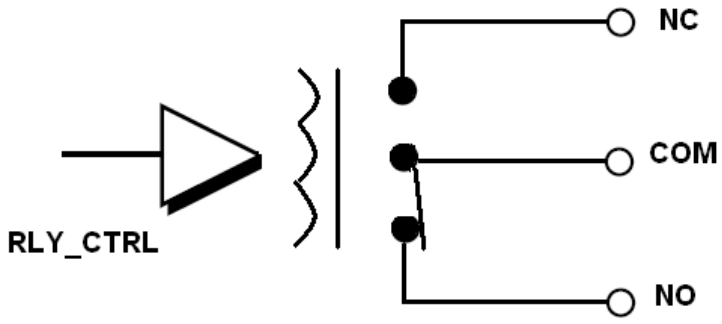
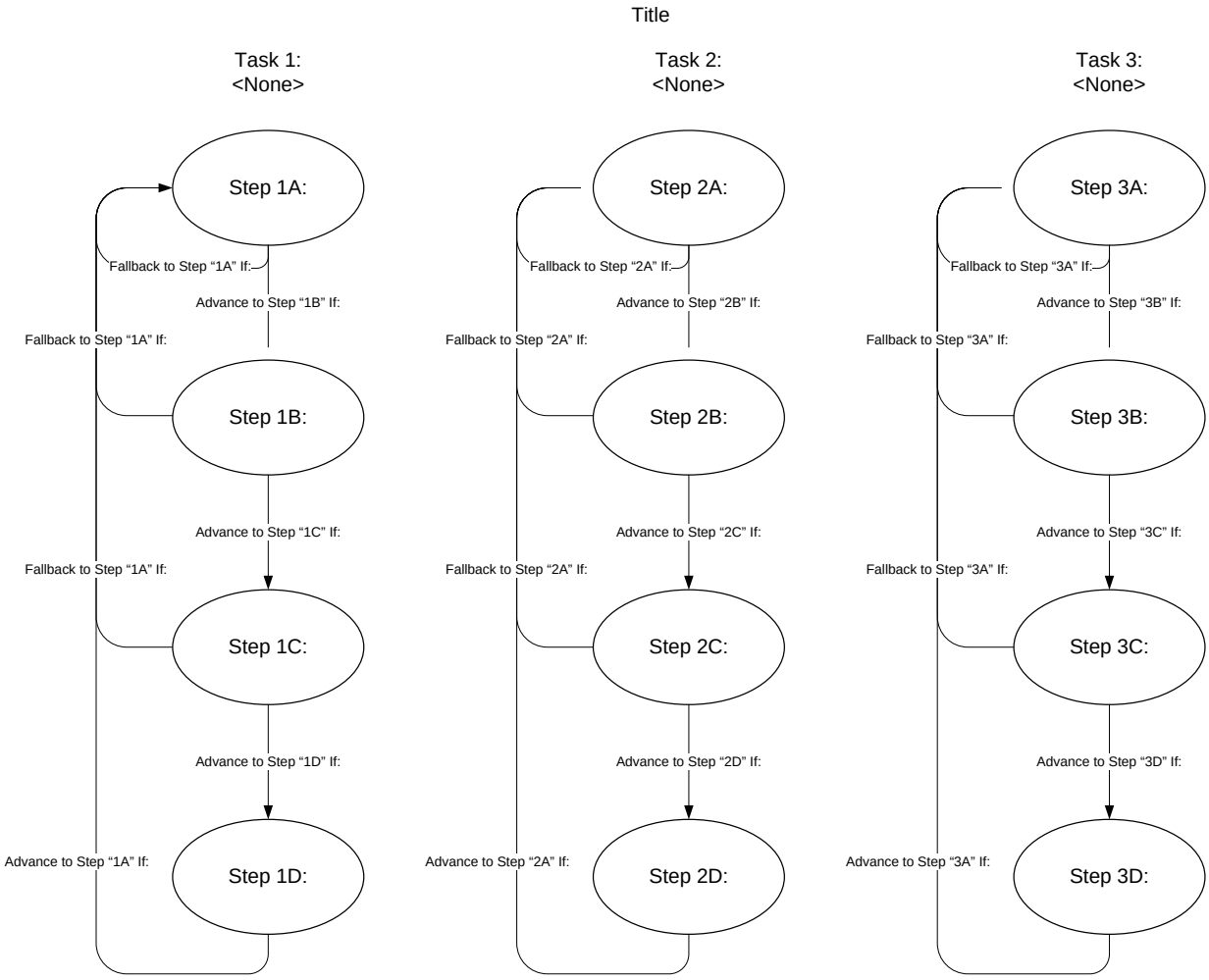


Figure C6 Relay Contact position when energized



F: State Diagram Template

The following is a state diagram template that you may find helpful when creating an EventTrak.



G: Technical Support

If you are unable to resolve an issue using the information in this documentation:

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

Technical Support Europe, Middle East, Africa

Phone: +33 1 39 30 41 72
Email: eu_techsupp@lantronix.com or eu_support@lantronix.com

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

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

- Your name, and your company name, address, and phone number
- Lantronix model number
- Lantronix serial number
- Software version (on the first screen shown when you Telnet to port 23)
- 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)

H: Compliance

Declaration of Conformity

(according to ISO/IEC Guide 22 and BS 7514)

Manufacturer's Name & Address:

Lantronix, 167 Technology Drive, Irvine, CA 92618 USA

Declares that the following product:

Product Name Model: IntelliBox-I/O 2100 2 Port Industrial Device Server

Description: 2-Port Industrial Device Server with Optically Isolated Digital I/Os and a Relay

Conforms to the following standards or other normative documents:

Safety:

UL 60950-1

CSA 22.2. No 60950-1-03

EN 60950-1

TUV

VCCI

C-Tick

Electromagnetic Emissions and Immunity:

ITE	
Emissions:	**Immunity:**
FCC Part 15 Subpart B Class A ICES-003 Issue 4 February 2004 Class A AS/NZS CISPR 22: 2006 Class A EN55022: 1998 + A1: 2000 + A2: 2003 CLASS A EN61000-3-2: 2000 Class A EN61000-3-3: 1995 +A1: 2001	EN55024: 1998 +A1: 2001 +A2: 2003 IEC_61000-4-2: 1995 IEC_61000-4-3: 1995 IEC_61000-4-4: 1995 IEC_61000-4-5: 1995 IEC_61000-4-6: 1996 IEC_61000-4-8: 1993 IEC_61000-4-11: 1994

Industrial Environment	
Emissions:	**Immunity**
FCC Part 18 Subpart C ICES-001 Issue 4 July 2004 EN61000-6-4: 2001 and AS/NZS 4251.2: 1999 CISPR11	EN61000-6-2: 2001 and AS/NZS 61000.6.2: 2002 IEC_61000-4-2: 1995 IEC_61000-4-3: 1995 IEC_61000-4-4: 1995 IEC_61000-4-5: 1995 IEC_61000-4-6: 1996 IEC_61000-4-8: 1993 IEC_61000-4-11: 1994

Supplementary Information:

This Class A digital apparatus complies with Canadian ICES-003 (CSA) and has been verified as being compliant within the Class A limits of the FCC Radio Frequency Device Rules (FCC Title 47, Part 15, Subpart B CLASS A), measured to CISPR 22: 1993 limits and methods of measurement of Radio Disturbance Characteristics of Information Technology Equipment. The product complies with the requirements of the Low Voltage Directive 72/23/EEC and the EMC Directive 89/336/EEC.

Manufacturer's Contact:

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

I: Warranty

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

Index