



## xPico<sup>®</sup> Wi-Fi<sup>®</sup> Embedded Device Server User Guide

---

## Intellectual Property

© 2018 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

*Lantronix* and *xPico* are registered trademarks of Lantronix, Inc. in the United States and other countries. *DeviceInstaller* is a trademark of Lantronix, Inc.

Patented: <http://patents.lantronix.com>; additional patents pending.

*Internet Explorer* is a registered trademark of Microsoft Corporation. *Mozilla* and *Firefox* are registered trademarks of the Mozilla Foundation. *Chrome* is a trademark of Google Inc. *Wi-Fi* is a registered trademark of Wi-Fi Alliance Corporation. All other trademarks and trade names are the property of their respective holders.

## Warranty

For details on the Lantronix warranty policy, please go to our web site at [www.lantronix.com/support/warranty](http://www.lantronix.com/support/warranty).

## Contacts

### Lantronix, Inc. Corporate Headquarters

7535 Irvine Center Drive  
Suite 100  
Irvine, CA 92618, USA

Toll Free: 800-526-8766  
Phone: 949-453-3990  
Fax: 949-453-3995

### Technical Support

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

### Sales Offices

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

## Disclaimer

All information contained herein is provided "AS IS." Lantronix undertakes no obligation to update the information in this publication. Lantronix does not make, and specifically disclaims, all warranties of any kind (express, implied or otherwise) regarding title, non-infringement, fitness, quality, accuracy, completeness, usefulness, suitability or performance of the information provided herein. Lantronix shall have no liability whatsoever to any user for any damages, losses and causes of action (whether in contract or in tort or otherwise) in connection with the user's access or usage of any of the information or content contained herein. The information and specifications contained in this document are subject to change without notice.

---

## Revision History

| Date           | Rev. | Comments   |
|----------------|------|--|
| July 2013      | A    | Initial document (firmware 1.0.0.0R7).   |
| November 2013  | B    | Updated serial port information.   |
| January 2014   | C    | Updated for firmware 1.1.0.2. to include new CPM, diagnostics, modem emulation, monitor, performance, SPI, XML, CLI and command reference information. |
| February 2014  | D    | Updated for firmware version 1.1.0.2R10.   |
| February 2014  | E    | Updated serial port configuration information.   |
| November 2014  | F    | Updated for version 1.3.0.0 of the firmware.   |
| January 2015   | G    | Updated with new Japan ID numbers.   |
| April 2015     | H    | Updated XCR DTD instructions.  |
| March 2016     | J    | Updated for version 1.4.0.0 of the firmware to include the addition of Bridging and Radio features.  |
| September 2017 | K    | Updated compliance information.  |
| March 2018     | L    | Updated for firmware version 1.5.0.0.  |

---

# Table of Contents

|  |           |
|--|-----------|
| Intellectual Property                        | 2         |
| Warranty                                     | 2         |
| Contacts                                     | 2         |
| Disclaimer                                   | 2         |
| Revision History                             | 3         |
| List of Figures                              | 11        |
| List of Tables                               | 12        |
| <b>1: Using This Guide</b>                   | <b>14</b> |
| Purpose and Audience                         | 14        |
| Summary of Chapters                          | 14        |
| Additional Documentation                     | 15        |
| <b>2: Introduction</b>                       | <b>16</b> |
| Key Features                                 | 16        |
| Protocol Support                             | 17        |
| Troubleshooting Capabilities                 | 18        |
| Configuration Methods                        | 18        |
| Addresses and Port Numbers                   | 18        |
| Hardware Address                             | 18        |
| IP Address                                   | 18        |
| Port Numbers                                 | 18        |
| Product Information Label                    | 19        |
| <b>3: Configuration Using XML</b>            | <b>20</b> |
| XML Architecture and Device Control          | 20        |
| XML over Serial Port                         | 20        |
| To Configure Flow Control Options on the CLI | 21        |
| To Import or Export XML Configuration        | 21        |
| XML over the Network                         | 22        |
| XML Configuration Language                   | 22        |
| XML Syntax                                   | 23        |
| Element Start and End Tags                   | 23        |
| Element Attributes                           | 23        |
| Record, Group, Item, and Value Tags          | 24        |

---

|   |           |
|---|-----------|
| <b>4: Configuration Using Web Manager</b>                         | <b>25</b> |
| Accessing Web Manager _____                                       | 25        |
| Status Page _____   | 26        |
| Web Manager Components _____                                      | 27        |
| Navigating Web Manager _____                                      | 27        |
| <b>5: WebAPI</b>  | <b>29</b> |
| Export Status Group _____   | 29        |
| Export Configuration Group _____                                  | 29        |
| Take Status Action _____  | 30        |
| Import Configuration Group _____                                  | 31        |
| <b>6: OEM Management</b>  | <b>32</b> |
| Protected Configuration Details _____                             | 32        |
| XCR OEM Group Configuration Group _____                           | 32        |
| OEM Group Configuration Password _____                            | 33        |
| Reading and Writing the Region Code of the xPico Wi-Fi Unit _____ | 34        |
| Reading the Current OEM Configuration Group from the CLI _____    | 34        |
| Writing the OEM Configuration Group from the CLI _____            | 34        |
| Setting OEM Configuration Defaults _____                          | 36        |
| Branding the xPico Wi-Fi _____                                    | 37        |
| <b>7: Wireless Network Settings</b>                               | <b>38</b> |
| Network ap0 Interface Configuration _____                         | 38        |
| To Configure Network ap0 Interface Settings _____                 | 38        |
| To View Network ap0 Interface Status _____                        | 39        |
| Network ap0 Link Settings _____                                   | 39        |
| Triggered AP Mode _____   | 40        |
| To Configure Network ap0 Link Settings _____                      | 40        |
| To View Network ap0 Link Status _____                             | 41        |
| Network wlan0 Interface Configuration _____                       | 41        |
| To Configure Network wlan0 Interface Settings _____               | 42        |
| To View Network wlan0 Interface Status _____                      | 42        |
| Network wlan0 Link Status _____                                   | 43        |
| To View Network wlan0 Link Status _____                           | 43        |
| WLAN Profiles _____   | 43        |
| To Configure WLAN Profiles _____                                  | 43        |
| To Configure WLAN Profile Settings _____                          | 44        |
| WLAN Quick Connect _____  | 46        |
| To Configure WLAN Quick Connect _____                             | 46        |
| Hidden Access Points _____  | 47        |
| Lantronix Smart Connect EasyWEP _____                             | 47        |

---

|  |           |
|--|-----------|
| Radio Configuration _____                          | 48        |
| To View or Configure Radio _____                   | 49        |
| <b>8: Interface Settings</b>                       | <b>50</b> |
| Line Settings (Serial) _____                       | 50        |
| To Configure Line Settings _____                   | 51        |
| To View Line Status _____                          | 51        |
| Serial Command Mode _____                          | 51        |
| Boot to CLI _____                                  | 52        |
| Escape Characters _____                            | 53        |
| Device Recovery _____                              | 54        |
| Serial Peripheral Interface (SPI) Settings _____   | 54        |
| To Configure SPI Settings _____                    | 55        |
| To View SPI Status _____                           | 55        |
| Lantronix Query Port _____                         | 55        |
| Discovery _____                                    | 56        |
| To Configure Discovery Settings _____              | 56        |
| <b>9: Tunnel Settings</b>                          | <b>57</b> |
| Tunnel Settings _____                              | 57        |
| Line Settings _____                                | 57        |
| To View Tunnel Serial Settings _____               | 57        |
| Packing Mode _____                                 | 58        |
| To Configure Tunnel Packing Mode Settings _____    | 59        |
| Accept Mode _____                                  | 59        |
| To Configure Tunnel Accept Mode Settings _____     | 61        |
| Connect Mode _____                                 | 61        |
| To Configure Tunnel Connect Mode Settings _____    | 62        |
| Disconnect Mode _____                              | 63        |
| To Configure Tunnel Disconnect Mode Settings _____ | 63        |
| Statistics _____                                   | 63        |
| To View Tunnel Statistics _____                    | 64        |
| <b>10: Modem Emulation Settings</b>                | <b>65</b> |
| <b>11: Configurable Pin Manager</b>                | <b>67</b> |
| CP Roles _____                                     | 67        |
| To Configure CPM Settings _____                    | 68        |
| Configurable Pin Status _____                      | 68        |

---

|  |           |
|--|-----------|
| <b>12: Application Aware Power Management</b>                                    | <b>70</b> |
| Power Up Mode _____  | 70        |
| Sleep Mode _____   | 70        |
| Standby Mode _____   | 70        |
| Dynamic Power Mode Configuration _____   | 71        |
| Power Settings _____   | 71        |
| To Configure Power _____   | 72        |
| <br>   |           |
| <b>13: Services Settings</b>   | <b>73</b> |
| HTTP Server _____  | 73        |
| To Configure HTTP Settings and Security _____                                    | 73        |
| HTTP Security _____  | 73        |
| To View HTTP Status _____  | 74        |
| Real Time Clock and Current Time _____   | 74        |
| To View or Configure the Clock _____   | 75        |
| Simple NTP Client _____  | 75        |
| To View or Configure the NTP _____   | 76        |
| CLI Server _____   | 76        |
| To View or Configure the CLI Server _____  | 76        |
| <br>   |           |
| <b>14: Maintenance and Diagnostics</b>   | <b>78</b> |
| File System Settings _____   | 78        |
| File System Statistics _____   | 78        |
| To View File System Statistics, Compact or Format the File System _____          | 78        |
| File Display _____   | 78        |
| To Display Files _____   | 78        |
| File Manipulation _____  | 79        |
| To Transfer or Modify File System Files _____                                    | 79        |
| Device Settings _____  | 79        |
| Device Management _____  | 79        |
| To Save Configuration, Reboot, Restore Factory Defaults or Upload Firmware _____ | 80        |
| User _____   | 80        |
| To Configure Admin User on the Device _____                                      | 81        |
| Diagnostics Settings _____   | 81        |
| To View Buffer Pool Status _____   | 81        |
| To View Hardware Status _____  | 81        |
| To View Heap Status _____  | 82        |
| To View IP Socket Status _____   | 82        |
| To View Modules Status _____   | 82        |
| To Ping _____  | 83        |
| To View Threads Status _____   | 83        |

---

|  |            |
|--|------------|
| <b>15: Security Settings</b>                               | <b>84</b>  |
| Serial Tunneling: TCP AES _____                            | 84         |
| AES Credential Management _____                            | 84         |
| To Manage AES Credentials _____                            | 85         |
| <br>   |            |
| <b>16: Lantronix Application Toolbox for IOT Solutions</b> | <b>86</b>  |
| Serial Multiplexer _____                                   | 86         |
| Usage _____  | 86         |
| xPico Wi-Fi Mux Command Reference _____                    | 86         |
| Example #1 _____   | 91         |
| Example #2 of Using Mux Feature _____                      | 91         |
| Monitor Settings _____                                     | 92         |
| Explorer _____   | 93         |
| Configuration _____  | 94         |
| To Configure Monitor _____                                 | 96         |
| Example: Data Capture on a Serial Device _____             | 97         |
| Initialization _____                                       | 98         |
| Polling _____  | 98         |
| Filtering _____  | 99         |
| Data Mining _____  | 101        |
| Presenting _____   | 102        |
| Data Capture on SPI _____                                  | 103        |
| <br>   |            |
| <b>17: Branding the xPico Wi-Fi Unit</b>                   | <b>104</b> |
| Customizing Web Manager Appearance _____                   | 104        |
| Path Format _____  | 104        |
| Other Overridable Files _____                              | 105        |
| Adding Your Own Web Files _____                            | 105        |
| Creating Your Own Webpages _____                           | 105        |
| OEM Configgroup Options _____                              | 105        |
| <br>   |            |
| <b>18: Updating Firmware Over the Air</b>                  | <b>106</b> |
| Obtaining Firmware _____                                   | 106        |
| Loading New Firmware through Web Manager _____             | 106        |
| Loading New Firmware without Web Manager _____             | 108        |
| Importing WLAN Configuration with XML _____                | 108        |
| <br>   |            |
| <b>Appendix A: Command Reference</b>                       | <b>109</b> |
| Conventions _____  | 109        |
| Configuration Using Serial Port _____                      | 110        |
| Boot to CLI _____  | 110        |
| Navigating the CLI Hierarchy _____                         | 111        |

---

|  |     |
|--|-----|
| Using Keyboard Shortcuts and CLI _____           | 111 |
| Understanding the CLI Level Hierarchy _____      | 112 |
| XML for xPico Wi-Fi Embedded Device Server _____ | 113 |
| configgroup Access Point _____                   | 113 |
| configgroup Clock _____                          | 114 |
| configgroup CPM _____                            | 115 |
| configgroup HTTP Server _____                    | 116 |
| configgroup HTTP Server Security _____           | 116 |
| configgroup Interface _____                      | 118 |
| configgroup Line _____                           | 119 |
| configgroup Power _____                          | 121 |
| configgroup Radio _____                          | 123 |
| configgroup SPI _____                            | 124 |
| configgroup User _____                           | 125 |
| configgroup WLAN Profile _____                   | 126 |
| configgroup XML Import Control _____             | 127 |
| configgroup AES Credential _____                 | 128 |
| configgroup CLI Server _____                     | 129 |
| configgroup Discovery _____                      | 129 |
| configgroup Modem Emulation _____                | 129 |
| configgroup Monitor Initialization _____         | 131 |
| configgroup Monitor Control _____                | 132 |
| configgroup Monitor Poll _____                   | 133 |
| configgroup Monitor Filter _____                 | 134 |
| configgroup Monitor Data _____                   | 135 |
| configgroup NTP _____                            | 135 |
| configgroup Tunnel Accept _____                  | 136 |
| configgroup Tunnel Line _____                    | 138 |
| configgroup Tunnel Connect _____                 | 138 |
| configgroup Tunnel Disconnect _____              | 141 |
| configgroup Tunnel Packing _____                 | 142 |
| configgroup Custom _____                         | 143 |

## **Appendix B: Technical Support 145**

## **Appendix C: Compliance 146**

|   |     |
|---|-----|
| Federal Communication Commission Interference Statement _____ | 150 |
| Radiation Exposure Statement _____                            | 150 |
| End Product Labeling _____                                    | 150 |
| Manual Information To the End User _____                      | 151 |
| Industry Canada Statement _____                               | 151 |
| Radiation Exposure Statement _____                            | 151 |
| Déclaration d'exposition aux radiations _____                 | 151 |

---

|  |     |
|--|-----|
| End Product Labeling _____                       | 152 |
| Plaque signalétique du produit final _____       | 152 |
| Manual Information To the End User _____         | 152 |
| Manuel d'information à l'utilisateur final _____ | 152 |
| Antenna Requirement _____                        | 153 |
| RoHS, REACH and WEEE Compliance Statement _____  | 153 |

---

## List of Figures

|   |     |
|---|-----|
| Figure 2-1 xPico Wi-Fi Product Label          | 19  |
| Figure 3-1 Single Character Commands          | 21  |
| Figure 3-2 XML Example                        | 23  |
| Figure 3-3 XML Example                        | 24  |
| Figure 4-1 Status Page                        | 26  |
| Figure 4-2 Components of the Web Manager Page | 27  |
| Figure 16-7 Monitor Initialization            | 98  |
| Figure 16-8 Monitor Polling (1 of 2)          | 98  |
| Figure 16-9 Monitor Polling (2 of 2)          | 99  |
| Figure 16-10 Monitor Filtering (1 of 2)       | 99  |
| Figure 16-11 Monitor Filtering (2 of 2)       | 100 |
| Figure 16-12 Monitor Data Mining (1 of 2)     | 101 |
| Figure 16-13 Monitor Data Mining (2 of 2)     | 101 |
| Figure 16-14 Monitor Presenting               | 102 |
| Figure 16-15 Monitor CLI Command Level        | 102 |
| Figure 16-16 Monitor XML Commands             | 103 |
| Figure 18-1 Uploading New Firmware            | 107 |
| Figure A-2 Root Level Commands                | 112 |
| Figure C-2 EU Declaration of Conformity       | 147 |

---

## List of Tables

|  |    |
|--|----|
| Table 4-3 Web Manager Pages                            | 28 |
| Table 7-1 Network Interface Settings                   | 38 |
| Table 7-2 Network ap0 Link Settings                    | 39 |
| Table 7-3 Network Interface Settings                   | 41 |
| Table 7-4 Creating, Deleting or Enabling WLAN Profiles | 44 |
| Table 7-5 WLAN Profile Basic Settings                  | 45 |
| Table 7-6 WLAN Profile Security Settings               | 45 |
| Table 7-7 WLAN Profile Advanced Settings               | 46 |
| Table 7-8 WLAN Quick Connect                           | 47 |
| Table 7-9 Radio Settings                               | 48 |
| Table 8-1 Line Configuration Settings                  | 50 |
| Table 8-2 SPI Configuration Settings                   | 54 |
| Table 8-3 Discovery Settings                           | 56 |
| Table 9-1 Tunnel Line Settings                         | 57 |
| Table 9-2 Tunnel Packing Mode Settings                 | 58 |
| Table 9-3 Tunnel Accept Mode Settings                  | 59 |
| Table 9-4 Tunnel Connect Mode Settings                 | 61 |
| Table 9-5 Tunnel Disconnect Mode Settings              | 63 |
| Table 10-1 Modem Emulation Settings                    | 65 |
| Table 10-2 Modem Emulation Commands and Descriptions   | 66 |
| Table 11-1 Role Configuration                          | 68 |
| Table 11-2 Current Configurable Pins                   | 68 |
| Table 11-3 CP Status                                   | 69 |
| Table 12-1 Power Settings                              | 71 |
| Table 13-1 HTTP Settings                               | 73 |
| Table 13-2 HTTP Security Settings                      | 73 |
| Table 13-3 Clock Settings                              | 75 |
| Table 13-4 NTP Settings                                | 76 |
| Table 13-5 CLI Server Settings                         | 76 |
| Table 14-1 File System Statistics Settings             | 78 |
| Table 14-2 Device Management Settings                  | 79 |
| Table 14-3 User Management                             | 80 |
| Table 14-4 User Settings                               | 80 |
| Table 14-5 IP Socket Settings                          | 82 |
| Table 14-6 Ping Settings                               | 83 |

---

|   |     |
|---|-----|
| Table 14-7 Threads Settings                     | 83  |
| Table 15-1 AES Credential Settings              | 84  |
| Table 16-1 Monitor Explorer Settings            | 93  |
| Table 16-2 Monitor Initialization Settings      | 94  |
| Table 16-3 Monitor Control Settings             | 95  |
| Table 16-4 Monitor Poll Settings                | 95  |
| Table 16-5 Monitor Filter Settings              | 96  |
| Table 16-6 Monitor Data Settings                | 96  |
| Table A-1 Keyboard Shortcuts                    | 111 |
| Table C-1 Country Certifications                | 146 |
| Table C-3 Country Transmitter IDs               | 148 |
| Table C-4 Safety                                | 148 |
| Table C-5 Europe – EU Declaration of Conformity | 148 |
| Table C-6 Approved Antenna(s) List              | 153 |

# 1: Using This Guide

## Purpose and Audience

This guide provides the information needed to configure, use, and update the Lantronix® xPico® Wi-Fi® embedded device server. It is intended for software developers and system integrators who are embedding this product into their designs.

## Summary of Chapters

The remaining chapters in this guide include:

| Chapter   | Description  |
|---|--|
| <a href="#">2: Introduction</a>                                     | Main features of the product and the protocols it supports. Includes technical specifications.                   |
| <a href="#">3: Configuration Using XML</a>                          | Instructions for using XML to configure settings for the device.   |
| <a href="#">4: Configuration Using Web Manager</a>                  | Instructions for accessing Web Manager and using it to configure settings for the device.                        |
| <a href="#">5: WebAPI</a>   | Instructions for viewing status information and configuring a unit through HTTP request.                         |
| <a href="#">6: OEM Management</a>                                   | Provides OEM-specific configuration options.   |
| <a href="#">7: Wireless Network Settings</a>                        | Instructions for configuring wireless client and access point network settings.                                  |
| <a href="#">8: Interface Settings</a>                               | Instructions for configuring various interface settings.   |
| <a href="#">9: Tunnel Settings</a>                                  | Instructions for configuring tunnel settings.  |
| <a href="#">10: Modem Emulation Settings</a>                        | Instructions for configuring modem emulation.  |
| <a href="#">11: Configurable Pin Manager</a>                        | Information about the Configurable Pin Manager (CPM) and how to set the configurable pins to work with a device. |
| <a href="#">12: Application Aware Power Management</a>              | Description and information on how to configure and use power management framework capabilities.                 |
| <a href="#">13: Services Settings</a>                               | Instructions for configuring HTTP settings.  |
| <a href="#">14: Maintenance and Diagnostics</a>                     | Instructions to maintain the xPico Wi-Fi embedded device server, view statistics, files, and diagnose problems.  |
| <a href="#">15: Security Settings</a>                               | Instructions for updating TCP AES and AES Credential Management.   |
| <a href="#">16: Lantronix Application Toolbox for IOT Solutions</a> | Instructions for configuring MUX and monitor settings.   |
| <a href="#">17: Branding the xPico Wi-Fi Unit</a>                   | Instructions for branding the Web Manager user interface.  |
| <a href="#">18: Updating Firmware Over the Air</a>                  | Instructions for obtaining the latest firmware and updating the xPico Wi-Fi units.                               |
| <a href="#">Appendix A: Command Reference</a>                       | Information on configuring settings using XML or the command line interface.                                     |
| <a href="#">Appendix B: Technical Support</a>                       | Instructions for contacting Lantronix Technical Support.   |
| <a href="#">Appendix C: Compliance</a>                              | Lantronix compliance information.  |

## Additional Documentation

Visit the Lantronix Web site at [www.lantronix.com/support/documentation](http://www.lantronix.com/support/documentation) for the latest documentation and the following additional documentation.

| Document   | Description  |
|--|--|
| <b>xPico Wi-Fi SMT Embedded Device Server Datasheet</b>                    | Datasheet for the xPico Wi-Fi W1002 and W1003 SMT modules.   |
| <b>xPico Wi-Fi Embedded Device Server Integration Guide</b>                | Information about the xPico Wi-Fi SMT hardware testing the device server using the demonstration board and integrating the unit into your product.   |
| <b>xPico Wi-Fi SMT Embedded Device Server Integration Guide</b>            | Information about the xPico Wi-Fi SMT hardware, testing the device server using the demonstration board, and integrating the unit into your product. |
| <b>xPico Wi-Fi Evaluation Kit Embedded Device Server Quick Start Guide</b> | Instructions for getting the xPico Wi-Fi unit up and running.  |
| <b>xPico Wi-Fi Evaluation Kit Embedded Device Server User Guide</b>        | Information needed to use the xPico Wi-Fi embedded device server on the evaluation board.  |

## 2: Introduction

This chapter summarizes the basic information and features of the xPico Wi-Fi embedded device server.

### Key Features

- ◆ **Wireless LAN Interface:**
  - IEEE 802.11 b/g and IEEE 802.11n (single stream)
  - WLAN interface (2.4 GHz only)
  - IEEE 802.11 d/h/i/j/k/w/r
  - IEEE 802.11i Support - WEP(Client only), WPA-Personal, WPA2-Personal
  - On Module Antenna version (XPCW1003100)
  - Version with u.FL connector for external antenna
  - Soft Access Point (SoftAP) with DHCP Server
  - Simultaneous SoftAP and Client
  - Roaming: continually tracks Wi-Fi signal strength within range, resulting in smooth and automatic transition between access points without delay.
  - QuickConnect: Dynamic Profiles facilitate easy and rapid connections to access points
- ◆ **Host Interface:**
  - **Serial Interface**

Two Serial CMOS Ports 1200 to 921.6 Kbps

Flow control: XON/XOFF, RTS/CTS  
(Line 1 uses dedicated hardware, Line 2 uses configurable pins)

Lantronix tunneling application

Modem Emulation

MUX commands

Trouble log

Command line
  - **SPI Interface**

Configurable master SPI interface that can be clocked at 30MHz.
  - **USB Interface 2.0 (device)**

USB 2.0 (12 Mbps) Full Speed Device port interfaces for connection to an upstream USB host device.

Support for USB CDC Serial profile<sup>1</sup>

---

1.Feature will be available in a future software release. Contact Lantronix for more information.

- **GPIO Interface**
  - 8 configurable general purpose Input/Output pins
  - Custom pin manager
- ◆ **Network Protocols:** TCP/IP, UDP/IP<sup>1</sup>, DHCP Server (software-enabled Access Point interface), ARP, ICMP, DHCP Client (WLAN interface), Auto-IP, DNS, HTTP
- ◆ **Management and Control:**
  - Web Server
  - CLI (Serial Monitor Port)
  - XML Configuration Import and Export (XCR, XML Status Export [XSR])
  - WebAPI
  - Field upgradable firmware (OTA)
  - Power Management Framework
  - OEM Support Kit
  - Simple Customization and device configuration management
- ◆ **Security:**
  - 256-bit AES encryption
- ◆ **Architecture:**
  - ARM Cortex-M3 class processor with on-chip Flash and SRAM
  - 1 MB Flash and 128KB SRAM
  - SPI Flash 1 MB
  - Zero Host Load Driver
- ◆ **Physical Interface:** 40-pin Board-to-Board SMT Connector
 

*Note:* See the *xPico Wi-Fi SMT Embedded Device Server Integration Guide* to view the *xPico Wi-Fi SMT unit footprint*.
- ◆ **Certifications:** FCC, IC, EU, Japan, UL, CE, AU/NZ
- ◆ **Warranty:** 5-Year Limited

## Protocol Support

The xPico Wi-Fi embedded device server contains a full-featured IP stack and WLAN connection manager. Supported protocols include:

- ◆ IEEE 802.11 b/g and IEEE 802.11n (single stream) WLAN interface (2.4 GHz only)
- ◆ 802.11i - WPA-Personal, WPA2-Personal
- ◆ Soft-AP with DHCP Server
- ◆ HTTP Server

- ◆ TCP/IP, UDP/IP<sup>1</sup>, DHCP Server (Software enabled Access Point interface), ARP, ICMP, DHCP Client (WLAN interface), Auto-IP, DNS

## Troubleshooting Capabilities

The xPico Wi-Fi device offers the ability to view Trouble Log messages (see [Line Settings \(Serial\) on page 50](#)).

## Configuration Methods

After installation, the xPico Wi-Fi device server requires configuration. For the unit to operate correctly on a network, it must have a unique IP address on the network. These methods may be used for logging into the xPico Wi-Fi and assigning IP addresses and other configurable settings:

- ◆ **Web Manager:** View and configure settings easily through a web browser using the Lantronix Web Manager. See [“Configuration Using Web Manager” on page 25](#).
- ◆ **XML:** The xPico Wi-Fi supports XML import and XML export. See [“Power Settings” on page 71](#).
- ◆ **Command Mode:** Access the Command Mode (CLI) by connecting a PC or other host running a terminal emulation program to the unit’s serial port. See [“Command Reference” on page 109](#).

The xPico Wi-Fi unit also supports a cloud function WebAPI allowing partial access to configuration and status information of xPico Wi-Fi embedded device server through standard HTTP request. See [“WebAPI” on page 29](#). Some OEM configuration options are also available.

## Addresses and Port Numbers

### Hardware Address

The hardware address is also referred to as the physical address or MAC address, and can be found on the product label of the device. Sample hardware address:

- ◆ 00-80-A3-FF-FF-FF
- ◆ 00:80:A3:FF:FF:FF

### IP Address

Every device connected to an IP network must have a unique IPv4 address. This address references the specific unit.

### Port Numbers

Available IP address port numbers enabled and accessible on the xPico Wi-Fi unit include the following:

---

1.Feature will be available in a future software release. Contact Lantronix for more information.

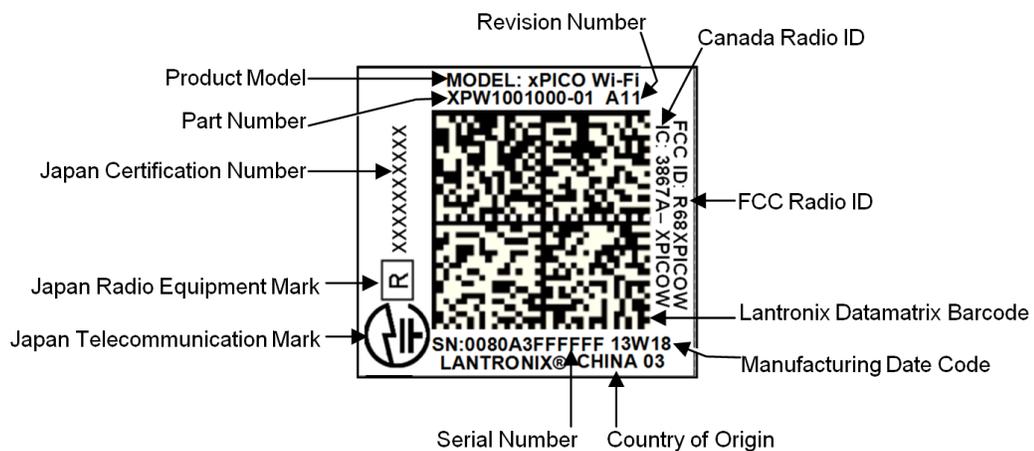
- ◆ TCP Port 80: HTTP Server (Web Manager configuration)
- ◆ TCP Port 10001: Tunnel (Line 1)
- ◆ TCP Port 10002: Tunnel (Line 2)

## Product Information Label

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

- ◆ Lantronix Datamatrix Code
- ◆ Product Revision
- ◆ Part Number
- ◆ Serial Number Hardware Address (MAC Address)
- ◆ Manufacturing Date Code

**Figure 2-1 xPico Wi-Fi Product Label**



## 3: Configuration Using XML

The xPico Wi-Fi embedded device server supports four convenient configuration methods: Extensible Markup Language (XML), Web Manager, Command Line Interface (CLI), and WebAPI. This chapter describes how to configure the xPico Wi-Fi embedded device server using Extensible Markup Language (XML).

**Note:** For more information about the Web Manager, see [Chapter 4: Configuration Using Web Manager](#). For more information about using CLI to access device configuration and management interface, see [Appendix A: Command Reference](#). For more information about using Web API to configure and manage the xPico Wi-Fi device, see [Chapter 5: WebAPI](#). For more information about OEM Configuration, see [Chapter 6: OEM Management](#) and [Chapter 17: Branding the xPico Wi-Fi Unit](#).

### XML Architecture and Device Control

XML is a fundamental building block for the future growth of Machine-to-Machine (M2M) networks. The xPico Wi-Fi embedded device server supports XML configuration records that make configuring the device server easy for users and administrators. XML configuration records are easy to edit with a standard text editor or an XML editor.

For a brief overview of XML, see [XML Configuration Language](#). It provides rules on basic XML syntax, a guide to the specific XML tags used, and a guide to using XML configuration records.

### XML over Serial Port

The serial port can be used to import and export XML configuration. To use the serial port in this manner refer to the set up and use of the Boot to CLI as described in [Line Settings \(Serial\) \(on page 50\)](#).

To ensure optimal performance when configuring and managing the device using XML, it is required that serial port flow control is enabled. This maybe hardware or soft flow control, which can be set up initially by means of the CLI if necessary. Lantronix recommends the use of hardware flow control to ensure the best throughput.

**Note:** The xPico Wi-Fi module itself only supports serial TTL signaling on both Lines. If used with the evaluation board (see the [xPico Embedded Device Server Evaluation Kit User Guide](#)), then Line 2 may be routed through a serial-to-USB converter via jumper settings.

The Command Line Interface can be accessed via these methods:

- ◆ Boot to CLI as described on [page 50](#).
- ◆ Permanently enable a serial port to Command Line Interface as described in [Line Settings \(on page 57\)](#).
- ◆ From the Modem Emulation serial application by entering the ATD 0 command.
- ◆ From the Mux serial application by entering the D command.

## To Configure Flow Control Options on the CLI

### Selecting Hardware Flow Control

1. Start at the `>` prompt.
2. Type `config` and press **Enter** on the keyboard to get to the `config>` prompt.
3. Type `Line 1` and press **Enter** on the keyboard to get to the `config Line 1>` prompt.
4. Type `Flow Control Hardware` and press **Enter** on the keyboard.

### Selecting Software Flow Control

1. Start at the `>` prompt.
2. Type `config` and press **Enter** on the keyboard to get to the `config>` prompt.
3. Type `Line 1` and press **Enter** on the keyboard to get to the `config Line 1>` prompt.
4. Type `Flow Control Software` and press **Enter** on the keyboard.

## To Import or Export XML Configuration

1. Connect the xPico Wi-Fi embedded device server to the PC.
2. Configure command line on line and select hardware or software flow control.
 

**Note:** *If you are using hardware flow control on line 2, make sure the line 2 flow CP roles are enabled and the hardware is wired to the xPico Wi-Fi unit. Flow control is not supported over USB. CLI Server Mode must be enabled in Web Manager before you are able to log onto a terminal emulator.*
3. Open a terminal emulator from the PC, e.g., Tera Term version 4.58.
4. Select the Com port and set the serial settings on the terminal emulator to match the appropriate line on the device server.
5. When you see the `>` prompt on the terminal emulator, type '?' to view the single character commands available.

**Figure 3-1 Single Character Commands**

```
>?
config                documentation
file system          help
status               tlog
wlan scan [network-name]  xml
exit

>
```

6. Issue `xml` command to access xml level commands.
7. Issue `xcr dump` command to dump xml configuration.
8. Copy and paste the configuration text into notepad or some other basic text editor.
9. Remove all the spaces in the script within the text editor. This basic text is the exported XML configuration and is now available for copy-paste into any xPico Wi-Fi embedded device server.

10. Make any additional changes to the configuration text to modify the XML configuration.
11. Copy and paste <CR> all of the text into the terminal emulator connected to the desired xPico Wi-Fi embedded device server, to "import" the new configuration.

**Note:** *Software flow control experiences overrun above 460800 baud.*

## XML over the Network

The XML configuration can be imported and exported using the WebAPI. Refer to [Chapter 5: WebAPI on page 29](#).

## XML Configuration Language

The xPico Wi-Fi embedded device server provides an Extensible Markup Language (XML) interface that you can use to configure xPico Wi-Fi embedded device servers. Every configuration setting, excluding XML import and export, that can be issued from the xPico Wi-Fi Web Manager and CLI can be specified using XML.

The xPico Wi-Fi embedded device server can import and export configuration settings as an XML document known as an XML Configuration Record (XCR). An XCR can be imported or exported via the CLI or the xPico Wi-Fi embedded device server filesystem. An XCR can contain many configuration settings or just a few. For example, it might change all of the configurable parameters for a xPico Wi-Fi embedded device server, or it may only change the baud rate for a single serial line. Using XCRs is a straightforward and flexible way to manage the configuration of multiple xPico Wi-Fi embedded device servers.

**Imported and exported XCRs begin with this text:**

```
<?xml version="1.0" standalone="yes"?>
<!DOCTYPE configrecord [
  <!ELEMENT configrecord (configgroup+)>
  <!ELEMENT configgroup (configitem+)>
  <!ELEMENT configitem (value+)>
  <!ELEMENT value (#PCDATA)>
  <!ATTLIST configrecord version CDATA #IMPLIED>
  <!ATTLIST configgroup name CDATA #IMPLIED>
  <!ATTLIST configgroup instance CDATA #IMPLIED>
  <!ATTLIST configitem name CDATA #IMPLIED>
  <!ATTLIST configitem instance CDATA #IMPLIED>
  <!ATTLIST value name CDATA #IMPLIED>
]>
<configrecord version = "0.1.0.1">
```

**All configgroups are positioned in the middle. Then, the xml must end with this text:**

```
</configrecord>
```

## XML Syntax

- ◆ A <configrecord> must have one or more <configgroup> elements.
- ◆ Each <configgroup> must have one or more <configitem> elements, must have a name attribute, and may have an instance attribute.
- ◆ A <configitem> element must have one or more <value> elements, must have a name attribute, and may have an instance attribute.
- ◆ A <value> element contains data and may have a name attribute.
- ◆ The name attribute identifies a group, item, or value. It is always a quoted string.
- ◆ The instance attribute identifies the specific instance when more than one instance is possible,

## Element Start and End Tags

An element typically consists of two tags: start tag and an end tag that surrounds text and other elements (element content). The start tag consists of a name surrounded by angle brackets, for example <configrecord>. The end tag consists of the same name surrounded by angle brackets, but with a forward slash preceding the name, for example </configrecord>. The element content can also contain other "child" elements.

## Element Attributes

The XML element attributes that are name-value pairs included in the start tag after the element name. The values must always be quoted, using single or double quotes. Each attribute name should appear only once in an element.

[Figure 3-2](#) shows an XML example which consists of a declaration (first line), nested elements with attributes and content.

**Figure 3-2 XML Example**

```
<configgroup name = "HTTP Server">
  <configitem name = "State">
    <value>Enabled</value>
  </configitem>
  <configitem name = "Port">
    <value>80</value>
  </configitem>
  <configitem name = "Inactivity Timeout">
    <value>5 minutes</value>
  </configitem>
  <configitem name = "Access Control" instance = "1">
    <value name = "URI"/></value>
    <value name = "AuthType">Basic</value>
    <value name = "Users">admin</value>
  </configitem>
</configgroup>
```

The xPico Wi-Fi embedded device server uses the attributes in the following subsections to label the group configuration settings.

## Record, Group, Item, and Value Tags

A `<configgroup>` is a logical grouping of configuration parameters and must contain one or more `<configitem>` elements. It must have a name attribute and may have an instance attribute.

A `<configitem>` is a specific grouping of configuration parameters relevant to its parent group. An item takes the name attribute and must contain one or more value elements. For example, the line group might have parameters such as baud rate, data bits, and parity.

A value may specify the value of a configuration parameter. It may contain the name attribute. In this example, a value of 9600 might be specified for baud rate; 7 may be specified for data bits, and even may be specified for parity.

A name attribute identifies the group, item, or value. It is always quoted (as are all XML attributes). For example, a group that contains serial port parameters has the name "line".

An instance attribute identifies which of several instances is being addressed. It is always quoted. For example, the serial port name (in the line configgroup) has the instance "1" to indicate serial port 1 or "2" to specify serial port 2.

The following figures show examples of XML configuration records and the use of the `<configrecord>`, `<configgroup>`, `<configitem>`, and `<value>` XML elements.

**Figure 3-3 XML Example**

```
<configrecord version = "0.1.0.1">
  <configgroup name = "Access Point" instance = "ap0">
    <configitem name = "SSID">
      <value>XpicoWiFi_98010B</value>
    </configitem>
    <configitem name = "Channel">
      <value>1</value>
    </configitem>
    <configitem name = "Suite">
      <value>WPA2</value>
    </configitem>
    <configitem name = "Encryption">
      <value>CCMP</value>
    </configitem>
    <configitem name = "Passphrase">
      <value>&lt;Configured&gt;</value>
    </configitem>
    <configitem name = "Mode">
      <value>Always Up</value>
    </configitem>
  </configgroup>
```

## 4: Configuration Using Web Manager

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

- ◆ [Accessing Web Manager](#)
- ◆ [Web Manager Components](#)
- ◆ [Navigating Web Manager](#)

**Note:** For more information about using XML to access device configuration and management interface, see [Configuration Using Serial Port on page 110](#). For more information about the CLI, see [Appendix A: Command Reference](#). For more information about using Web API to configure and manage the xPico Wi-Fi device, see [Chapter 5: WebAPI](#). For more information about OEM Configuration, see [Chapter 6: OEM Management](#) and [Chapter 17: Branding the xPico Wi-Fi Unit](#).

### Accessing Web Manager

To access Web Manager, perform the following steps:

1. Open a standard web browser. Lantronix supports the latest version of Internet Explorer, Mozilla Firefox, Safari and Chrome browsers.
2. Enter the IP address or hostname of the xPico Wi-Fi device in the address bar. The IP address may have been assigned manually or automatically by DHCP. If connecting via the SoftAP interface, the default IP address of the xPico Wi-Fi device server is 192.168.0.1.
3. Enter your username and password. The factory-default username is “**admin**” and the password is “**PASSWORD**” (all capitalized). The Status web page displays product information, network settings, line settings, and tunneling settings.

## Status Page

The Status page is the first to appear after you log into Web Manager. The Status page also appears when you click **Status** tab in Web Manager.

Figure 4-1 Status Page

The screenshot shows the xPico Wi-Fi Status Page. The page header includes the xPico Wi-Fi logo and the LANTRONIX logo. A navigation menu on the left lists various system functions, with 'Status' highlighted. The main content area is divided into several sections:

- Product Information:**

|                   |                        |
|-------------------|------------------------|
| Product Type:     | xPicoWifi              |
| Firmware Version: | 1.5.0.0R43             |
| Build Date:       | Feb 13 2018 (10:34:15) |
| Serial Number:    | 0080A3A00382           |
| Uptime:           | 8 days 09:58:06        |
| Permanent Config: | saved                  |
- Network Settings:**

|              |                   |
|--------------|-------------------|
| MAC Address: | 00:80:A3:A0:03:82 |
|--------------|-------------------|
- Interface ap0:**

|                 |                  |
|-----------------|------------------|
| State:          | Up               |
| SSID:           | XpicoWiFi_A00382 |
| Security Suite: | WPA2             |
| IP Address:     | 192.168.0.1/24   |
- Interface wlan0:**

|                      |                     |
|----------------------|---------------------|
| Connection State:    | Connected           |
| Active WLAN Profile: | dev_cisco3800_24ghz |
| IP Address:          | 172.19.100.79/16    |
| Default Gateway:     | 172.19.0.1          |
| Hostname:            |                     |
| Primary DNS:         | 172.19.1.1          |
| Secondary DNS:       | 172.19.1.2          |
- Line Settings:**

|         |  |
|---------|--|
| Line 1: | 9600, None, 8, 1, None<br>Protocol: Tunnel       |
| Line 2: | 9600, None, 8, 1, None<br>Protocol: Command Line |
- Tunneling:**

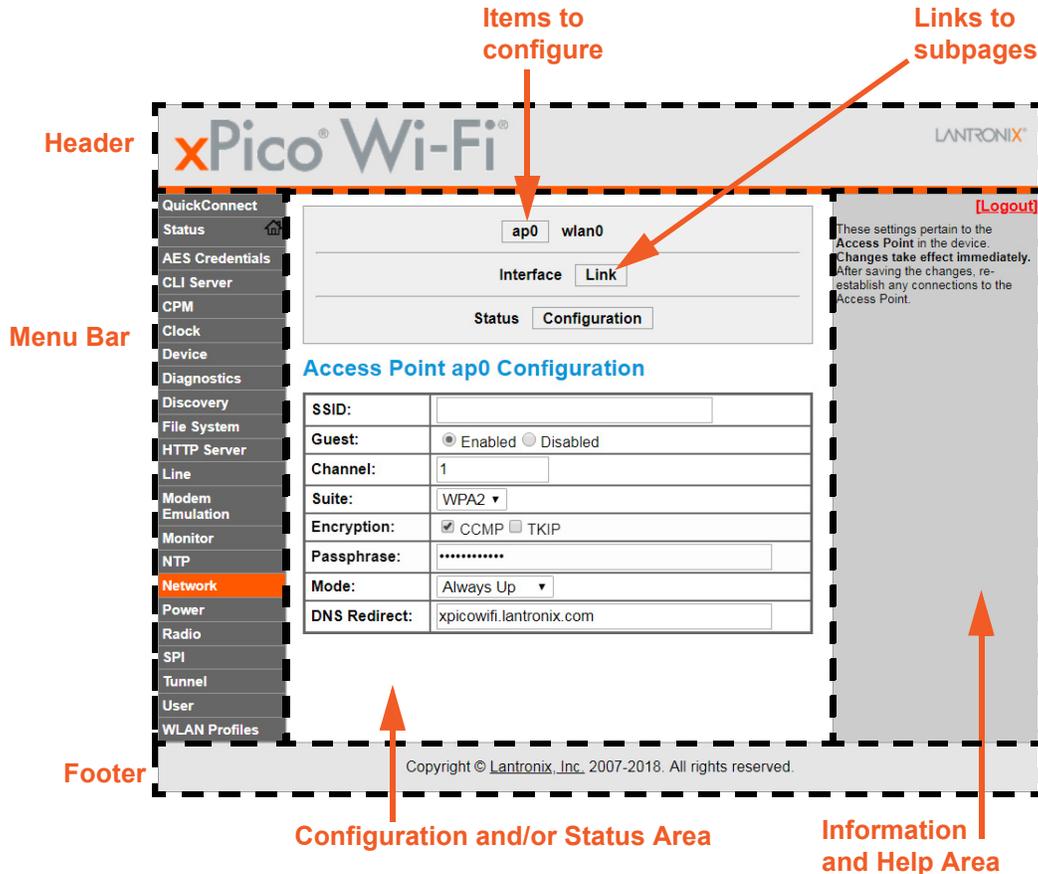
|           | Accept Mode | Connect Mode |
|-----------|-------------|--------------|
| Tunnel 1: | Waiting     | Disabled     |
| Tunnel 2: | Inhibited   | Inhibited    |

A [Logout] link is located in the top right corner. The footer contains the copyright notice: Copyright © Lantronix, Inc. 2007-2018. All rights reserved.

## Web Manager Components

The layout of a typical Web Manager page is below.

Figure 4-2 Components of the Web Manager Page



## Navigating Web Manager

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

**Note:** There may be times when you must reboot the xPico Wi-Fi unit for the new configuration settings to take effect. The chapters that follow indicate when a change requires a reboot. Anytime you reboot the unit, this operation will take some time to complete. Please wait a minimum of 10-20 seconds after rebooting the unit before attempting to make any subsequent connections.

**Table 4-3 Web Manager Pages**

| <b>Web Manager Page</b> | <b>Description</b>  | <b>See Page</b>    |
|-------------------------|---|--------------------|
| <b>Status</b>           | Shows product information, network, line status, and tunneling settings.  | <a href="#">26</a> |
| <b>AES Credentials</b>  | Lets you view, edit and delete or create an AES credential.   | <a href="#">85</a> |
| <b>CLI Server</b>       | Lets you view and configure CLI server settings and enable or disable access to the CLI server.                                   | <a href="#">76</a> |
| <b>CPM</b>              | Shows information about the Configurable Pins Manager (CPM) and how to set the configurable pins and roles to work with a device. | <a href="#">67</a> |
| <b>Clock</b>            | Lets you view and configure clock settings for keeping time.  | <a href="#">74</a> |
| <b>Device</b>           | Lets you reboot the device, restore factory defaults and upload new firmware.   | <a href="#">79</a> |
| <b>Diagnostics</b>      | Lets you perform various diagnostic procedures.   | <a href="#">81</a> |
| <b>Discovery</b>        | Lets you view and configure discovery settings.   | <a href="#">56</a> |
| <b>File System</b>      | Shows file system statistics and lets you perform file system operations.   | <a href="#">78</a> |
| <b>HTTP Server</b>      | Shows HyperText Transfer Protocol (HTTP) status and lets you change the current configuration and authentication settings.        | <a href="#">73</a> |
| <b>Line</b>             | Shows statistics and lets you change the current configuration and Command mode settings of a serial line.                        | <a href="#">57</a> |
| <b>Modem Emulation</b>  | Lets you view and configure Modem Emulation.  | <a href="#">64</a> |
| <b>Monitor</b>          | Lets you query and capture information during serial port to serial device connection.  | <a href="#">68</a> |
| <b>Network</b>          | Shows status and lets you configure the network interface.  | <a href="#">38</a> |
| <b>NTP</b>              | Lets you view the statistics from the last successful NTP server synchronization as well as configuration of simple NTP (SNTP).   | <a href="#">75</a> |
| <b>Quick Connect</b>    | Lets you scan for available network in vicinity and create WLAN profile easily.   | <a href="#">46</a> |
| <b>Power</b>            | Lets you change settings effecting power.   | <a href="#">78</a> |
| <b>Radio</b>            | Lets you configure radio modes.   | <a href="#">48</a> |
| <b>SPI</b>              | Lets you configure SPI settings.  | <a href="#">54</a> |
| <b>Tunnel</b>           | Lets you change the current configuration settings for an incoming tunnel connection.   | <a href="#">57</a> |
| <b>Users</b>            | Lets you configure Admin User password.   | <a href="#">80</a> |
| <b>WLAN Profiles</b>    | Lets you view, edit, delete and create a WLAN profile on a device.  | <a href="#">43</a> |

## 5: WebAPI

WebAPI allows access to configuration and status information of the xPico Wi-Fi embedded device server through standard HTTP requests.

**Note:** For more information about using XML to access device configuration and management interface, see [Configuration Using Serial Port on page 110](#). For more information about the CLI, see [Appendix A: Command Reference](#). For more information about using Web Manager to configure and manage the xPico Wi-Fi device, see [Chapter 4: Configuration Using Web Manager](#). For more information about OEM Configuration, see [Chapter 6: OEM Management](#) and [Chapter 17: Branding the xPico Wi-Fi Unit](#).

### Export Status Group

An HTTP POST request can be sent to the device to retrieve status information.

- ◆ **Protocol:** HTTP
- ◆ **Method:** Post
- ◆ **URL:** <http://<hostname>/export/status>

#### **Parameters:**

**optionalLine:** Optional line index for line oriented XML groups

**optionalGroupList:** Optional list of XML groups separated by semicolon. If omitted, all status groups will be returned.

#### **CURL example:**

```
curl -u admin:PASSWORD -X POST http://<hostname>/export/status
curl -u admin:PASSWORD -X POST -d "optionalGroupList=Device" http://
<hostname>/export/status
Javascript example:
myXmlHttpRequest.open(
    "POST",
    "/export/status",
    true
);
request.send(
    "optionalGroupList=Device"
);
```

### Export Configuration Group

An HTTP POST request can be sent to the device to retrieve configuration information.

- ◆ **Protocol:** HTTP
- ◆ **Method:** Post
- ◆ **URL:** <http://<hostname>/export/config>

**Parameters:**

- ◆ **optionalLine:** Optional line index for line oriented XML groups
- ◆ **optionalGroupList:** Optional list of XML groups separated by semicolon. If omitted, all configuration groups will be returned.

**CURL example:**

```
curl--digest -u admin:PASSWORD -X POST http://<hostname>/export/config
curl--digest -u admin:PASSWORD -X POST -d
"optionalGroupList=Interface:wlan0" http://<hostname>/export/config
Javascript example:
myXmlHttpRequest.open(
    "POST",
    "/export/config",
    true
);
request.send(
    "optionalGroupList= Interface:wlan0"
);
```

## Take Status Action

An HTTP POST request can be sent to the device to take a status action.

- ◆ **Protocol:** HTTP
- ◆ **Method:** Post
- ◆ **URL:** <http://<hostname>/action/status>

**Parameters:**

- ◆ **group:** Required. The status group where action is defined.
- ◆ **optionalGroupInstance:** Optional instance of status group.
- ◆ **optionalItem:** Optional item of status group where action is defined.
- ◆ **optionalItemInstance:** Optional instance of status item.
- ◆ **action:** Required. The action to be taken.

**CURL example:**

```
curl--digest -u admin:PASSWORD -X POST -d
"group=Interface&optionalGroupInstance=wlan0&action=Renew"
http://<hostname>/action/status

Javascript example:
myXmlHttpRequest.open(
    "POST",
    "/action/status",
    true
);
```

```
request.send(
    "group=Interface&optionalGroupInstance=wlan0&action=Renew"
);
```

## Import Configuration Group

An HTTP POST request can be sent to the device to set configuration.

**Protocol:** HTTP

**Method:** Post

**Content-Type:** multipart/form-data

**URL:** <http://<hostname>/import/config>

### Parameters:

**configrecord:** Content of configuration group in XML format.

CURL example (configuration is saved in a local file config.xml):

```
curl--digest -u admin:PASSWORD -X POST --form configrecord=@config.xml
http://<hostname>/import/config
```

### CURL example (configuration as part of command):

```
curl--digest -u admin:PASSWORD -X POST --form-string 'configrecord=<?xml
version="1.0" standalone="yes"?>
<!DOCTYPE configrecord [
    <!ELEMENT configrecord (configgroup+)>
    <!ELEMENT configgroup (configitem+)>
    <!ELEMENT configitem (value+)>
    <!ELEMENT value (#PCDATA)>
    <!ATTLIST configrecord version CDATA #IMPLIED>
    <!ATTLIST configgroup name CDATA #IMPLIED>
    <!ATTLIST configgroup instance CDATA #IMPLIED>
    <!ATTLIST configitem name CDATA #IMPLIED>
    <!ATTLIST configitem instance CDATA #IMPLIED>
    <!ATTLIST value name CDATA #IMPLIED>
]>
<configrecord version = "0.1.0.1">
    <configgroup name = "Access Point" instance = "ap0">
        <configitem name = "SSID">
            <value>MY DEVICE</value>
        </configitem>
    </configgroup>
</configrecord>' http://<hostname>/import/config
```

## 6: OEM Management

The xPico Wi-Fi embedded device server allows for a more protected original equipment manufacturer (OEM) configuration options. This allows an OEM to configure the xPico Wi-Fi unit with settings that can be saved and retained specifically for the OEM application (i.e. OEM factory defaults). Some of these configurations cannot be modified by any of their end users. Configuration parameters such as MAC address and region code are sensitive and designed to not be changed easily. The Wi-Fi region code has to be protected because it affects the certification requirements for the country of operation. The MAC address is also unique and must not be changed without some reasonable steps to make sure it stays unique and protected. The following section describes how to manage the protected OEM's configuration of the xPico Wi-Fi embedded device server.

### Protected Configuration Details

There are multiple options for configuring the xPico Wi-Fi device including the Web Manager, Command Line Interface (CLI) and XML Configuration Records (XCR). For the OEM protected configuration, the only configuration option is using XCRs. One advantage of the XCR configuration is that the multiple units can be configured in an automated way. The xPico Wi-Fi embedded device server can only accept XCR configuration via the CLI or through the WebAPI.

### XCR OEM Group Configuration Group

To configure the protected OEM settings you will use an XCR. The XCR will need to define a configgroup called "OEM". The XML for the configgroup = "OEM" is as follows:

```
<configrecord version = "0.1.0.1">
  <configgroup name = "OEM">
    <configitem name = "MAC Address">
      <value>00 80 A3 98 06 1C</value>
    </configitem>
    <configitem name = "Region">
      <value>United States</value>
    </configitem>
  </configgroup>
</configrecord>
```

As you can see, with the OEM Group, you can change or set the value for two different settings: MAC Address and Wi-Fi region. See below for more detail on how to configure these settings.

Please keep in mind that this XML can be read from the CLI on a serial port but the entire record is hidden when the XML configuration is exported over the Network using the WebAPI.

## OEM Group Configuration Password

The ability to change the OEM protected configuration like the MAC address and region code is protected by a password. This is to prevent unauthorized changes to these configuration parameters. The password is set in a configgroup called "OEM". The password value is controlled by the `<configitem name = "password">`. Initially the password by default is set as blank (i.e. no password). It is highly recommended that the OEM set the password to a unique value.

Here is an example of what that should look like to set a unique password:

```
<configgroup name = "OEM">
  <configitem name = "password">
    <value>Set your OEM password here</value>
  </configitem>
</configgroup>
```

Once an OEM password is set, it must be provided in the "XML Import Control" group in order for the xPico Wi-Fi to accept any changes to the OEM group. For example:

```
<?xml version="1.0" standalone="yes"?>
<!DOCTYPE configrecord [
  <!ELEMENT configrecord (configgroup+)>
  <!ELEMENT configgroup (configitem+)>
  <!ELEMENT configitem (value+)>
  <!ELEMENT value (#PCDATA)>
  <!ATTLIST configrecord version CDATA #IMPLIED>
  <!ATTLIST configgroup name CDATA #IMPLIED>
  <!ATTLIST configgroup instance CDATA #IMPLIED>
  <!ATTLIST configitem name CDATA #IMPLIED>
  <!ATTLIST configitem instance CDATA #IMPLIED>
  <!ATTLIST value name CDATA #IMPLIED>
]>
<configrecord version = "0.1.0.1">
  <configgroup name = "OEM">
    <configitem name = "Region">
      <value>Japan</value>
    </configitem>
  </configgroup>
  <configgroup name = "XML Import Control">
    <configitem name = "Password">
      <value>You provide your OEM password here</value>
    </configitem>
  </configgroup>
</configrecord>
```

The OEM password protects the OEM configgroup as well as the OEM configitem in the XML Import Control configgroup.

**Note:** Once set, keep your OEM configuration password secure. Once the OEM password and OEM configuration settings are saved, they become the new device factory defaults, overriding and erasing the original Lantronix factory default settings. The OEM configuration will no longer be able to be modified without providing the OEM password. See [“Setting OEM Configuration Defaults” on page 36](#).

## Reading and Writing the Region Code of the xPico Wi-Fi Unit

The following procedure describes how to modify the region code of an xPico Wi-Fi device server. The region codes are text strings and are used to configure the device for that region.

The available country codes are:

- ◆ United States (Default)
- ◆ Canada
- ◆ European Union
- ◆ Japan

When selected, the radio is automatically configured to the channel and transmit power levels necessary for operation in that country per the certification requirements.

### Reading the Current OEM Configuration Group from the CLI

As previously mentioned, there is only one option to read the OEM configuration record but there are two options to write it.

To read the OEM configuration from the serial port (configured for CLI) you can use the following commands to read the configuration

```
>xml
xml>xcr dump OEM
```

This will display the OEM configuration Group XML with the current settings.

### Writing the OEM Configuration Group from the CLI

To write the OEM configuration group, you can use the CLI or the WebAPI. To write the OEM configuration group using the CLI, you can write the desired OEM configgroup at any point in the CLI (there is no explicit command required). For this example, we changed the region value as follows:

```
</configitem>
  <configitem name = "Region">
    <value>Japan</value>
  </configitem>
```

To test, you can simply cut and paste the configgroup in a valid XCR into the terminal program at a CLI prompt.

```
>xml or >
```

After writing a valid XCR record, the CLI will respond with

```
Importing XML
```

WARNING: Region code change requires reboot to take effect.  
XML import completed.

>

After a reboot, the xPico Wi-Fi embedded device server will be configured for the Japan Wi-Fi settings. To make this setting become your OEM factory defaults. See the section below.

To write a new Wi-Fi region code using the WebAPI, you would use the WebAPI Import Configuration Group command.

```
Content-Type: multipart/form-data
URL: http://<hostname>/import/config
Parameters:
configrecord: configuration group in XML format.
```

For this example we will use the CURL utility and the WebAPI to set the Wi-Fi region code back to the United States. We created a file called OEMconfig.xml that contains a valid XCR record. Here is a copy of that file (the prelog has been omitted for clarity):

```
configrecord version = "0.1.0.1">
  <configgroup name = "OEM">
    <configitem name = "MAC Address">
      <value>00 80 A3 98 06 1C</value>
    </configitem>
    <configitem name = "Region">
      <value>United States</value>
    </configitem>
  </configgroup>
</configrecord>
```

The following is a sample of the CURL command you would use.

```
curl--digest -u admin:PASSWORD -X POST --form
configrecord=@OEMconfig.xml
http://<hostname>/import/config
```

The WebAPI returned the following response:

```
<!-- Automatically generated XML -->
<!DOCTYPE function [
  <!ELEMENT function (return)>
  <!ELEMENT return (result,message+)>
  <!ELEMENT result (#PCDATA)>
  <!ELEMENT message (#PCDATA)>
  <!ATTLIST function version CDATA #IMPLIED>
]>
<function version = "0.1.0.0">
  <return>
    <message>WARNING: Region code change requires reboot to take
effect.</message>
    <message>XML import completed.</message>
    <result>Succeeded</result>
  </return>
```

```
</function>
```

After a reboot, the xPico Wi-Fi embedded device server will be configured for the United States Wi-Fi settings.

## Setting OEM Configuration Defaults

It is possible for the OEM to change the default configuration settings of the xPico Wi-Fi embedded device server. This is controlled within the group "XML Import Control". To set ALL current configuration values to the default, use the configitem ="OEM" value and set that value to "Set Configuration". After writing the XML Import Control XCR to the CLI or the WebAPI, ALL current settings become your OEM factory defaults.

There are two options:

- ◆ **Set Configuration:** Sets the OEM defaults to be whatever the current product settings are.
- ◆ **Remove Configuration:** Removes the OEM defaults, leaving just Lantronix defaults.

Here is what the configitem name = "OEM" looks like in XML:

```
<configitem name="OEM">
  <value>Set Configuration</value>
OR
  <value>Remove Configuration</value>
</configitem>
```

Interesting note: the configitem ="OEM" is a hidden field in the XML Import Control group whether you read it from the WebAPI or the CLI. This is what it would look like if you could read it

```
<configrecord version="0.1.0.1">
<configgroup name="XML Import Control">
<configitem name="Restore Factory Configuration">
  <value>Disabled</value>
</configitem>
<configitem name="Reboot">
  <value>Disabled</value>
</configitem>
<configitem name="Missing Values">
  <value>Set to Default</value>
</configitem>
<configitem name="Delete WLAN Profiles">
  <value>Enabled</value>
</configitem>
<configitem name="WLAN Profile delete">
  <value name="name" />
</configitem>
</configitem>
<configitem name="OEM">
```

```
<value>Set Configuration</value>
</configitem>
</configgroup>
</configrecord>
```

**Note:** Be careful when writing the "XML Import Control" group to make sure this *configitem* is not included if you do not intend to set the default configuration.

If you are unsure about any of the device settings we recommend that you reset to (Lantronix) factory defaults first, configure your unique settings, then commit then to the OEM defaults by writing the group "XML Import Control" with the OEM item set to "Set Configuration".

After you set your OEM factory defaults, anytime a reset to factory defaults is executed the OEM default configuration will be used rather than the Lantronix factory default settings.

Import controls can set or restore factory configuration, reboot the device, determine how to manage values and manage the password setting.

### Branding the xPico Wi-Fi

Please see Chapter 17: Branding the xPico Wi-Fi Unit for information on branding your xPico Wi-Fi device server.

## 7: Wireless Network Settings

The xPico Wi-Fi embedded device server contains two network interfaces. The software-enabled Access Point interface is also called ap0, and the WLAN interface is called wlan0.

A maximum of four clients can be connected to the SoftAP interface if the STA interface is disabled. If the STA interface is enabled a maximum of three clients may be connected

The wireless network settings show the status of the Software-enabled Access Point (SoftAP) or WLAN interface/link and let you configure the settings on the device. Interface settings are related to the configuration of the IP and related protocols. Link settings are related to the physical link connection, which carries the IP traffic.

**Note:** All network settings require a reboot to take effect. Wait a minimum of 20 seconds after rebooting the unit before attempting to make any subsequent connections.

### Network ap0 Interface Configuration

Table 7-1 shows the network interface settings that can be configured. These settings apply to the Software enabled Access Point (ap0) interface.

**Table 7-1 Network Interface Settings**

| Network (ap0) Interface Settings | Description  |
|----------------------------------|--|
| <b>State</b>                     | Click to enable or disable the SoftAP. If enabled, the DHCP server will assign IP addresses to the SoftAP's clients.<br><br><b>Note:</b> A DHCP lease lasts for a day. If the IP network is managed manually, a static IP can be used outside the range of the DHCP address pool.  |
| <b>IP Address</b>                | If not using the DHCP capabilities of the device, enter the static IP address to use for the interface. You may enter it in one of the following ways: <ul style="list-style-type: none"><li>◆ Alone (i.e., 192.168.1.1)</li><li>◆ In CIDR format (i.e., 192.168.1.1/24)</li><li>◆ With an explicit mask (i.e., 192.168.1.1 255.255.255.0)</li></ul> |
| <b>MSS</b>                       | Enter the bytes for the Maximum Segment Size (MSS) as it applies to TCP connections on the Interface. This can be useful to avoid fragmentation over the network, which may be required because this device does not perform reassembly.   |

### To Configure Network ap0 Interface Settings

#### Using Web Manager

- ◆ To modify Software enabled Access Point (ap0) settings, go to **Network** on the menu and select **ap0 -> Interface -> Configuration**.

#### Using CLI

- ◆ To enter the Interface command level: `config -> Interface <ap0>`

### Using XML

- ◆ Include in your file: `<configgroup name = "Interface" instance = "ap0">`

## To View Network ap0 Interface Status

### Using Web Manager

In Network Interface Status, you can view both the current operational settings as well as the settings that would take effect upon a device reboot.

- ◆ To view current access point (ap0) settings, go to **Network** on the menu and select **ap0 -> Interface -> Status**.

### Using CLI

- ◆ To enter the Interface command level: `status -> Interface <ap0>`

### Using XML

- ◆ Include in your file: `<configgroup name = "Interface">`

## Network ap0 Link Settings

Physical link parameters can be configured for an access point (ap0) Network Interface (see [Table 7-2](#)).

**Table 7-2 Network ap0 Link Settings**

| Network ap0 Link Settings | Description  |
|---------------------------|--|
| <b>SSID</b>               | Specify the name of the wireless network (SSID) for the SoftAP. SoftAP configurations will take effect immediately.<br><br><i>Note:</i> You may connect to the SoftAP SSID from a PC or any client using a wireless connection. After a wireless connection is successfully established, access the device Web Manager from any standard web browser by entering the URL <a href="http://xpicowifi.lantronix.com">http://xpicowifi.lantronix.com</a> . Make sure to use the latest version of the web browser. |
| <b>Guest</b>              | Click to enable or disable.  |
| <b>Channel</b>            | Specify the channel for the SoftAP.<br><ul style="list-style-type: none"> <li>◆ The channel for the SoftAP will be this value if the wlan0 interface is not connected to an Access Point.</li> <li>◆ If the wlan0 interface is connected, then the channel used in that interface will be the one used for the SoftAP.</li> </ul>  |
| <b>Suite</b>              | Specify the security suite to be used for the SoftAP.<br><ul style="list-style-type: none"> <li>◆ <b>None</b> = no authentication or encryption method will be used.</li> <li>◆ <b>WPA</b> = Wi-Fi protected access</li> <li>◆ <b>WPA2</b> = robust secure network.</li> </ul>   |
| <b>Encryption</b>         | Select one or more encryption types, listed from strongest to least strong.<br><ul style="list-style-type: none"> <li>◆ <b>CCMP</b> = Uses AES as basis and is the strongest encryption option.</li> <li>◆ <b>TKIP</b> = Uses WEP as the basis, but adds extra checks and variations for added protection.</li> </ul>  |

| Network ap0 Link Settings | Description  |
|---------------------------|--|
| <b>Passphrase</b>         | Select the passphrase which may consist of a minimum of 8 and up to 63 characters.<br><br><i>Note: This configuration option becomes available only when suites WPA or WPA2 are selected. Lantronix recommends using a passphrase of 20 characters or more for maximum security. Spaces and punctuation characters are permitted. The passphrase input is not the same as ASCII input (as used on some products.) ASCII is translated directly into hexadecimal bytes according to the ASCII table, while a possibly larger passphrase is hashed into a key and provides better security through a larger range of key values.</i> |
| <b>Mode</b>               | Select the desired mode for the link connection from the drop-down menu:<br><ul style="list-style-type: none"> <li>◆ <b>Always Up:</b> when enabled, the SoftAP is always on.</li> <li>◆ <b>Triggered:</b> when enabled, the SoftAP operates in Triggered mode.</li> </ul>   |
| <b>Uptime</b>             | Enter the length of uptime for the link connection.<br><br><i>Note: This feature is available when Triggered Mode is selected above.</i>   |
| <b>DNS Redirect</b>       | Update the DNS Redirect address as desired. Blank to restore the default. May contain up to 128 characters. The DNS Redirect name will map to the IP address of the Interface. It may contain upper case, but not that DNS names are case insensitive.   |

## Triggered AP Mode

Triggered AP mode is a means to enable the xPico Wi-Fi SoftAP via a hardware signal. This allows a user to have the SoftAP operating only when an external signal/button is activated. This might be useful when power consumption is a concern yet the SoftAP is needed. One potential use is device provisioning. When triggered, the SoftAP will remain active for the configured uptime waiting for a client to connect. If no client connects before the uptime expires, the SoftAP goes back down. If one or more clients connect, the SoftAP will remain active until the last client disconnects, at which point it will go down.

Refer to [Chapter 11: Configurable Pin Manager](#) for details on how to set up the xPico Wi-Fi unit for this feature.

## To Configure Network ap0 Link Settings

### Using Web Manager

- ◆ To modify network ap0 Link information, click **Network** on the menu and select **apo > Link > Configuration**.

### Using CLI

- ◆ To enter the Access Point command level: `config -> Access Point`

### Using XML

- ◆ Include in your file: `<configgroup name = "Access Point" instance = "ap0">`

## To View Network ap0 Link Status

### Using Web Manager

In Network Link Status, you can view the current operational settings.

- ◆ To view current network ap0 settings, go to **Network** on the menu and select **ap0 -> Link -> Status**.

### Using CLI

- ◆ To enter the Access Point command level: `status -> Access Point`

### Using XML

- ◆ Look for the status header: `<statusgroup name = "Access Point" instance = "ap0">`

## Network wlan0 Interface Configuration

This page is used to configure the network wlan0 interface on the device. To see the effect of these items after a reboot, view the Status page.

**Table 7-3 Network Interface Settings**

| Network Interface Settings | Description  |
|----------------------------|--|
| <b>State</b>               | Click to enable or disable the WLAN interface.   |
| <b>DHCP Client</b>         | Click to enable or disable the DHCP client. If enabled, any configured IP address, network mask, gateway or hostname will be ignored. DHCP will auto-discover and eclipse those configured items. When DHCP fails to discover an IP address, a new address will automatically be generated using AutoIP. This address will be within the 169.254.x.x space. At boot up, after the physical link is up, the xPico Wi-Fi will attempt to obtain IP settings from a DHCP server and will periodically renew these settings with the server.<br><br><i>Note: Click renew on Interface Status page to force DHCP lease renewal.</i> |
| <b>IP Address</b>          | Enter the static IP address to use for the interface. You may enter it in one of the following ways: <ul style="list-style-type: none"> <li>◆ Alone (i.e., 192.168.1.1)</li> <li>◆ In CIDR format (i.e., 192.168.1.1/24)</li> <li>◆ With an explicit mask (i.e., 192.168.1.1 255.255.255.0)</li> </ul> <i>Note: This setting will be used if Static IP is active (DHCP Client is Off).</i>   |
| <b>Default Gateway</b>     | Enter the IP address of the router for this network.<br><br><i>Note: This setting will be used if Static IP is active (DHCP Client is Off).</i>  |
| <b>Hostname</b>            | Enter the hostname for the interface. It must begin with a letter, continue with a letter, number or hyphen, and must end with a letter or number. The device will not register the hostname with a DNS server until the next reboot.  |

| Network Interface Settings (continued) | Description  |
|--|--|
| <b>Primary DNS</b>                     | Enter the IP address of the primary Domain Name Server.<br><i>Note: This setting will be used when Static IP is active.</i>  |
| <b>Secondary DNS</b>                   | Enter the IP address of the secondary Domain Name Server.<br><i>Note: This setting will be used when Static IP is active.</i>  |
| <b>MSS</b>                             | Enter the bytes for the Maximum Segment Size (MSS) as it applies to TCP connections on the Interface. This can be useful to avoid fragmentation over the network, which may be required because this device does not perform reassembly. |

## To Configure Network wlan0 Interface Settings

### Using Web Manager

- ◆ To modify network wlan0 interface information, click **Network** on the menu and select **wlan0 > Interface > Configuration**.

### Using CLI

- ◆ To enter the Interface command level: `config -> Interface <wlan0>`

### Using XML

- ◆ Include in your file: `<configgroup name = "Interface" instance = "wlan0">`

## To View Network wlan0 Interface Status

### Using Web Manager

In Network Interface Status, you can view both the current operational settings as well as the settings that would take effect upon a device reboot.

- ◆ To view current WLAN (wlan0) settings, go to **Network** on the menu and select **wlan0 -> Interface -> Status**.

### Using CLI

- ◆ To enter the WLAN command level: `status -> interface`

### Using XML

- ◆ Not applicable.

---

## Network wlan0 Link Status

This page shows status of a Link on the device.

### To View Network wlan0 Link Status

#### *Using Web Manager*

- ◆ To view network 2 link interface information, click **Network** on the menu and select **wlan0 > Link > Status**.

#### *Using CLI*

- ◆ To enter the WLAN command level: `status -> WLAN`

#### *Using XML*

- ◆ Not Available.

## WLAN Profiles

A WLAN profile defines all of the settings necessary to establish a wireless connection with an access point (in infrastructure mode). A maximum of four profiles can exist on the xPico Wi-Fi embedded device server at a time and only one profile may be active at any given time.

The xPico Wi-Fi device supports dynamic profiles. Dynamic Profiles are the ones created via the Lantronix QuickConnect feature.

### *WLAN Profile WEP Settings*

WEP is a simple and efficient security mode encrypting the data via the RC4 algorithm. However, WEP is acknowledged to have become more vulnerable due to advances in hacking technology. For stronger security, please use WPA, or better, WPA2 with AES (CCMP). WEP is only supported on the wlan0 interface and should only be used for associating with older access points that do not have the more secure technologies.

### *WLAN Profile WPA and WPA2 Settings*

WPA is a security standard specified by the Wi-Fi Alliance and is a close derivative of an early draft of the IEEE802.11i specification. WEP was becoming vulnerable when finalizing the IEEE802.11i standard was still far away. WPA2 is a Wi-Fi technology subset of the broad IEEE802.11i standard to enforce better interoperability. The xPico Wi-Fi embedded device server is compliant with both WPA2 and IEEE802.11i.

### To Configure WLAN Profiles

You can view, edit, create or delete a WLAN profile.

#### *Using Web Manager*

- ◆ Click **WLAN Profiles** on the menu.

### Using CLI

- ◆ To enter the WLAN Profile command level: `config -> WLAN Profile`
- ◆ To enter the WLAN Profile Basic command level: `config -> WLAN Profile Basic`
- ◆ To enter the WLAN Profile Security command level: `config -> WLAN Profile Security`
- ◆ To enter the WLAN Profile Security WEP command level: `config -> WLAN Profile Security WEP`
- ◆ To enter the WLAN Profile Security WEP Key command level: `config -> WLAN Profile Security Key`
- ◆ To enter the WLAN Profile Security Advanced command level: `config -> WLAN Profile Advanced`
- ◆ To enter the WLAN Profile Security WEP command level: `config -> WLAN Profile`

### Using XML

- ◆ Include in your file: `<configgroup name = "WLAN Profile" instance = "name">`

**Table 7-4 Creating, Deleting or Enabling WLAN Profiles**

| WLAN Profile Basic Settings                       | Description  |
|---|--|
| <b>Create new WLAN Profile</b>                    | Type the name of the new profile to be created into the <b>Create new WLAN Profile</b> field. Then, click the <b>Submit</b> button which appears to create the profile. Once created, the profile name may be clicked so you may edit profile settings.  |
| <b>Delete</b> (checkbox)                          | Click the <b>Delete</b> checkbox beside the profile(s) to be deleted. Two buttons will appear: <ul style="list-style-type: none"> <li>◆ Click the <b>Apply</b> button to delete the profile for testing purposes. If the device reboots, this change will not be applied.</li> <li>◆ Click the <b>Submit</b> button to permanently delete profile(s).</li> </ul> |
| <b>View or Edit</b><br>(link to specific profile) | Click on a specific WLAN Profile name to edit the WLAN profile basic settings.   |

## To Configure WLAN Profile Settings

### Using Web Manager

- ◆ To view or edit an existing WLAN profile, click **WLAN Profiles** on the menu and select an existing profile (see [Table 7-5](#), [Table 7-6](#) and [Table 7-7](#)).

### Using CLI

- ◆ To enter the WLAN Profile command level: `config -> WLAN Profile <instance>`

### Using XML

- ◆ Include in your file: `<configgroup name = "WLAN Profile" instance = "name">`

Table 7-5 WLAN Profile Basic Settings

| WLAN Profile Basic Settings | Description                                      |
|-----------------------------|--|
| Network Name (SSID)         | Specify the name of the wireless network (SSID.) |
| State                       | Select to enable or disable this profile.        |

Table 7-6 WLAN Profile Security Settings

| WLAN Profile Security Settings | Description  |
|--------------------------------|--|
| Suite                          | Specify the security suite to be used for this profile. <ul style="list-style-type: none"> <li>◆ <b>None</b> = no authentication or encryption method will be used.</li> <li>◆ <b>WEP</b> = wired equivalent privacy</li> <li>◆ <b>WPA</b> = Wi-Fi protected access</li> <li>◆ <b>WPA2</b> = robust secure network.</li> </ul>   |
| WEP Key Size                   | Select the appropriate key size in bits. Select 40 for WEP40 and WEP64; select 104 for WEP104 and WEP128.<br><br><i>Note:</i> This option is available if WEP suite is selected above.   |
| WEP TX Key Index               | Select one of four index listing keys for transmitting data. Reception is allowed with all four keys.<br><br><i>Note:</i> For operability with some products that generate four identical keys from a passphrase, this index must be one. This option is available if WEP suite is selected above.   |
| WEP Key 1-4                    | Enter one or more encryption keys in hexadecimal format. Enter 10 hexadecimal digits (0-9, a-f) for WEP40 and 26 for WEP104. The configured keys are not shown for security reasons.<br><br><i>Note:</i> This option is available if WEP suite is selected above. Some access point devices do not support transmit key index 2, 3 and 4 for WEP.  |
| WPAX Key Type                  | Select the format of the security key.<br><br><i>Note:</i> This configuration option becomes available only when suites, WPA or WPA2 are selected.   |
| WPAX Key                       | Enter the WPAX key.<br><br><i>Note:</i> This configuration option becomes available only when suites, WPA or WPA2 are selected and the Hex key type is selected.   |
| WPAX Passphrase                | Select the password consists of up to 63 characters.<br><br><i>Note:</i> Lantronix recommends using a passphrase of 20 characters or more for maximum security. Spaces and punctuation characters are permitted. The passphrase input is not the same as ASCII input (as used on some products.) ASCII is translated directly into hexadecimal bytes according to the ASCII table, while a possibly larger passphrase is hashed into a key and provides better security through a larger range of key values. This configuration option becomes available only when suites, WEP, WPA or WPA2 are selected. |

| WLAN Profile Security Settings | Description  |
|--------------------------------|--|
| <b>WPAX Encryption</b>         | <p>Select one or more encryption types, listed from strongest to least strong. At least one selection will have to match the Access Points intended to connect with.</p> <ul style="list-style-type: none"> <li>◆ <b>CCMP</b> = Uses AES as basis and is the strongest encryption option.</li> <li>◆ <b>TKIP</b> = Uses WEP as the basis, but adds extra checks and variations for added protection.</li> </ul> <p><i>Note: In case the encryption settings on the Access Point(s) can still be chosen, the capabilities of the Access Point(s) and the other clients that need to use the network need to be taken into account. This configuration option becomes available only when suites WPA or WPA2 are selected.</i></p> |

Table 7-7 WLAN Profile Advanced Settings

| WLAN Profile Advanced Settings | Description  |
|--------------------------------|--|
| <b>TX Power Maximum</b>        | Specify the maximum transmission output power in dBm.  |
| <b>Power Management</b>        | <p>Select to <b>Enable</b> or <b>Disable</b> power management, which reduces the overall power consumption of the xPico Wi-Fi unit, but can increase latency.</p> <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = allows the xPico Wi-Fi to turn off the receiver when it is idling.</li> <li>◆ <b>Disabled</b> = keeps the receiver on at all times.</li> </ul> |
| <b>PM Interval</b>             | <p>Select number of beacons (100 msec interval) between 1 and 5. The above-mentioned latency can be up to this number "X" 100 msec.</p> <p><i>Note: This field is available for configuration when power management is enabled.</i></p>  |

## WLAN Quick Connect

Lantronix WLAN QuickConnect allows users to view and add up to four WLAN profiles from a list of up to 20 wireless devices sorted by RSSI. Details of the selected network are pre-populated, so little or no configuration is required by the user.

### To Configure WLAN Quick Connect

#### Using Web Manager

- ◆ To view or edit an existing WLAN Quick Connect settings, click **QuickConnect** on the menu.

#### Using CLI

- ◆ To enter the WLAN Profile Quick Connect command level: `config -> WLAN Profile Quick Connect`

#### Using XML

- ◆ Include in your file: `<configgroup name = "WLAN Profile" instance = "name">`

Table 7-8 WLAN Quick Connect

| WLAN Quick Connect Settings        | Description   |
|------------------------------------|---|
| <b>Network Name</b> (search field) | Enter a network name and click Scan to search for a network.  |
| <b>Scan</b> “<network SSID>”       | Perform a scan for devices within range of the xPico Wi-Fi. Including the optional network SSID limits the scan to devices configured with the specified network SSID. Omitting the network SSID performs a scan for all devices in range.  |
| <b>Network Name</b> (link)         | Lists the SSID of a network. Click a specific <b>Network Name</b> to display the Quick Connect profile. If you provide the <b>Password</b> for a specific Quick Connect Profile, you can add that profile to your list of <a href="#">WLAN Profiles</a> . Up to four WLAN profiles may be added, and only one may be connected at any given time. |
| <b>BSSID</b>                       | Lists the basic service set identifier. This is a unique 48-bits address that identifies the access point that creates the wireless network.  |
| <b>CH</b>                          | Provides the channel number of a network.   |
| <b>RSSI</b>                        | Displays an instantaneous value indicating the signal strength of the network. The best to worst signal strength is indicated by green, yellow and red respectively.<br><br><i>Note: RSSI reported in scan results is a single sampling.</i>  |
| <b>Security Suite</b>              | Lists the security suite of a network (e.g., WEP, WPA, WPA2).   |

### Hidden Access Points

SSIDs can be hidden for a particular access point (AP). In this case, QuickConnect will display a blank table entry for that device. QuickConnect indicates there is an access point present during a scan. Knowledge of the SSID and the passphrase are required for connection to a 'hidden' access point.

It is possible to connect to an AP with a hidden SSID if the SSID is known by entering the SSID in the **Network** field of the QuickConnect page and clicking **Scan**. The xPico Wi-Fi unit then performs a directed scan for the selected network. The scan will produce a list of all in-range APs with that SSID. From this point, click on the desired entry in the list, fill in the required details, and submit the changes.

### Lantronix Smart Connect EasyWEP

Lantronix recommends that you use WPA2 with AES encryption for all Wi-Fi networks. However your device might be deployed into a legacy network that uses the less-secure WPA with TKIP encryption, or WEP. For that reason, the xPico Wi-Fi supports all three methods for the Client connection.

WEP requires a key of either 10 (WEP64) or 26 (WEP128) hexadecimal digits. Because such a key is difficult for end users to remember, Access Point manufacturers allow users to enter a passphrase instead. Since the passphrase to hexadecimal key conversion is not part of the WEP specification, different Access Point manufacturers chose different conversion algorithms. Lantronix has identified 32 different algorithms and permutations that Access Points use.

The Lantronix Smart Connect EasyWEP feature takes care of managing the different conversion algorithms so that your users can enter their passphrase and are not required to use a hexadecimal key to connect to their WEP network. The Smart Connect EasyWEP feature uses the

xPico Wi-Fi's WebAPI to accept a passphrase, and then tries each known conversion algorithm to try to establish a connection to the Access Point. When it finds the conversion algorithm that completes the connection, it saves the WLAN Profile into flash with the correct hexadecimal key for future use.

The following is an example application of using the WebAPI to trigger the SmartConnect EasyWEP:

```
$ curl--digest -u admin:PASSWORD -X POST -d
"ajax=WLANSmartConnect&ssid=ejl-wep&passphrase=testpass" http://
<hostname>
```

Where IP Address, ssid and passphrase are user inputs.

The response is ajax xml which logs progress and error messages.

**Note:** It can take 30 seconds to try each transform method supported. There may be existing Access Points that use proprietary key generation algorithms which may not be supported by the Lantronix Smart Connect EasyWEP.

## Radio Configuration

The xPico Wi-Fi module can be configured for BGN, BG or B radio modes.

**Table 7-9 Radio Settings**

| Radio Commands          | Description   |
|-------------------------|---|
| <b>Modes</b>            | Select a radio mode: <ul style="list-style-type: none"> <li>◆ <b>Disabled:</b> holds the Radio in low power.</li> <li>◆ <b>Enabled:</b> allows the Radio to operate.</li> <li>◆ <b>Triggered:</b> waits for CPM Role, "Radio Trigger", to become active. Then the Radio stays up indefinitely.</li> </ul> <p><b>Note:</b> If Radio is disabled or not yet triggered, this inhibits both ap0 and wlan0 from operating.</p> |
| <b>Keep Alive</b>       | Select to enable or disable. Enabling Keep Alive causes a Null-Function Data frame to be sent on wlan0 once per second to keep the link up.   |
| <b>Max Volley Delay</b> | Enter the number of maximum volley delay in seconds or minutes. While wlan0 is disconnected, it scans in turn for each WLAN Profile. One scan per profile comprises a volley. The interval delay is doubled after failure to join, subject to the Max Volley Delay. <p><b>Warning:</b> Short delay will compromise ap0 performance; ap0 cannot communicate while the radio is scanning.</p>                               |
| <b>Scan Period</b>      | Enter the Scan Period in seconds and/or minutes. The Scan Period is the time between scans looking for a roaming candidate.   |
| <b>Trigger Delta</b>    | Enter the device Trigger Delta in dBI. A device with RSSI Trigger Delta higher than the current Access Point is a roaming candidate.  |
| <b>RSSI Floor</b>       | Enter the device RSSI Floor in dBI. When the signal drops below the RSSI Floor, the radio attempts to roam.   |

## To View or Configure Radio

### *Using Web Manager*

- ◆ To view configure radio, click **Radio** in the menu.

### *Using CLI*

- ◆ To enter the Radio command level: `config -> radio`

### *Using XML*

- ◆ Include in your file: `<configgroup name = "Radio">`

## 8: Interface Settings

This section describes the configuration and use of the line and host interfaces for the xPico Wi-Fi embedded device server.

### Line Settings (Serial)

The Line Settings allow configuration of the serial lines (ports). Some settings may be specific to only certain lines. Such settings are noted below.

**Table 8-1 Line Configuration Settings**

| Line Settings       | Description   |
|---------------------|---|
| <b>Name</b>         | Enter a name or short description for the line, if desired. By default, there is no name specified. A name that contains white space must be quoted.  |
| <b>State</b>        | Select to <b>Enable</b> or <b>Disable</b> the operational state of the Line. The default is an enabled state.   |
| <b>Protocol</b>     | Set the operational protocol for the Line. The default is <b>Tunnel</b> for Line 1 and <b>Command Line</b> for Line 2. Choices are: <ul style="list-style-type: none"><li>◆ <b>Command Line</b></li><li>◆ <b>Modem Emulation</b></li><li>◆ <b>Monitor</b></li><li>◆ <b>Mux</b></li><li>◆ <b>None</b></li><li>◆ <b>Trouble Log</b></li><li>◆ <b>Tunnel</b> = Serial Network tunneling protocol</li></ul> |
| <b>Baud Rate</b>    | Set the Baud Rate (speed) of the Line. The default is <b>9600</b> .<br>A custom speed or any set speed between 1200 and 921600 may be selected: 1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 115200, 230400, 460800, 921600. If a custom speed is selected, indicate the bits per second in the field which appears.   |
| <b>Parity</b>       | Set the Parity of the Line. The default is <b>None</b> .<br><b>Note:</b> Serial lines do not support the following Data Bit/Parity combinations:<br>a) 7 Data Bits with No Parity and 1 Stop Bit.<br>b) 8 Data Bits with 2 Stop Bits.   |
| <b>Data Bits</b>    | Set the number of data bits for the Line. The default is <b>8</b> .<br><b>Note:</b> Serial lines do not support the following Data Bit/Parity combinations:<br>a) 7 Data Bits with No Parity and 1 Stop Bit.<br>b) 8 Data Bits with 2 Stop Bits.  |
| <b>Stop Bits</b>    | Set the number of stop bits for the Line. The default is <b>1</b> .   |
| <b>Flow Control</b> | Set the flow control for the Line. The default is <b>None</b> . Hardware flow control is only supported on Line 1.  |
| <b>Xon Char</b>     | Specify the Xon Character which is used when Flow Control is set to Software. Set the prefix in one of the three ways: <ul style="list-style-type: none"><li>◆ Prefix decimal with a backslash (\17)</li><li>◆ Prefix hexadecimal with 0x (0x11)</li><li>◆ Prefix control character with &lt;control&gt; (&lt;control&gt;Q)</li></ul>   |

| Line Settings    | Description  |
|------------------|--|
| <b>Xoff Char</b> | Specify the Xoff Character which is used when Flow Control is set to Software. Set the prefix in one of the three ways: <ul style="list-style-type: none"> <li>◆ Prefix decimal with backslash (\19)</li> <li>◆ Prefix hexadecimal with 0x (0x13)</li> <li>◆ Prefix control character with &lt;control&gt; (&lt;control&gt;S)</li> </ul> |
| <b>Gap Timer</b> | Set the Gap Timer delay to Set the number of milliseconds to pass from the last character received before the driver forwards the received serial bytes. By default, the delay is four character periods at the current baud rate (minimum 1 msec). Gap Timer range is 1 to 5000 milliseconds.   |
| <b>Threshold</b> | Set the number of threshold bytes which need to be received in order for the driver to forward received characters. Default value is 56 bytes.   |

## To Configure Line Settings

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

### Using Web Manager

- ◆ To configure a specific line, click **Line** in the menu and select **Line 1 -> Configuration** ([Table 8-1](#)).

### Using CLI

- ◆ To enter the Line command level: `config -> Line <1>`

### Using XML

- ◆ Include in your file: `<configgroup name = "Line" instance = "1">`

## To View Line Status

### Using Web Manager

- ◆ To view statistics for a specific line, click **Line** in the menu and select **Line 1 -> Status**.

### Using CLI

- ◆ To enter the Line command level: `config -> Line <1>`

### Using XML

- ◆ Look for the status header: `<statusgroup name = "Line" instance = "1">`

## Serial Command Mode

The serial port can be configured to operate in command mode permanently or to be triggered under specified conditions. See the `line <line>` level command description for more information.

## Boot to CLI

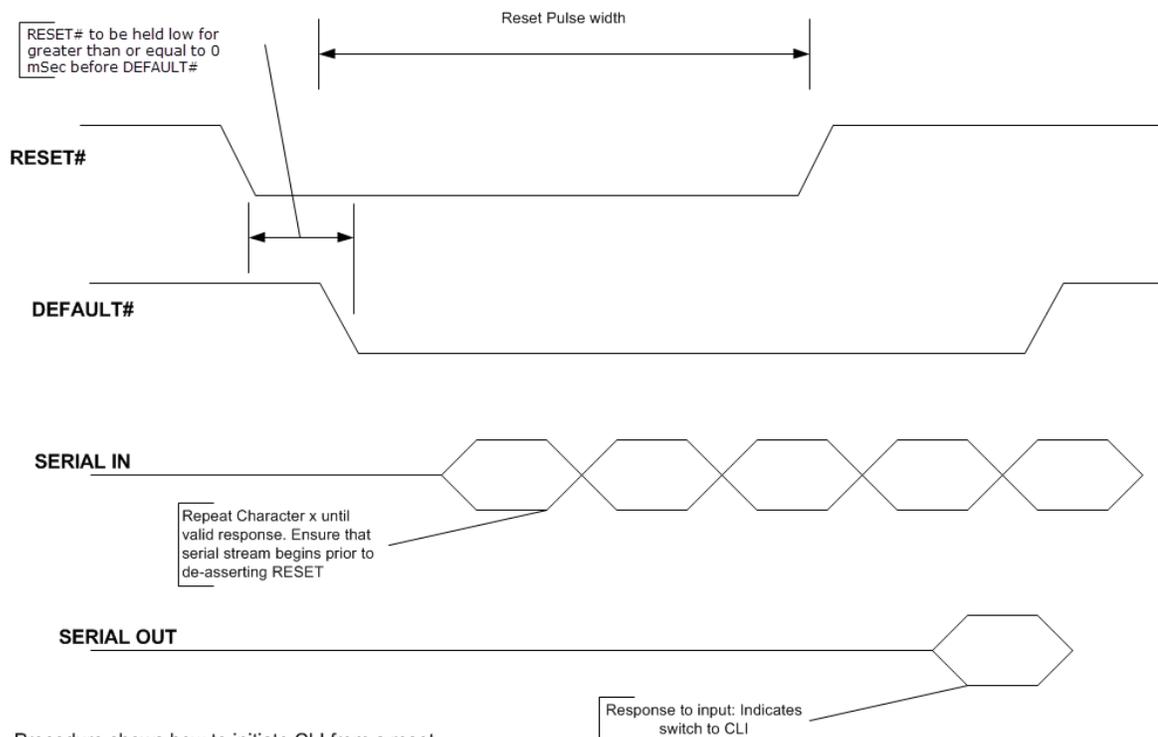
The Boot to CLI feature allows a host to have initial access to the status and configuration CLI via a single serial port that is subsequently used for Tunnel or another application. Examples of this mode would be to allow loading of a region code using the OEM group configuration, to allow the user to switch the line protocol to modem emulation or other required default configuration parameter etc.

Regardless of the configured settings, the CLI can be accessed via Line 1 using fixed settings and the "Boot to CLI" procedure. The original configured line settings will be restored once the user exits the CLI, unless any Line 1 settings are changed within the CLI.

To configure the Lantronix xPico Wi-Fi embedded device server locally using a serial port:

**Note:** *The xPico Wi-Fi embedded device server requires that flow control be used on the serial port when importing XML.*

1. Connect a terminal or a PC running a terminal emulation program host to Line 1 of the xPico Wi-Fi embedded device server's serial ports.
  2. Configure the terminal host to the following settings:
    - 9600 baud
    - 8-bit
    - No parity
    - 1 stop bit
  3. Power off the device.
  4. Follow the Boot to CLI procedure referring to the timing diagram shown below Get into the serial backdoor as follows:
    - a. While asserting the defaults signal,
    - b. Reset the device while sending x, y, or z ASCII characters.
    - c. When the incoming characters are recognized, a prompt in the following form will be seen:  
`xPicoWifi <MAC ADDRESS>`
    - d. Release the default line.
- OR**
- a. While asserting the defaults signal,
  - b. Reset the device while sending the ASCII ! character until it is echoed back.
  - c. Then release the defaults line, and enter xyz.
5. Use CLI to enable hardware or software flow control (required in order to import XML over the serial port.)



Procedure shows how to initiate CLI from a reset.  
Once initiated a user can then make any configuration changes.

The Host may query the device or change configuration without time limitation. The host exits from the Command Line Interface (via the "exit" command) and subsequent characters are directed to the Tunnel or other application (depending on the Line "Protocol" setting). When the Tunnel closes, the device shuts down (if Power Management has enabled the specific Tunnel application) and the sequence can repeat. The Host can see the message "Command Line started" when the device boots up.

## Escape Characters

There are three escape codes that can be used with the Boot to CLI procedure. These are the ASCII characters 'X', 'Y' and 'Z' (not case sensitive). The choice of code is dependent upon how the CLI is to be used. The 'X' character is intended to be used if the CLI requires human intervention; the response to the 'X' character is the device identifier string followed by a prompt to continue:

```
xPicoWifi <MAC ADDRESS>
Press <enter> to continue>
```

Once a newline is sent, the CLI prompt will appear.

The 'Y' and 'Z' characters are intended for use when there is automated intervention. The response in both cases is just the device identifier string. As with the 'X' escape sequence, a subsequent newline will result in the CLI prompt.

In addition to the 'X', 'Y' and 'Z' characters, the escape string '!xyz' is also recognized. The procedure starts similar to the one described above: assert the default signal and send a single character, '!' in this case. Once the '!' is recognized, it will be echoed back by the device. At this point, de-assert the defaults line and send the 'xyz' string; the device identifier string will be presented as it is with the 'X' and 'Y' escape modes.

Depending on the escape sequence used, a prompt may also be presented. The Host may query the device or change configuration without time limitation. The host exits from the Command Line Interface (via the "exit" command) and subsequent characters are directed to the Tunnel or other application (depending on the Line "Protocol" setting). When the Tunnel closes, the device shuts down (if Power Management has enabled the specific Tunnel application) and the sequence can repeat. The Host can see the message "Command Line started" when the device boots up.

This feature applies only to Serial Line 1 and not to Serial Line 2.

### Device Recovery

The Boot to CLI procedure can also serve as a device recovery method, the Command Line Interface will come up using default Line settings (NOT any user configured settings). Any changes to the Line settings take place immediately, replace any previous stored settings, and affect the CLI operation. Upon exit from the CLI, the Line will use configured settings (which could be different if the CLI session has not made changes to the Line configuration) and apply the designated Line Protocol.

## Serial Peripheral Interface (SPI) Settings

SPI settings pertaining to the bus master device can be modified in the xPico Wi-Fi unit. SPI settings, like line settings, allow for the selection of a protocol to be used with SPI. Changes take effect immediately.

**Table 8-2 SPI Configuration Settings**

| Line Settings           | Description   |
|-------------------------|---|
| <b>Name</b>             | Enter a name or short description for the line, if desired. By default, there is no name specified. This name is for display only.  |
| <b>State</b>            | Select to enable or disable the SPI.  |
| <b>Protocol</b>         | Select the operational protocol for connection to the SPI: <ul style="list-style-type: none"> <li>◆ <b>None</b>: selects no application to connect to the SPI.</li> <li>◆ <b>Monitor</b>: selects Monitor application to connect to the SPI.</li> </ul>   |
| <b>Target Speed</b>     | Set the target clock speed of the SPI in Hz (range is 234.375 KHz - 30 MHz). The target speed may be lowered to the closest operating speed capability of the device. If so, a warning will be noted. 0 or clearing the selection selects the minimum speed.  |
| <b>Idle Clock Level</b> | Select the level of the clock or clock polarity (CPOL) when the clock is idle: <ul style="list-style-type: none"> <li>◆ <b>Low</b>: the idle clock is at a low level. This is equivalent to CPOL=0.</li> <li>◆ <b>High</b>: the idle clock is at a high level. This is equivalent to CPOL=1.</li> </ul>                         |
| <b>Clock Edge</b>       | Select the clock edge or clock phase (CPHA) for latching data: <ul style="list-style-type: none"> <li>◆ <b>First</b>: each bit is latched on the first edge of the clock. This is equivalent to CPHA=0.</li> <li>◆ <b>Second</b>: each bit is latched on the second edge of the clock. This is equivalent to CPHA=1.</li> </ul> |
| <b>Bits Per Word</b>    | Select the number of bits per word to transfer. Choices in drop-down menu are 8 or 16.  |

| Line Settings  | Description  |
|----------------|--|
| First Transfer | Select the first transfer bit of each word. Choices in the drop-down menu include: <ul style="list-style-type: none"> <li>◆ Most Significant Bit</li> <li>◆ Least Significant Bit</li> </ul> |

## To Configure SPI Settings

### Using Web Manager

- ◆ To configure the SPI bus master device settings, click **SPI** in the menu and select **Configuration**.

### Using CLI

- ◆ To enter the SPI command level: `config -> SPI`

### Using XML

- ◆ Include in your file: `<statusgroup name = "SPI" instance = "1">`

## To View SPI Status

### Using Web Manager

- ◆ To view the current status and statistics for the SPI bus master device, click **SPI** in the menu and select **Status**.

### Using CLI

- ◆ To enter the SPI command level: `status -> SPI`

### Using XML

- ◆ Include in your file: `<statusgroup name = "SPI" instance = "1">`

## Lantronix Query Port

The xPico Wi-Fi embedded device server supports a query port discovery service. The query port is a Lantronix proprietary discovery protocol which implements a simple protocol on port 0x7FFE (30718). This service can be used by Lantronix network tools such as the *Lantronix DeviceInstaller™ utility* and *Com Port Redirector*. See <http://www.lantronix.com/support/downloads/> for more information. The port is simply enabled or disabled via the Query Port Configuration web page.

**Note:** *Certain aspects of the DeviceInstaller utility are not supported as the xPico Wi-Fi device does not support TFTP.*

## Discovery

Discovery status for ap0 and wlan0 can be viewed and configured utilizing the Lantronix discovery protocol server. Changes to discovery settings take effect immediately.

**Table 8-3 Discovery Settings**

| Discovery Settings | Description                            |
|--------------------|--|
| State              | Select to enable or disable discovery. |

### To Configure Discovery Settings

#### Using Web Manager

- ◆ To configure Discovery settings for ap0, click **Discovery** in the menu and select **ap0 > Configuration**.
- ◆ To configure Discovery settings for wlan0, click **Discovery** in the menu and select **wlan0 > Configuration**.

#### Using CLI

- ◆ To enter the Discovery command level: `config -> Discovery`

#### Using XML

- ◆ Include in your file: `<configgroup name = "Discovery">`

## 9: Tunnel Settings

Serial tunneling allows serial devices to communicate over a network, without "being aware" of the devices which establish the network connection between them. Tunneling parameters are configured using the Tunnel menu and submenus in Web Manager as described in this chapter.

### Tunnel Settings

The Tunnel settings allow you to configure how the Serial-Network tunneling operates.

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

### Line Settings

These serial settings for the tunnel apply to the Serial Line interface. The Line Settings and Protocol are displayed for informational purposes and must be configured from the Line settings.

**Table 9-1 Tunnel Line Settings**

| Tunnel Serial Settings | Description   |
|------------------------|---|
| Line Settings          | Line Settings information here is display only. Go to the section, <a href="#">To Configure Line Settings</a> to modify these settings.   |
| Protocol               | Protocol information here is display only. Go to the section, <a href="#">To Configure Line Settings</a> to modify these settings.  |
| DTR                    | Select the DTR conditions in which Data Terminal Ready control signal on the Serial Line is asserted. <ul style="list-style-type: none"><li>◆ <b>Asserted while connected</b><br/>(Causes DTR to be asserted whenever either a connect or an accept mode tunnel connection is active).</li><li>◆ <b>Continuously asserted</b></li><li>◆ <b>Unasserted</b></li></ul> |

### To View Tunnel Serial Settings

#### Using Web Manager

- ◆ To view the Serial Settings for a specific tunnel, click **Tunnel** in the menu and select **Tunnel 1 -> Line**.

#### Using CLI

- ◆ To enter the Tunnel command level: `config -> Tunnel`
- ◆ To enter the Tunnel Accept command level: `config -> Tunnel Accept`
- ◆ To enter the Tunnel Line command level: `config -> Tunnel Line`
- ◆ To enter the Tunnel Connect command level: `config -> Tunnel Connect`
- ◆ To enter the Tunnel Connect Host command level: `config -> Tunnel Connect Host`

- ◆ To enter the Tunnel Disconnect command level: `config -> Tunnel Disconnect`
- ◆ To enter the Tunnel Packing command level: `config -> Tunnel Packing`

### Using XML

- ◆ Include in your file `<configgroup name = "Tunnel Accept">`
- ◆ Include in your file `<configgroup name = "Tunnel Line">`
- ◆ Include in your file `<configgroup name = "Tunnel Connect">`
- ◆ Include in your file `<configgroup name = "Tunnel Disconnect">`
- ◆ Include in your file `<configgroup name = "Tunnel Packing">`

### Packing Mode

With Packing, data from the serial Line is not sent over the network immediately. Instead, data is queued and sent in segments, when either the timeout or byte threshold is reached. Packing applies to both Accept and Connect Modes.

**Table 9-2 Tunnel Packing Mode Settings**

| Tunnel Packing Mode Settings | Description  |
|------------------------------|--|
| <b>Mode</b>                  | Configure the Tunnel Packing Mode. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Disable</b> = Data not packed.</li> <li>◆ <b>Timeout</b> = data sent after timeout occurs.</li> <li>◆ <b>Send Character</b> = data sent when the Send Character is read on the Serial Line.</li> </ul>   |
| <b>Timeout</b>               | Set the timeout value, in milliseconds, after the first character is received on the serial line, before data is sent on the network. Valid range is 1 to 30000 milliseconds. Default is 1000.<br><br><i>Note: This configuration option becomes available when Timeout is the selected Mode.</i>  |
| <b>Threshold</b>             | Set the threshold (byte count). If the received serial data reaches this threshold, then the data will be sent on the network. Valid range is 100 to 1450 bytes. Default is 512.<br><br><i>Note: This configuration option becomes available when Timeout is the selected Mode.</i>  |
| <b>Send Character</b>        | Enter Control Characters in any of the following forms: <ul style="list-style-type: none"> <li>◆ <code>&lt;control&gt;J</code></li> <li>◆ <code>0xA</code> (hexadecimal)</li> <li>◆ <code>\10</code> (decimal)</li> </ul> If used, the Send Character is a single printable character or a control character that, when read on the Serial Line, forces the queued data to be sent on the network immediately.<br><br><i>Note: This configuration option becomes available when Send Character is the selected Mode.</i> |
| <b>Flush Send Character</b>  | Click to enable or disable.  |

| Tunnel Packing Mode Settings (continued) | Description  |
|--|--|
| <b>Trailing Character</b>                | <p>Enter Control Characters in any of the following forms:</p> <ul style="list-style-type: none"> <li>◆ &lt;control&gt;J</li> <li>◆ 0xA (hexadecimal)</li> <li>◆ \10 (decimal).</li> </ul> <p>If used, the Trailing Character is a single printable character or a control character that is injected into the outgoing data stream right after the Send Character. Disable the Trailing Character by blanking the field (setting it to &lt;None&gt;).</p> <p><i>Note: This configuration option becomes available when Send Character is the selected Mode.</i></p> |

## To Configure Tunnel Packing Mode Settings

### Using Web Manager

- ◆ To configure the Packing mode for a specific tunnel, click **Tunnel** in the menu and select **Tunnel 1 -> Packing**.

### Using CLI

- ◆ To enter the Tunnel command level: `config -> Tunnel <instance> -> Packing`

### Using XML

- ◆ Include in your file: `<configgroup name = "Tunnel Packing" instance = "1">`

## Accept Mode

In Accept mode, the xPico Wi-Fi listens (waits) for incoming connections from the network. A remote node on the network initiates the 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 port 2.

Serial data can still be received while waiting for a network connection, keeping in mind serial data buffer limitations.

**Table 9-3 Tunnel Accept Mode Settings**

| Tunnel Accept Mode Settings | Description   |
|-----------------------------|---|
| <b>Mode</b>                 | <p>Set the method used to start a tunnel in Accept mode. Choices are:</p> <ul style="list-style-type: none"> <li>◆ <b>Disable</b> = do not accept an incoming connection.</li> <li>◆ <b>Always</b> = accept an incoming connection (<i>default</i>).</li> <li>◆ <b>Any Character</b> = start waiting for an incoming connection when any character is read on the serial line.</li> <li>◆ <b>Start Character</b> = start waiting for an incoming connection when the start character for the selected tunnel is read on the serial line.</li> <li>◆ <b>Modem Control Asserted</b> = start when the modem control pin is asserted on the serial line.</li> </ul> |

| Tunnel Accept Mode Settings (continued) | Description   |
|---|---|
| <b>Local Port</b>                       | Set the port number for use as the network local port. The default local port is 10001 for serial port 1, and 10002 for serial port 2..   |
| <b>Protocol</b>                         | Select the TCP type for use with Accept Mode.   |
| <b>Credential</b>                       | Name the credential associated with the selected protocol. Configure the named credential on a separate page. A credential typically contains keys, certificates, passwords or usernames required for connection using the selected protocol.   |
| <b>Start Character</b>                  | <p>Enter the start character which will enable the tunnel to listen for a network connection. The start character may be designated as a single printable character or as a control character. Control characters may be input in any of the following forms:</p> <p>&lt;control&gt;J or 0xA (hexadecimal) or \10 (decimal)</p> <p><i>Note: This configuration option becomes available when Start Character is the selected Mode.</i></p>  |
| <b>Flush Start Character</b>            | <p>Enable or disable the flush start character:</p> <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = prevents forwarding of a start character from the Line into the network.</li> <li>◆ <b>Disabled</b> = the flush start character allows forwarding of a start character from the line into the network.</li> </ul> <p><i>Note: This configuration option becomes available when Start Character is the selected Mode.</i></p>  |
| <b>Flush Line</b>                       | <p>Set whether the serial line data buffer is flushed upon a new network connection. Choices are:</p> <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = serial data buffer is flushed on network connection</li> <li>◆ <b>Disabled</b> = serial data buffer is not flushed on network connection (default)</li> </ul>   |
| <b>Block Line</b>                       | <p>Set whether Block Line is enabled for debugging purposes. Choices are:</p> <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = if Enabled, incoming characters from the serial line will not be forwarded to the network. Instead, they will be buffered and will eventually flow off the serial line if hardware or software flow control is configured.</li> <li>◆ <b>Disabled</b> = this is the default setting; incoming characters from the Serial Line are sent into the network. Any buffered characters are sent first.</li> </ul> |
| <b>Block Network</b>                    | <p>Set whether Block Network is enabled for debugging purposes. Choices are:</p> <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = if Enabled, incoming characters from the network will not be forwarded to the Serial Line. Instead, they will be buffered and will eventually flow off the network side.</li> <li>◆ <b>Disabled</b> = this is the default setting; incoming characters from the network are sent on the Serial Line. Any buffered characters are sent first.</li> </ul>  |

| Tunnel Accept Mode Settings (continued) | Description  |
|---|--|
| <b>Password</b>                         | <p>Enter a password. This password can be up to 31 characters in length and must contain only alphanumeric characters and punctuation. When set, clients must send the correct password string to the unit within 30 seconds from opening network connection in order to enable data transmission. The password sent to the unit must be terminated with one of the following:</p> <ul style="list-style-type: none"> <li>◆ 0A (Line Feed)</li> <li>◆ 00 (Null)</li> <li>◆ 0D 0A (Carriage Return/Line Feed)</li> <li>◆ 0D 00 (Carriage Return/Null)</li> </ul> <p>If, <b>Prompt for Password</b> is set to <b>Enabled</b> and a password is provided, the user will be prompted for the password upon connection.</p> |

## To Configure Tunnel Accept Mode Settings

### Using Web Manager

- ◆ To configure the Accept Mode for a specific tunnel, click **Tunnel** in the menu and select **Tunnel 1 -> Accept**.

### Using CLI

- ◆ To enter the Tunnel command level: `config -> Tunnel <instance> -> Accept`

### Using XML

- ◆ Include in your file: `<configgroup name = "Tunnel Accept" instance = "1">`

## Connect Mode

Specifies the conditions for connecting any Accept Mode connection that may be established locally.

**Table 9-4 Tunnel Connect Mode Settings**

| Tunnel Connect Mode Settings | Description   |
|------------------------------|---|
| <b>Mode</b>                  | <p>Select the method to start the Connect Tunnel:</p> <ul style="list-style-type: none"> <li>◆ <b>Disable</b>: never started.</li> <li>◆ <b>Always</b>: always started</li> <li>◆ <b>Any Character</b>: started when any character is detected on the Serial Line</li> <li>◆ <b>Start Character</b>: started when the Start Character is detected on the Serial Line.</li> <li>◆ <b>Modem Control Asserted</b>: started when the modem control pin is asserted on the serial line.</li> </ul> |
| <b>Local Port</b>            | <p>View and if desired, override the default Local Value values.</p> <ul style="list-style-type: none"> <li>◆ Local port default values: Tunnel 1 is 10001 and Tunnel 2 is 10002.</li> <li>◆ Blank the display field to restore to default random setting.</li> </ul>   |

| Tunnel Connect Mode Settings             | Description  |
|--|--|
| <b>Host &lt;Number&gt; (Edit button)</b> | <p>Lists existing hosts, if any for viewing and editing.</p> <ul style="list-style-type: none"> <li>◆ Click the <b>Edit</b> button beside a particular host to view and edit Host fields: <ul style="list-style-type: none"> <li>➢ Address</li> <li>➢ Port</li> <li>➢ Protocol</li> <li>➢ Initial Send</li> </ul> </li> <li>◆ Make any changes, as desired in the Address, Port and Protocol fields and click <b>Submit</b> to save.</li> <li>◆ Up to 2 hosts can be established. Additional hosts become available for editing/submitting as a host is edited.</li> </ul> |
| <b>Connections</b>                       | <p>Select the type of connection.</p> <ul style="list-style-type: none"> <li>◆ <b>Sequential:</b> connections for tunneling will begin from host 1 and proceed in sequence until a connection is accepted.</li> <li>◆ <b>Simultaneous:</b> all hosts accepting connections will be connected.</li> <li>◆ <b>Round-Robin:</b> the tunnel connection attempts to start with the host after whichever host had previously connected.</li> </ul>   |
| <b>Reconnect Time</b>                    | <p>Enter the reconnection time, which specifies how long the xPico Wi-Fi device server will wait in seconds before trying to reconnect to the remote host after a failed attempt or closed connection. Blank the display field to restore the default.</p>   |
| <b>Flush Line</b>                        | <p>Select to enable or disable the flush line at the time a connection is established with the network.</p> <ul style="list-style-type: none"> <li>◆ <b>Enabled:</b> buffered characters from the serial line will be discarded when a connection is established.</li> <li>◆ <b>Disabled:</b> any characters received on the serial line will be buffered and sent after a connection is established.</li> </ul>   |
| <b>Block Line</b>                        | <p>Select to enable or disable the block line, which is used for debugging purposes.</p> <ul style="list-style-type: none"> <li>◆ <b>Enabled:</b> incoming characters from the serial line will not be forwarded to the network but will be buffered and will eventually flow off the serial line, if hardware or software flow control is configured.</li> <li>◆ <b>Disabled:</b> incoming characters from the serial line are sent to the network. Any buffered characters are sent first. This is the “normal” setting.</li> </ul>                                      |
| <b>Block Network</b>                     | <p>Select to enable or disable the block network, which is used for debugging purposes.</p> <ul style="list-style-type: none"> <li>◆ <b>Enabled:</b> incoming characters from the network will not be forwarded to the serial line but will be buffered and eventually flow off the network side.</li> <li>◆ <b>Disabled:</b> incoming characters from the network are sent on into the serial line. Any buffered characters are sent first. This is the “normal” setting.</li> </ul>  |

## To Configure Tunnel Connect Mode Settings

### Using Web Manager

- ◆ To configure the Disconnect Mode for a specific tunnel, click **Tunnel** in the menu and select **Tunnel 1 -> Connect**.

### Using CLI

- ◆ To enter the Tunnel command level: `config -> Tunnel <instance> -> Connect`

### Using XML

- ◆ Include in your file: `<configgroup name = "Tunnel Connect" instance = "1">`

### Disconnect Mode

This capability specifies the optional conditions for disconnecting any Accept Mode connection that may be established. If any of these conditions are selected but do not occur and the network disconnects from the device, a Connect Mode connection will attempt to reconnect. However, if none of these conditions are selected, a closure from the network is perceived as a disconnect.

**Table 9-5 Tunnel Disconnect Mode Settings**

| Tunnel Disconnect Mode Settings | Description  |
|---------------------------------|--|
| <b>Stop Character</b>           | Enter the Stop Character which when received on the Serial Line, disconnects the tunnel. The Stop Character may be designated as a single printable character or as a control character. Control characters may be input in any of the following forms: <code>&lt;control&gt;J</code> or <code>0xA</code> (hexadecimal) or <code>\10</code> (decimal). Disable the Stop Character by blanking the field to set it to <code>&lt;None&gt;</code> . |
| <b>Modem Control</b>            | Select to enable or disable the disconnect when modem control pin is not asserted on the serial line.  |
| <b>Timeout</b>                  | Enter the number of milliseconds a tunnel may be idle before disconnection. The value of zero disables the idle timeout.   |
| <b>Flush Line</b>               | Set whether to flush the Serial Line when the Tunnel is disconnected. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Enabled</b></li> <li>◆ <b>Disabled</b> (default)</li> </ul>   |

### To Configure Tunnel Disconnect Mode Settings

#### Using Web Manager

- ◆ To configure the Disconnect Mode for a specific tunnel, click **Tunnel** in the menu and select **Tunnel 1 -> Disconnect**.

#### Using CLI

- ◆ To enter the Tunnel command level: `config -> Tunnel <instance> -> Disconnect`

#### Using XML

- ◆ Include in your file: `<configgroup name = "Tunnel Disconnect" instance = "1">`

### Statistics

Tunnel statistics contains data counters, error counters, connection time and connection information. Statistics are available at each individual connection and aggregated across all connections.

## To View Tunnel Statistics

### *Using Web Manager*

- ◆ To view statistics for a specific tunnel, click **Tunnel** in the menu and select the **Tunnel 1 -> Status**.

### *Using CLI*

- ◆ To enter the Tunnel command level: `status -> Tunnel <instance>`

### *Using XML*

- ◆ Look for the status header: `<statusgroup name = "line" instance = "1">`

## 10: Modem Emulation Settings

For commands that can take address information (ATD, ATDT, ATDP), the destination address can be specified by entering the IP Address, or entering the IP Address and port number. The destination can also be specified with a Fully Qualified Domain Name, and the xPico Wi-Fi embedded device server will perform a DNS query to find the IP address of the destination address. For example, <ipaddress>:<port>. The port number cannot be entered on its own. For ATDT and ATDP commands less than 255 characters, the xPico Wi-Fi replaces the last segment of the IP address with the configured Connect Mode remote station address. It is possible to use the last two segments also, if they are under 255 characters. For example, if the IP address is 100.255.15.5, entering the command "ATDT 16.6" results in 100.255.16.6. Use the "ATDT 0" or "ATDP 0" to switch to the Command Line Interface (CLI). Once the CLI is terminated by using the CLI exit command, the xPico Wi-Fi embedded device server reverts back to modem emulation mode. By default, the +++ characters are not passed through the connection. Turn on this capability using the modem echo pluses command.

Note: If the network connection is slow or faulty, data characters received from the Host may be backed up to the point that the Modem Emulation application is no longer reading characters from the Line, so +++ will not be effective. A Line "break" can be used to flush the queued data, close any network connection, and return to command mode.

The following describes the configuration capabilities of the xPico Wi-Fi for the Modem Emulation Mode of operation. It is important to note that this mode is not the same as Serial Tunneling. The configuration pages for Modem Emulation 1 and Modem Emulation 2 are the same. Modem Emulation does not offer the same level of capabilities and does not use the Zero-Host Load mode of operation.

The following section describes the steps to view and configure Modem Emulation 1 settings; these steps also apply to Modem Emulation 2 settings.

**Table 10-1 Modem Emulation Settings**

| <b>Modem Emulation Settings</b> | <b>Description</b>  |
|---------------------------------|---|
| <b>Listen Port</b>              | Specify a listen port to accept connections.  |
| <b>Echo Pluses</b>              | Select to enable or disable echo pluses to be echoed back during "pause +++ pause" escape sequence on the serial line.                            |
| <b>Echo Commands</b>            | Select to enable or disable echo commands. If enabled, characters read on the serial line are echoed while the modem is in Modem Command Mode.    |
| <b>Verbose Response</b>         | Select to enable or disable verbose response. If enabled, modem response codes are sent out on the serial line.                                   |
| <b>Response Type</b>            | Select either Text or Numeric representation for the modem response codes sent out on the serial line.  |
| <b>Error Unknown Commands</b>   | Select to enable or disable error unknown commands. If enabled, ERROR is returned to the serial line for unrecognized AT commands.                |
| <b>Incoming Connection</b>      | Select <b>Automatic</b> , <b>Manual</b> or <b>Disabled</b> for the handling of incoming connections.  |
| <b>Connect String</b>           | Specify a customized string to be sent with the CONNECT modem response code to the serial line, if any.   |
| <b>Display Remote IP</b>        | Select to enable or disable display remote IP. If enabled, the incoming ring sent on the serial line is followed by the IP address of the caller. |

### Using Web Manager

- ◆ To configure the modem emulation for a specific tunnel, click **Modem Emulation** in the menu and select **Modem Emulation 1 -> Configuration**.
- ◆ To view the modem emulation status for a specific tunnel, click **Modem Emulation** in the menu and select **Modem Emulation 1 -> Status**.

### Using the CLI

- ◆ To enter the Modem Emulation command level: `config -> Modem Emulation`

### Using XML

- ◆ Include in your file: `<configgroup name="Modem Emulation">`

**Table 10-2 Modem Emulation Commands and Descriptions**

| Command | Description   |
|---------|---|
| AT?     | Help. Displays this table.  |
| ATA     | Answer incoming call request (if ATS0=2 or greater).                    |
| ATD     | Connects to the configured Connect Mode address and port.               |
| ATD     | <address>:<port> Connects to the specified address and port.            |
| ATD 0   | Enters the Command Line Interface (CLI); exit returns to AT commands.   |
| ATDP    | Same as ATD.  |
| ATDT    | Same as ATD.  |
| ATEn    | Switches echo in command mode (n=0: off, n=1: on).                      |
| ATH     | Disconnects the network session.  |
| ATI     | Displays modem information.   |
| ATO     | Switches to data mode if connection still exists. Reverse of '+++'.     |
| ATQn    | Quiet mode (n=0: enable results code, n=1: disable results code.)       |
| ATS0=n  | Accept connection. (n=0: no, n=1: auto, n=2+: via ATA command).         |
| ATUn    | Accept unknown commands. (n=0: off, n=1: on).                           |
| ATVn    | Verbose mode (n=0: numeric result codes, n=1: text result codes.)       |
| ATXn    | Command does nothing and returns OK status.                             |
| ATZ     | Restore active settings from defaults.                                  |
| AT&F    | Reset saved settings in NVR to factory defaults.                        |
| AT&V    | Display current and saved settings.                                     |
| AT&W    | Save active settings to NVR.  |
| AT&Z    | Restore active settings from NVR.                                       |
| A/      | Repeat last command.  |
| +++     | Switches to command mode if entered from serial port during connection. |

## 11: Configurable Pin Manager

The Configurable Pin Manager (CPM) is responsible for the assignment and control of the configurable pins (CPs) available on the xPico Wi-Fi embedded device server. There are eight configurable pins on the xPico Wi-Fi unit. Each of these pins can be defined as general purpose input/output (GPIO) or a special role. You must configure the CPs by making them part of a role. A CP role may consist of one or more CPs. This increases flexibility when incorporating the xPico Wi-Fi device into another system. The currently supported special roles include:

- ◆ Serial flow and modem control
- ◆ Triggered SoftAP
- ◆ SPI
- ◆ User data updated
- ◆ WLAN is active

### CP Roles

The CP Role settings allow for the management of CP roles. Roles are configurable, may be enabled or disabled and can be assigned or unassigned to a configurable pin. A role, based on its state, can trigger outside events. Only an enabled role can be a trigger.

The xPico Wi-Fi roles available for assignment to a configurable pin include the following:

- ◆ Role AP Trigger (activates or deactivates the SoftAP interface)
- ◆ Role HTTP Server Trigger
- ◆ Role Line 1 DSR
- ◆ Role Line 1 DTR
- ◆ Role Line 2 DSR
- ◆ Role Line 2 DTR
- ◆ Role Line 2 Flow.CTS
- ◆ Role Line 2 Flow.RTS
- ◆ Role Radio Trigger
- ◆ Role SPI.CS
- ◆ Role SPI.MISO
- ◆ Role SPI.MOSI
- ◆ Role SPI.SCK
- ◆ Role User Data Updated
- ◆ Role WLAN Active (indicate when the wlan0 interface has an active IP address)

The CP **Role User Data Updated** pertains to the User Data module which allows definition of custom configurable data. It provides a hardware signal indicating that a Web user has changed at least one of the User Data items. The Custom status group contains the action "Acknowledge" that clears this signal.

The items listed in the [Table 11-1](#) can be configured for each role.

**Table 11-1 Role Configuration**

| CPM – Role Current Configuration | Description  |
|----------------------------------|--|
| <b>CP</b>                        | View or modify the number of the configurable pin assigned to this role. Enter 0 or blank the field to revert to <No CP Selected>. |
| <b>State</b>                     | View or modify whether the role is enabled or disabled for use.  |
| <b>Assert</b>                    | View or modify the polarity of the cp role as High or Low.   |
| <b>Mode</b>                      | Select <b>Push-Pull</b> or <b>Weak Pullup</b> mode from the drop-down menu.  |

## To Configure CPM Settings

### Using Web Manager

- ◆ To view or configure a configurable pin, click **CPM** in the menu, select **CPs** then the **Detail** link to the right of a specific CP to configure.
- ◆ To configure a CPM role, click **CPM** in the menu, select **Roles > Configuration** and then the **Edit** link to the right of a specific role to configure.
- ◆ To view a CPM role status, click **CPM** in the menu, select **Roles > Status** and then the **Detail** link to the right of a specific role to view details.

### Using the CLI

- ◆ To enter the CPM command level: `config -> CPM`

### Using XML

- ◆ Include in your file: `<configgroup name="cpm" >`

## Configurable Pin Status

Each configurable pin (CP) is associated with an external hardware pin. The current configuration table shows the sample settings for each CP.

**Table 11-2 Current Configurable Pins**

| CP         | Ref    | Usage | Assert | Mode      | Value | Roles | Active in Role |
|------------|--------|-------|--------|-----------|-------|-------|----------------|
| <b>CP1</b> | Pin 35 | Input | High   | Push-Pull | 0     | 1     | <available>    |
| <b>CP2</b> | Pin 26 | Input | High   | Push-Pull | 1     | 1     | <available>    |
| <b>CP3</b> | Pin 28 | Input | High   | Push-Pull | 0     | 0     | <available>    |
| <b>CP4</b> | Pin 30 | Input | High   | Push-Pull | 1     | 0     | <available>    |
| <b>CP5</b> | Pin 32 | Input | High   | Push-Pull | 0     | 0     | <available>    |
| <b>CP6</b> | Pin 34 | Input | High   | Push-Pull | 0     | 0     | <available>    |
| <b>CP7</b> | Pin 27 | Input | High   | Push-Pull | 0     | 0     | <available>    |
| <b>CP8</b> | Pin 3  | Input | High   | Push-Pull | 0     | -0    | <available>    |

**Table 11-3 CP Status**

| <b>CPM – CPs Status</b> | <b>Description</b>   |
|-------------------------|--|
| <b>Ref</b>              | Indicates the pin number on the device which corresponds to this configurable pin.                             |
| <b>Usage</b>            | Indicates whether this pin is set as Input, Output or Reserved (for a different use).                          |
| <b>Assert</b>           | Indicates the polarity of the configurable pin as High or Low.   |
| <b>Mode</b>             | Indicates whether this pin is setup for push-pull or if it enables an internal weak pullup.                    |
| <b>Value</b>            | Indicates the logical value of the configurable pin.   |
| <b>Roles</b>            | Indicates the number of configurable pin roles which refer to this pin.  |
| <b>Active in Role</b>   | Indicates the current active role that uses this pin. If there is currently no role, <available> will display. |

To modify a CP, all roles in which it is a member must be disabled.

The changes to a CP configuration are not saved in FLASH. Instead, these CP settings are used when the CP is added to a CP Role. When the CP Role is saved, its CP settings are saved with it. Thus, a particular CP may be defined as "Input" in one role but as "Output" in another. Only one role containing any particular CP may be enabled at once.

## 12: Application Aware Power Management

The xPico Wi-Fi embedded device server is intended to be used in applications that require or are sensitive to the amount of power consumed. Consequently the power management framework of the xPico Wi-Fi is intended to provide methods in which users can optimally manage the power consumption of the device.

The Power Management framework offers Dynamic Power Modes that supports the compromise between power savings and response time that best suits the application. It is generally accepted that the lowest power consuming mode has the longer response time from the low power mode to being fully connected and active. The power management framework also allows the ability for the device to be managed by a host using the dedicated Wake-Up System Pin.

The Power Management Framework consists of the following modes.

- ◆ Power Up Mode
- ◆ Sleep Mode
- ◆ Standby Mode

**Note:** *More information on the on response times and power values will be provided in the xPico Wi-Fi user collateral as soon as it is available.*

### Power Up Mode

This is the only mode available if the Access Point is enabled or if none of the Dynamic Power Saving modes are enabled for the WLAN interface. However, even in the Continuous Transmission mode, the xPico Wi-Fi embedded device server provides some form of power savings capability. The xPico Wi-Fi device supports "ps-poll", when a STA makes an initial association with an access point, it negotiates and informs of its ability of supporting a low power mode and what the low power duration is. The connected Access Point must be capable of supporting the standard capabilities of Traffic Indication Map (TIM) and Power Save Poll (ps-poll). The xPico Wi-Fi device automatically manages this capability when in the continuous mode.

### Sleep Mode

Sleep mode is the power saving mode which the xPico Wi-Fi embedded device server powers down the Wi-Fi radio and system clocks while preserving the system state. This mode offers a compromise of power versus wake response time for those applications that need reduced power consumption but with a speedy wake up and connection reacquisition response time.

### Standby Mode

Standby mode of operation is the deepest sleep mode of the xPico Wi-Fi, and offers the lowest power consumption. In this mode the xPico Wi-Fi has the only the RTC operating and the system runtime state is not preserved. This mode has the longest wake up response time, since the system state has to be reinitialized and connections reacquired.

## Dynamic Power Mode Configuration

All the power framework parameters are located and can be configured on the "Performance" page of the on-board Web page. Changing any of the fields on this page takes effect immediately.

**Dynamic Power Mode:** The drop down configuration allows the user to select which of the power modes to use. Either Sleep or Standby. Note if SoftAP is enabled then these modes are not enabled.

**Application:** This configuration parameter allows the user to select which application can override the power settings. For example if Tunnel Connect and Tunnel Connect are both checked then if there is any activity with these applications the ability to switch to the power reduction off state is over-ridden. The application can also cause the power framework to wake up earlier.

**WKUP Pin Power Down:** If enabled the system will only transition into the selected Dynamic Power Mode power savings state if there is a falling edge on the WKUP system pin.

**WKUP Pin Power Up:** Similar to the previous parameter, enabling this option will cause the system to return to the active power on state either on a rising edge of the WKUP pin or after the Maximum Time Powered Down timer is expired. If the option is disabled, then the system will use the Maximum Time Powered Down timer expiration only to return to its active condition.

**Maximum Time Powered Down:** This parameter determines how long the device can remain in the selected power savings state. The device can be woken earlier if the WKUP Pin Power Up or an Application override is enabled. The Value for this field is in seconds.

**Time Powered Up:** This is the maximum duration in which the device is powered on before transitioning into the selected Power Savings mode. If the WKUP Pin Power Down is enabled, the system will not transition until a falling edge of the pin is detected.

## Power Settings

Change settings pertaining to power consumption including application, maximum time powered down, wake-up pin power up, and time powered up.

**Table 12-1 Power Settings**

| Power Settings                   | Description   |
|----------------------------------|---|
| <b>Dynamic Power Mode</b>        | Select a power down mode or disable the power mode.   |
| <b>Time Powered Up</b>           | Indicate the amount of time the device will hold power during <b>Time Powered Up</b> . Default time powered up is 1 hour.   |
| <b>Application</b>               | Select the performance application: <ul style="list-style-type: none"> <li>◆ Command Line</li> <li>◆ HTTP Server</li> <li>◆ Tunnel Accept</li> <li>◆ Tunnel Connect</li> </ul> Any application selected for performance may hold the power on longer or wake up sooner. |
| <b>WKUP Pin</b>                  | Select the role of the WKUP power up pin in powering up or staying up.  |
| <b>Maximum Time Powered Down</b> | Indicates the maximum amount of time for the device to be powered down. After this time, the device wakes up.   |

## To Configure Power

### *Using Web Manager*

- ◆ To modify performance settings, click **Power** in the menu.

### *Using CLI*

- ◆ To enter the Performance command level: `config -> Power`

### *Using XML*

- ◆ Include in your file: `<configgroup name = "Power">`

# 13: Services Settings

## HTTP Server

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

Table 13-1 HTTP Settings

| HTTP Settings                 | Description  |
|-------------------------------|--|
| <b>Mode</b>                   | Select to enable or disable the HTTP server: <ul style="list-style-type: none"><li>◆ <b>Enabled</b> (default)</li><li>◆ <b>Disabled</b></li><li>◆ <b>Triggered</b></li></ul> |
| <b>Port</b>                   | Enter the port for the HTTP server to use. The default (80) will be restored when the field is cleared.  |
| <b>Authentication Timeout</b> | Enter the Authentication Timeout. This setting only applies if HTTP Server is enabled in Performance.  |
| <b>Inactivity Timeout</b>     | Enter the amount of time the HTTP server will hold power on after completing a request. This setting only applies if Digest Authentication is being used.                    |

### To Configure HTTP Settings and Security

#### Using Web Manager

- ◆ To configure HTTP settings and security, click **HTTP** in the menu and select **Configuration**.

#### Using CLI

- ◆ To enter the HTTP Server command level: `config -> HTTP Server`

#### Using XML

- ◆ Include in your file: `<configgroup name = "HTTP Server">`

### HTTP Security

Changes to HTTP server security settings take effect immediately.

Table 13-2 HTTP Security Settings

| HTTP Security Settings | Description   |
|------------------------|---|
| <b>Edit</b>            | Click the <b>Edit</b> link beside an access control to view or edit the URI, Auth Type, and User Level. |
| <b>Summary</b>         | Click the <b>Summary</b> link beside a specific access control to close the summary details.            |

| HTTP Security Settings | Description   |
|------------------------|---|
| <b>URI</b>             | <p>Enter the Uniform Resource Identifier (URI) to apply access control settings. May contain up to 255 characters. The HTTP Server can be configured with many different authentication directives. The authentication is hierarchical in that any URI can be given an authentication directive in order to override a parent URI authentication directive.</p> <p>The URI must begin with '/' to refer to the entire file system.</p> <p>For example, create URI "/Welcome", then place our "hello.html" file in directory "/http/Welcome/", finally point your browser to "&lt;device IP address&gt;/Welcome/hello.html" to experiment with the authorization levels.</p> <p>The following URIs are built into the server:</p> <ul style="list-style-type: none"> <li>◆ "/ajax" Web Manager</li> <li>◆ "/logout" Digest authentication</li> <li>◆ "/mux_http" Mux HTTP listener</li> <li>◆ "/tlog" Trouble log</li> </ul> |
| <b>Auth Type</b>       | <p>Select the authentication type:</p> <ul style="list-style-type: none"> <li>◆ <b>None</b> requires no authentication is necessary.</li> <li>◆ <b>Basic</b> encodes passwords using Base64.</li> <li>◆ <b>Digest</b> hashes passwords using MD5</li> </ul>   |
| <b>User Level</b>      | <p>Select User Level:</p> <ul style="list-style-type: none"> <li>◆ <b>User</b> provides access to all users.</li> <li>◆ <b>Tech</b> provides users with Tech privilege access only if one or more of their Zones are configured here.</li> <li>◆ <b>Admin</b> provides access only to users with the Admin privilege.</li> <li>◆ <b>None</b> provides access to no users.</li> </ul>  |

## To View HTTP Status

### Using Web Manager

- ◆ To view HTTP status, click **HTTP** in the menu and select **Status**.

### Using CLI

- ◆ To enter the HTTP Server command level: `status -> HTTP Server>`

### Using XML

- ◆ Include in your file: `<configgroup name = "HTTP Server">`

## Real Time Clock and Current Time

The xPico Wi-Fi device includes the ability to display and access the current time. The status and configuration of the real time clock is located via the "Clock" Menu. The Status page displays the current time in a YYYY-MM-DD hh:mm:ss format, where the hours are in 24-hour format. The xPico Wi-Fi supports dates in the range 2000-01-01 00:00:00 to 2100-12-31 23:59:59 UTC.

Source: This parameter allows the user to select the timing source for the current time. The default time source for the clock is Manual, but can be changed to be NTP.

UTC offset: Offset to UTC is specified in minutes, between the ranges of -1440 and 1440 and can be up to 5 characters. Lists of common time zones and corresponding UTC offsets can be found at the following websites (IANA Time Zone Database or the Wikipedia list of UTC time offsets). If the time source is set to manual, the current time can be set with the "Current Time" status (set) action.

**Table 13-3 Clock Settings**

| HTTP Settings     | Description   |
|-------------------|---|
| <b>Set</b>        | Click the <b>Set</b> button in the <b>Status</b> window to manually configure the time source. The format for setting time is YYYY-MM-DD hh:mm:ss, where the hours are in 24-hour format. The xPico Wi-Fi unit supports dates in the range of 2000-01-01 00:00:00 to 2100-12-31 23:59:59 UTC.   |
| <b>Source</b>     | Set the time source: <ul style="list-style-type: none"> <li>◆ <b>Manual:</b> select this time source and click the <b>Status</b> link above to access the <b>Set</b> button (see description above.) This is the default setting.</li> <li>◆ <b>NTP:</b> select this time source and see <a href="#">Simple NTP Client</a> to set the NTP.</li> </ul> |
| <b>UTC Offset</b> | Specify the <b>UTC offset</b> in minutes between the range of -1440 and 1440. List of common time zones and corresponding UTC offsets can be found at several websites, including the IANA Time Zone Database or the Wikipedia list of UTC time offsets.  |

## To View or Configure the Clock

### Using Web Manager

- ◆ To configure HTTP settings, click **Clock** in the menu.

### Using CLI

- ◆ To enter the HTTP Server command level: `config -> clock`

### Using XML

- ◆ Include in your file: `<configgroup name = "clock">`

## Simple NTP Client

The xPico Wi-Fi embedded device server includes support of a Simple NTP (SNTP) client. To use SNTP, the time source must be configured as NTP as described in [Real Time Clock and Current Time](#). The configuration for the SNTP client is located via a separate NTP menu option.

When configured as the time source, NTP will automatically update the clock from the configured NTP server. The Server Hostname can be entered in the appropriate field in the NTP Configuration page. Additionally, an immediate manual NTP synchronization can be run with the "Sync" status action.

Table 13-4 NTP Settings

| HTTP Settings          | Description  |
|------------------------|--|
| <b>Sync</b>            | Click the <b>Sync</b> button (on the Status subpage) to immediately sync clock synchronization with the NTP server.                  |
| <b>Server Hostname</b> | Enter the name or IP address of the NTP server (e.g., <a href="http://pool.ntp.org">pool.ntp.org</a> ) at the Configuration subpage. |

## To View or Configure the NTP

### Using Web Manager

- ◆ To configure NTP settings, click **NTP** in the menu.

### Using CLI

- ◆ To enter the HTTP Server command level: `config -> ntp`

### Using XML

- ◆ Include in your file: `<configgroup name = "ntp">`

## CLI Server

The xPico Wi-Fi embedded device server includes support of Command Line Interface (CLI) server configuration. You can customize CLI inactivity timeout and change the CLI port assignment. CLI Server Mode must be enabled in Web Manager in order for you to access the CLI functionality. All changes take effect immediately.

Table 13-5 CLI Server Settings

| CLI Server Settings       | Description  |
|---------------------------|--|
| <b>Inactivity Timeout</b> | Enter the desired Inactivity Timeout in minutes. The default setting is 15 minutes. Enter 0 for "<None>". After this period of inactivity, the CLI Server will close the connection. |
| <b>Mode</b>               | Click to enable or disable CLI Server Mode.  |
| <b>Port</b>               | View and modify the Telnet port. The CLI Server listens on this port for incoming Telnet connections.  |

## To View or Configure the CLI Server

### Using Web Manager

- ◆ To configure the CLI server, click **CLI Server** in the menu.

### Using CLI

- ◆ To enter the CLI Server command level: `config -> cli server`

**Using XML**

- ◆ Include in your file: `<configgroup name = "cli server">`

# 14: Maintenance and Diagnostics

## File System Settings

The xPico Wi-Fi embedded device server uses a flash file system to store files. The file system can be formatted and compacted: formatting erases all files while preserving configuration, and compacting reclaims dirty space while preserving all files.

The file system also provides statistics and the ability to create, delete, and manipulate files and directories.

## File System Statistics

**Table 14-1 File System Statistics Settings**

| File System Commands | Description  |
|----------------------|--|
| <b>Compact</b>       | Compact the <b>File System</b> to reclaim dirty flash storage while preserving any existing files and directories. |
| <b>Format</b>        | Format the <b>File System</b> to erase all existing files and directories, while preserving configuration.         |

## To View File System Statistics, Compact or Format the File System

### Using Web Manager

- ◆ To view file system statistics, compact or format the file system, click **File System** in the menu and select **Statistics**.

### Using CLI

- ◆ To enter the File System command level: `status -> File System`

### Using XML

- ◆ Not applicable.

## File Display

It is possible to view the list of existing files, and to view their contents.

## To Display Files

### Using Web Manager

- ◆ To view existing files and file contents, click **File System** in the menu and select **Browse**.

### Using the CLI

- ◆ To enter the File System command level: `file system`

### Using XML

- ◆ Not applicable.

## File Manipulation

The xPico Wi-Fi embedded device server allows for files to be deleted, moved, renamed, and uploaded via HTTP. Directories can be created, deleted, moved, and renamed.

## To Transfer or Modify File System Files

### Using Web Manager

- ◆ To create a new file or directory, upload an existing file, copy or move a file, click **File System** in the menu and select **Browse**.

### Using the CLI

- ◆ To enter the File System command level: `enable -> file system`

### Using XML

- ◆ Not applicable.

## Device Settings

The xPico Wi-Fi device settings allow for rebooting the device, restoring factory defaults, and uploading new firmware.

Anytime you reboot the unit, this operation will take some time to complete. Please wait a minimum of 10-20 seconds after rebooting the unit before attempting to make any subsequent connections.

## Device Management

**Table 14-2 Device Management Settings**

| System Settings                  | Description   |
|----------------------------------|---|
| <b>Save</b>                      | Any cached configuration changes are committed, so they will apply after a reboot. Without saving, cached configuration changes are lost after a reboot.  |
| <b>Reboot</b> (button)           | Reboots the device. When rebooted, your browser should be refreshed and redirected to the main status page after 30 seconds.<br><br><i>Note: The redirect will not work as expected if the IP address of the devices change after reboot. After setting the configuration back to factory defaults, the device will automatically be rebooted. If Web Manager is access through SoftAP, your connection to SoftAP may be dropped when device reboots.</i> |
| <b>Factory Defaults</b> (button) | Restores the device to the original factory settings. All configuration will be lost. The xPico Wi-Fi automatically reboots upon setting back to the defaults.  |
| <b>Firmware Upload</b> (button)  | Device will reboot to the Over-The-Air (OTA) firmware upgrade application to continue the operation.  |

**Note:** Go to [Chapter 18: Updating Firmware Over the Air](#) for directions on uploading new firmware.

## To Save Configuration, Reboot, Restore Factory Defaults or Upload Firmware

### Using Web Manager

- ◆ To access the area with options to reboot, restore to factory defaults, upload new firmware, click **Device** in the menu.

### Using CLI

- ◆ To enter the Device command level: `status -> Device`

### Using XML

- ◆ Not applicable.

## User

View, edit, delete or create up to four users besides the Admin user on the device. For existing users, you can assign user privileges and specify passwords.

**Table 14-3 User Management**

| User Settings          | Description  |
|------------------------|--|
| <b>View or Edit</b>    | Select a user listed under the <b>View or Edit</b> heading to view or modify user password and privilege. The <b>admin</b> user exists in the firmware. This user password can also be modified (see <a href="#">Table 14-4</a> ).   |
| <b>Create new User</b> | To create a new user, enter a new user name in the text box and click the <b>Submit</b> button. The newly created user name will appear under the <b>View or Edit</b> heading under admin and will have no password and be assigned User privilege until edited. Up to 4 users may be created. |

**Table 14-4 User Settings**

These settings appear for the specific user clicked under the **View or Edit** heading ([Table 14-4](#)).

| User Settings    | Description   |
|------------------|---|
| <b>Password</b>  | Enter a new password. Users will need to log in again after changing the password.  |
| <b>Privilege</b> | Modify the privilege of the user as desired. Privilege governs what a user is able to do. Choices: <ul style="list-style-type: none"> <li>◆ <b>Admin</b> has access to all areas except where User Level is set to "None."</li> <li>◆ <b>User</b> has access to areas with User Level set to "User."</li> <li>◆ <b>Tech</b> has access to areas with <b>User Level</b> set to "User" or "Tech" in designated <b>Zones</b>.</li> </ul> |

## To Configure Admin User on the Device

### *Using Web Manager*

- ◆ To change the password setting, click **Users** in the menu.

### *Using CLI*

- ◆ To enter the Users command level: `config -> User`

### *Using XML*

- ◆ Look for the status header: `<configgroup name = "User">`

## Diagnostics Settings

The xPico Wi-Fi embedded device server has tools for diagnostics and statistics. Options allow for the viewing of hardware, IP sockets, threads, and buffer pools.

### To View Buffer Pool Status

Displays information for each Buffer Pool. Total is the number of buffers allocated to the pool and Free is the remaining number of buffers available in the pool.

#### *Using Web Manager*

- ◆ To view information for each Buffer Pool, click **Diagnostics** in the menu and select **Buffer Pools**.

#### *Using CLI*

- ◆ To enter the Buffer Pools command level: `status -> Diagnostics -> Buffer Pools`

#### *Using XML*

- ◆ Not applicable.

### To View Hardware Status

Displays hardware identification and capabilities.

#### *Using Web Manager*

- ◆ To view hardware information, click **Diagnostics** in the menu and select **Hardware**.

#### *Using CLI*

- ◆ To enter the Diagnostics command level: `status -> Diagnostics -> Hardware`

#### *Using XML*

- ◆ Not applicable.

## To View Heap Status

Displays heap usage, stage and statistics.

### Using Web Manager

- ◆ To view hardware information, click **Diagnostics** in the menu and select **Heap**.

### Using CLI

- ◆ To enter the Diagnostics command level: `status -> Diagnostics -> Heap`

### Using XML

- ◆ Not applicable.

## To View IP Socket Status

Displays information for each IP socket.

**Table 14-5 IP Socket Settings**

| IP Socket Settings | Description  |
|--------------------|--|
| <b>Detail</b>      | Click the <b>Detail</b> link beside a specific thread to view the protocol, interface, local port, remote address, remote port, state, Rx buffers, and Tx buffers. |
| <b>Summary</b>     | Click the <b>Summary</b> link beside a specific thread to close the summary provided about a specific IP socket.   |

### Using Web Manager

- ◆ To view IP Sockets information, click **Diagnostics** in the menu and select **IP Sockets**.

### Using CLI

- ◆ To enter the IP Sockets command level: `status -> Diagnostics -> IP Sockets`

### Using XML

- ◆ Not applicable.

## To View Modules Status

Displays modules present on the device and their static memory usage.

### Using Web Manager

- ◆ To view hardware information, click **Diagnostics** in the menu and select **Modules**.

### Using CLI

- ◆ To enter the Diagnostics command level: `status -> Diagnostics -> Modules`

### Using XML

- ◆ Not applicable.

### To Ping

Send a diagnostic ping by specifying host, timeout and count.

**Table 14-6 Ping Settings**

| Ping Settings  | Description   |
|----------------|---|
| <b>Host</b>    | Specify either a DNS hostname or an IP address when pinging a network host.   |
| <b>Timeout</b> | Enter the number of seconds to wait for a response for each ping packet sent. |
| <b>Count</b>   | Enter the number of ping packets to send.                                     |

### Using Web Manager

- ◆ To view hardware information, click **Diagnostics** in the menu and select **Ping**.

### Using CLI

- ◆ To enter the Diagnostics command level: `status -> Diagnostics -> Ping`

### Using XML

- ◆ Not applicable.

### To View Threads Status

Displays current existing Threads and their stack usage.

**Table 14-7 Threads Settings**

| Threads Settings | Description   |
|------------------|---|
| <b>Detail</b>    | Click the <b>Detail</b> link beside a specific thread to view the stack used, the stack size, stack percent, and stack condition. |
| <b>Summary</b>   | Click the <b>Summary</b> link beside a specific thread to close the summary provided about a specific thread.                     |

### Using Web Manager

- ◆ To view hardware information, click **Diagnostics** in the menu and select **Threads**.

### Using CLI

- ◆ To enter the Diagnostics command level: `status -> Diagnostics -> Threads`

### Using XML

- ◆ Not applicable.

# 15: Security Settings

## Serial Tunneling: TCP AES

Tunneling Security for TCP AES is enabled for both Accept and Connect Tunnel configurations. The function can be enabled from the Accept or Connect configuration pages under the Tunnel menu.

**Protocol:** The drop down configuration allows the user to select whether to use TCP or TCP with AES when a connection attempt originates from the network.

**AES Encrypt Key and AES Decrypt Key:** These two fields are used to enter the Encryption and Decryption keys. These keys are a shared secret, so both sides of the connection must be knowledgeable of them and kept secret. The keys can be 16, 24 or 32 bytes in length. A key that is entered with less than one of these options is padded with zeroes. The form is in hexadecimal and takes up to 32 bytes, separated by spaces. A byte specification comprises two nibble specifications with no intervening spaces. A nibble specification is a single digit from 0 to 9 or from "a" to "f" (representing 10 through 15). To delete the key blank its display.

**Example Hexadecimal Key:** 12 34 56 78 9a bc de f0 01 02 03 04 05 06 07 08.

To enable TCP-AES for Connect mode edit the Host 1 option on the Tunnel Connect Configuration page, as shown below. On selecting Edit the menu expands to offer the ability to select TCP AES as the protocol to be used on the connection. When TCP AES is selected the menu further expands to reveal the fields for the Encryption and Decryption Keys.

## AES Credential Management

AES credential management allows you to view, edit, delete or create an AES credential on the device.

**Table 15-1 AES Credential Settings**

| AES Credential Settings   | Description  |
|---|--|
| <b>Create new AES Credential (field)</b>  | Enter the name of the AES credential to be created in this field and click the <b>Submit</b> button which will appear.   |
| <b>View or Edit</b><br>(Links to AES credentials, if any, are listed below this header) | Existing AES credentials previous updated or never updated will be listed under the <b>View or Edit</b> header. <ul style="list-style-type: none"><li>◆ To delete a particular AES credential, click the checkbox to the right of a particular credential (under the <b>Delete</b> header), and click the <b>Submit</b> button which appears.</li><li>◆ To update or modify an AES credential, click on an AES credential.</li></ul> |
| <b>Encrypt Key</b>  | Enter the <b>Encrypt Key</b> to be used for decrypting incoming data. This field appears when a specific AES credential is selected/clicked under the <b>View or Edit</b> header (see field description above). The key may be 16, 24 or 32 bytes in length.   |

| AES Credential Settings (continued) | Description  |
|-------------------------------------|--|
| <b>Decrypt Key</b>                  | Enter the <b>Decrypt Key</b> to be used for encrypting outgoing data. This field appears when a specific AES credential is selected/clicked under the <b>View or Edit</b> header (see field description above). The key may be 16, 24 or 32 bytes in length. |

## To Manage AES Credentials

### Using Web Manager

- ◆ To view or manage AES credentials, click **AES Credentials** in the menu.

### Using CLI

- ◆ To enter the Tunnel command level: `config -> AES Credential <name>`

### Using XML

- ◆ Include in your file: `<configgroup name = "AES Credential" instance = "<name>">`

## 16: Lantronix Application Toolbox for IOT Solutions

The Lantronix Application Toolbox for IOT Solutions (LATIS) is a collection of software tools designed to make the application and use of the xPico Wi-Fi embedded device server simple to use.

The toolbox consists of Serial Multiplexer, Monitor and Explorer.

### Serial Multiplexer

As an interface, serial ports tend to be used as a dedicated data channel between two points. With data generally being asynchronous with a simple 'character' format that indicates the start and stop and sometimes error checking. There is a need to establish multiple data channels in order to support multiple applications simultaneously in the xPico Wi-Fi unit. This requires the need to create a protocol that supports the differentiation of data.

The xPico Wi-Fi embedded device server provides a "Mux" Line Protocol for the serial Line to manage and transfer data on multiple connections without requiring custom software on the device. A host processor that is connected to the device via the serial Line sees a simple command/response interface. There are no intentional delays required in the normal handshake.

#### Usage

The selected serial line on the device must be configured with Line Protocol set to "Mux" and with settings compatible with the connected device. Flow control is recommended.

The Mux intentionally does not require configuration, as it's behavior is governed entirely by the Mux commands themselves.

Some commands are expected to offer binary-escape encoding for data transfer. To use these commands, data must be 8 bits (not 7.) Hardware flow control is recommended to avoid errors due to contention between XON/XOFF software flow control characters and data in the binary stream. Software flow control is possible if the design can guarantee that the binary-escape encoding will not include the XON/XOFF characters, or if the data transfer is done via hex encoding.

#### xPico Wi-Fi Mux Command Reference

The Mux (Line Protocol) is intended for machine to machine communication, so it differs from the Command Line Interface in the following ways:

1. Command characters are NOT echoed.
2. Each command is terminated by a single <CR> or <LF> character unless designated otherwise.
3. Commands are terse.
4. Responses are terse.
5. No tab completion.
6. No help text.
7. Times out when command character(s) received but not yet ended with newline.

Most commands comprise readable ASCII characters. The exceptions use binary-escape encoding, but these have a hex encoding alternate.

### Controlling Connections

An "Accept" Connection listens on a designated port for a connection attempt from the network. More than one may be set up and used at a time. Once a connection is established, the device stops listening on the designated port; at this time the host may choose to begin accepting with the same port on another accept instance.

A "Connect" Connection initiates the attempt into the network. It must be provided with the destination port and address. More than one may be set up and used at a time.

In the following commands, <n> is the character 1, 2, 3, or 4, designating the connection instance.

```
<n>a[<interface> :]<port><protocol>[ ,<credential>]
```

Begin listening, where:

|              |  |
|--------------|--|
| <interface>  | (Optional): can be "ap0" or "wlan0" to restrict listening to that specific interface       |
| <port>       | is a decimal number from 1 to 65535 representing the port to listen on                     |
| <protocol>   | can be "TCP" or "TCP AES"  |
| <credential> | is the name of the credential to be used, present only if <protocol> requires a credential |

Possible responses are:

|               |   |
|---------------|---|
| K             | Successfully waiting for an inbound connection; may become Active any time  |
| E<string><LF> | Error, where <string> is a readable ASCII message terminated by a Line Feed |

```
<n>c<destination>:<port><protocol>[ ,<credential>]
```

Begin connecting, where:

|               |  |
|---------------|--|
| <destination> | is either a hostname or an IP address  |
| <port>        | is a decimal number from 1 to 65535 representing the destination port                      |
| <protocol>    | can be "TCP" or "TCP AES"  |
| <credential>  | is the name of the credential to be used, present only if <protocol> requires a credential |

Possible responses are:

|               |  |
|---------------|--|
| K             | Waiting for an outbound connection; will reach either Active or Disabled over time |
| E<string><LF> | Error, where <string> is a readable ASCII message terminated by a Line Feed        |

```
<n>h
```

Begin listening for HTTP. This option works with the HTTP server, listening for a transaction directed to the URL "/mux\_http".

Possible responses are:

|               |   |
|---------------|---|
| K             | Successfully waiting for an inbound connection; may become Active any time  |
| E<string><LF> | Error, where <string> is a readable ASCII message terminated by a Line Feed |

`<n>p`

Pushes out pending send data.

Possible responses are:

|               |   |
|---------------|---|
| K             | Successful  |
| E<string><LF> | Error, where <string> is a readable ASCII message terminated by a Line Feed |

`<n>e[<timeout>]`

Ends the instance gracefully, pushing out pending send data over time but immediately dropping any receive data.

|         |   |
|---------|---|
| timeout | (Option) This is a number representing milliseconds for timeout. If not provided, a 5000 millisecond timeout is applied by default. |
|---------|---|

Possible responses are:

|               |   |
|---------------|---|
| K             | Successful  |
| T             | Timed out before all the data could be sent; instance is not ended          |
| E<string><LF> | Error, where <string> is a readable ASCII message terminated by a Line Feed |

`<n>f[<timeout>]`

Sends fin, pushing out pending send data over time but receive direction remains open.

|         |  |
|---------|--|
| timeout | (Option) This is a number representing milliseconds for timeout. If not provided, a 5000 msec timeout is applied by default. |
|---------|--|

Possible responses are:

|               |   |
|---------------|---|
| K             | Successful  |
| T             | Timed out before all the data could be sent; instance remains open for send |
| E<string><LF> | Error, where <string> is a readable ASCII message terminated by a Line Feed |

`<n>k`

Kills the instance without delay.

Possible responses are:

|               |   |
|---------------|---|
| K             | Successful  |
| E<string><LF> | Error, where <string> is a readable ASCII message terminated by a Line Feed |

`<n>`

Requests the current status of the instance.

Possible responses are:

|   |                                       |
|---|---------------------------------------|
| D | Disabled                              |
| W | Waiting for connection establishment  |
| F | Received fin, but send remains active |

|          |                                      |
|----------|--------------------------------------|
| R        | Sent fin, but receive remains active |
| <b>K</b> | Active                               |

#### Transferring Data

In the following commands,

<n> is 1, 2, 3, or 4, and

<bytes> is a decimal number in ASCII numeric characters.

<n>sx

Send data coded in hex.

Possible responses are:

|          |   |
|----------|---|
| <bytes>K | Okay for no more than <bytes> number of bytes |
|----------|---|

Now the host sends hex bytes.

The host sends a newline character to terminate.

The device may terminate while the host is still sending bytes by sending E<string><LF>; otherwise the device will acknowledge the host terminating newline by sending K.

The host may decide not to send all the bytes that are allowed.

|               |   |
|---------------|---|
| E<string><LF> | Error, where <string> is a readable ASCII message terminated by a Line Feed |
|---------------|---|

<n>sb<escape>

Send data coded in binary-escape.

Possible responses are:

|          |                                  |
|----------|----------------------------------|
| <bytes>K | Okay for <bytes> number of bytes |
|----------|----------------------------------|

Now the host sends binary bytes.

To send a byte that matches <escape>, host sends it twice in a row.

The host sends <escape> followed by a newline to terminate.

The device may terminate while the host is still sending bytes by sending E<string><LF>; otherwise the device will acknowledge the host terminating newline by sending K.

The host may decide not to send all the bytes that are allowed.

|               |   |
|---------------|---|
| E<string><LF> | Error, where <string> is a readable ASCII message terminated by a Line Feed |
|---------------|---|

<n>rx<bytes>

Receive up to <bytes> number of bytes coded in hex.

Possible responses are:

|   |          |
|---|----------|
| K | Accepted |
|---|----------|

The host will possibly wait indefinitely until data arrives.

As data arrives, device sends to the host in hex.

Device sends `<LF>` after data when it terminates data mode.

Data mode terminates when

1. Number of bytes specified in command has been reached.
2. Connection is dropped.
3. Any single character is sent by the host.

|               |   |
|---------------|---|
| E<string><LF> | Error, where <string> is a readable ASCII message terminated by a Line Feed |
|---------------|---|

`<n>rb<escape><bytes>`

Receive up to `<bytes>` number of bytes coded in binary-escape.

Possible responses are:

|   |          |
|---|----------|
| K | Accepted |
|---|----------|

The host will possibly wait indefinitely until data arrives.

As data arrives, device sends to the host in binary.

If the host receives `<escape><escape>`, it treats it a single byte.

Device sends `<escape><LF>` after data when it terminates data mode.

Data mode terminates when

1. Number of bytes specified in command has been reached.
  - a. Connection is dropped.
  - b. Any single character is sent by the host.

|               |   |
|---------------|---|
| E<string><LF> | Error, where <string> is a readable ASCII message terminated by a Line Feed |
|---------------|---|

### Waiting for Events

In the following command,

`<n>` is 1, 2, 3, or 4; and

`<event>` is `<n>[s | r]` where `s` is for send ready and `r` is for receive ready, and

`<event list>` is one or more concatenated events.

`W<event list>`

Wait for any of the listed events.

Possible responses are:

|   |                          |
|---|--------------------------|
| K | Agreed to the event list |
|---|--------------------------|

Then, if any event in the list occurs, the first is returned, for example `2r<LF>`.

The device will wait indefinitely for any event on the list.

Host may cancel waiting by sending any single character. Device will not discard the character, so the host may send a newline for no operation or simply begin the next desired command.

Device confirms cancellation by sending a single <LF>.

|               |   |
|---------------|---|
| E<string><LF> | Error, where <string> is a readable ASCII message terminated by a Line Feed |
|---------------|---|

### Device Control

General device control is achieved via the Command Line Interface. Connections can remain open during this time.

D

Enters Command Line Interface, but with echo off. Exit from the top level returns to Mux commands.

### Example #1

Sends hello world to whoever connects TCP to port 10001:

```
1a10001TCP
KW1s
K<upon connection>1s
1sb~
50KHello world!~
```

### Example #2 of Using Mux Feature

The following is a simple example on how to use the xPico Wi-Fi Mux Feature.

This example shows how to create a simple Web Page that takes two text fields and uses a submit button to send the data to the serial connected host processor.<sup>1</sup>

The screenshot shows a web form with the following elements:

- A label "Username:" followed by a text input field containing the value "Speedy".
- A label "Email:" followed by a text input field containing the value "sgonzales@ltuns.com".
- A "Submit" button located below the input fields.

The HTML code for this simple form is;

```
<form name="input" action="/mux http" method="post" autocomplete="off">
Username: <input type="text" name="user"></br>
Email: <input type="text" name="email"></br>
<input type="submit" value="Submit">
</form>
```

### Setup Steps

1. Create a /http directory in the xPico Wi-Fi file system.
2. Save the HTML file into this directory. E.g. myform.html
3. Configure xPico Wi-Fi Line 1 or Line 2 protocol to "Mux" either using the Web manager or CLI.

The system is now ready to use the Mux protocol.

### Demonstration Steps

1. Perform HTTP listen on instance 1.
  - a. Type into Mux Line: "1h<enter>".
  - b. Expect "K" confirmation.
2. See that HTTP is not yet available.
  - a. Type into Mux Line: "1<enter>".
  - b. Expect "W" (waiting).
3. Point your browser to the form on your device. URL: "xxx.xxx.xxx.xxx/form.html".
4. Fill in a "Username" and "Email" of your choice in the form.
5. Press "Submit".
6. See that HTTP is available.
  - a. Type into Mux Line: "1<enter>".
  - b. Expect "K" confirmation.
7. Read data.
  - a. Type into Mux Line: "1rb.80<enter>".
  - b. Expect to see your data.
8. Send response.
  - a. Type into Mux Line: "1sb~<enter>"
 

Paste in: `<html>`

```

<head><title>An Example Page</title></head>
<body>Thank you for the information.</body>
</html>
          
```
  - b. Type into Mux Line: ~<enter>
9. Close connection.
  - a. Type into Mux Line: 1e<enter>.
  - b. Expect K confirmation.
  - c. The response appears in the browser.

## Monitor Settings

The Monitor feature can be used to query and capture desired information during an xPico Wi-Fi serial port to serial device connection. Through the Monitor feature in Web Manager, you may configure the monitoring of a connected serial device through a sequence of five pages via Explorer, or go to a specific Configuration page to make specific changes. The device monitoring status can be viewed through the Status page.

**Note:** *The easiest way to view monitor status or modify monitor settings is through Web Manager, however you can also utilize the CLI and XML (see [To Configure Monitor on page 96](#)).*

## Explorer

Configure the monitoring of a connected serial device through a sequence of pages via Explorer.

**Table 16-1 Monitor Explorer Settings**

| Explorer Settings   | Description  |
|---|--|
| <b>Next/Prev</b> (buttons)  | <p>Click the <b>Next</b> and <b>Prev</b> button to move between the five pages below, through which monitor settings are configured:</p> <ul style="list-style-type: none"> <li>◆ <b>Step 1: Setup Initiation</b></li> <li>◆ <b>Step 2: Setup Commands</b></li> <li>◆ <b>Step 3: Define Filters</b></li> <li>◆ <b>Step 4: Pick Data</b></li> <li>◆ <b>Step 5: Confirm and submit changes</b></li> </ul>  |
| <b>Initial Delay</b>  | <p>Set the initial delay time in milliseconds before the monitor starts processing the initialization message. This field appears in <b>Step 1: Setup Initiation</b>.</p>  |
| <p><b>Message &lt;Number&gt;</b></p> <p><i>Note: In subsequent screens (Commands/ Control and Poll) in Explorer or under Configuration, additional Message &lt;Number&gt; fields will become available to further filter and specify the information you wish to monitor.</i></p> | <p>Click the <b>Edit</b> link to edit a specific message; this is where a command is entered. Four message fields will open to allow configuration of a specific command. When you begin entering information in these fields, additional <b>Message &lt;Number&gt;</b> options become available containing the four message fields which will also open upon clicking <b>Edit</b>. Complete the <b>Message &lt;Number&gt;</b> fields:</p> <ul style="list-style-type: none"> <li>◆ <b>Command:</b> enter the command in binary format (printable characters or binary string)</li> <li>◆ <b>End Character:</b> indicate as a single printable character or as a control character. Control characters may be input as &lt;control&gt;J, 0xA (hexadecimal) or \10 (decimal).</li> <li>◆ <b>Length:</b> set the length of the response. Maximum response length is 2048 bytes.</li> <li>◆ <b>Timeout:</b> set the timeout to receive response. Minimum timeout length is 100 milliseconds.</li> </ul> <p>Click <b>Submit</b> after making changes to get real time response displayed if you are utilizing Explorer.</p>  |
| <b>Delay</b>  | <p>Enter the delay in seconds, minutes, hours and/or days to set the delay waited before the monitor starts processing all poll messages again. 0 means poll messages are sent only once.</p>  |
| <b>Rule &lt;Number&gt;</b>  | <p>Click the <b>Edit</b> link to edit a specific rule in the <b>Step 2: Setup Commands</b> page. Two rule configuration fields will open for this rule. When you begin entering information in these fields, additional <b>Rule &lt;Number&gt;</b> options become available containing the two rule configuration fields which will also open upon clicking <b>Edit</b>. Complete the <b>Rule &lt;Number&gt;</b> fields:</p> <ul style="list-style-type: none"> <li>◆ <b>Source:</b> indicate the input of the filter. For example, if the source of this filter is the second trunk of data created by filter 1, the source should be set to 1.2. A Source of 0 indicates the raw response.</li> <li>◆ <b>Mode:</b> select filter mode (All, Delimiters or Binary)</li> <li>◆ <b>Delimiter &lt;Number&gt; Binary String:</b> Enter the filter breaks input up to 8 trunks separated by binary string. Each trunk will not contain the delimiters. This field appears when Delimiter Mode is selected.</li> <li>◆ <b>Start index:</b> set to indicate when delimiters filter start breaking input into trunks, if the Delimiter Mode is selected.</li> <li>◆ <b>Offset:</b> set the size of the first trunk of data created by the binary filter, if selected.</li> <li>◆ <b>Length:</b> set the size of the second trunk of data created by the binary filter, if selected. The third trunk of data created by the binary filter will contain the rest of the input.</li> </ul> |

| Explorer Settings              | Description   |
|--------------------------------|---|
| <b>Selector &lt;Number&gt;</b> | <p>Click the <b>Edit</b> link to edit a specific selector in <b>Step 4: Pick Data</b> page. Three selector configuration fields will open for this selector. When you begin entering information in these fields, additional <b>Selector &lt;Number&gt;</b> options become available containing the three selector configuration fields which will also open upon clicking <b>Edit</b>. Complete the <b>Selector &lt;Number&gt;</b> fields:</p> <ul style="list-style-type: none"> <li>◆ <b>Name:</b> define the data name as it will display.</li> <li>◆ <b>Response:</b> set the response instance source of data. Response instance corresponds to poll or control message instance.</li> <li>◆ <b>Reference:</b> select the output of the monitor filter. For instance, if data should select the second trunk of data created by filter 1, the reference must be set to 1.2. A Reference of 0 indicates the raw response.</li> </ul> |
| <b>Display</b>                 | <p>Select the desired live response to view at any time while using Explorer, of the monitoring configuration being established. Filter rule options appear according to your progress establishing commands and rules. Changes in what is displayed can be useful during the configuration of monitor settings.</p> <ul style="list-style-type: none"> <li>◆ Responses 1-4</li> <li>◆ Filter Rules 1-4 or All Filter Rulers</li> </ul>   |
| <b>Data</b> (checkbox)         | <p>Check the Data checkbox to enable the Display feature anytime using the Explorer. Uncheck checkbox to disable Display.</p>   |

## Configuration

Configure the monitoring of a connected serial device through specific configuration settings pages : Initialization, Control, Poll , Filter, and Data. Access the configuration options displayed in [Table 16-2](#) on the **Initialization** page. These configuration fields are the same ones in **Step 1: Setup Initiation** if utilizing Explorer.

**Table 16-2 Monitor Initialization Settings**

| Initialization Settings   | Description   |
|---|---|
| <b>Initial Delay</b>  | <p>Set the initial delay time in milliseconds before the monitor starts processing the initialization message. This field also appears in <b>Step 1: Setup Initiation</b>.</p>  |
| <p><b>Message &lt;Number&gt;</b></p> <p><i>Note: In other pages (Commands/Control and Poll) in Explorer or under Configuration, additional Message &lt;Number&gt; fields will become available to further filter and specify the information you wish to monitor.</i></p> | <p>Click the <b>Edit</b> link to edit a specific message; this is where a command is entered. Four message fields will open to allow configuration of a specific command. When you begin entering information in these fields, additional <b>Message &lt;Number&gt;</b> options become available containing the four message fields which will also open upon clicking <b>Edit</b>. Complete the <b>Message &lt;Number&gt;</b> fields:</p> <ul style="list-style-type: none"> <li>◆ <b>Command:</b> enter the command in binary format (printable characters or binary string)</li> <li>◆ <b>End Character:</b> indicate as a single printable character or as a control character. Control characters may be input as &lt;control&gt;J, 0xA (hexadecimal) or \10 (decimal).</li> <li>◆ <b>Length:</b> set the length of the response.</li> <li>◆ <b>Timeout:</b> set the timeout length. Minimum timeout length is 100 milliseconds.</li> </ul> <p>Click <b>Submit</b> after making changes to get real time response displayed if you are utilizing Explorer.</p> |

Access the configuration options displayed in [Table 16-3](#) on the **Control** page. These configuration fields are the same ones in **Step 2: Setup Commands** if utilizing Explorer.

Table 16-3 Monitor Control Settings

| Control Settings  | Description   |
|---|---|
| <p><b>Message &lt;Number&gt;</b></p> <p><i>Note: In other pages (Commands/Control and Poll) in Explorer or under Configuration, additional Message &lt;Number&gt; fields will become available to further filter and specify the information you wish to monitor.</i></p> | <p>Click the <b>Edit</b> link to edit a specific message; this is where a command is entered. Four message fields will open to allow configuration of a specific command. When you begin entering information in these fields, additional <b>Message &lt;Number&gt;</b> options become available containing the four message fields which will also open upon clicking <b>Edit</b>. Complete the <b>Message &lt;Number&gt;</b> fields:</p> <ul style="list-style-type: none"> <li>◆ <b>Command:</b> enter the command in binary format (printable characters or binary string)</li> <li>◆ <b>End Character:</b> indicate as a single printable character or as a control character. Control characters may be input as &lt;control&gt;J, 0xA (hexadecimal) or \10 (decimal).</li> <li>◆ <b>Length:</b> set the length of the response.</li> <li>◆ <b>Timeout:</b> set the timeout length. Minimum timeout length is 100 milliseconds.</li> </ul> <p>Click <b>Submit</b> after making changes to get real time response displayed if you are utilizing Explorer.</p> |

Access the configuration options displayed in [Table 16-4](#) on the **Poll** page. These configuration fields are the same ones in **Step 3: Define Filters** if utilizing Explorer.

Table 16-4 Monitor Poll Settings

| Poll Settings   | Description   |
|---|---|
| <p><b>Message &lt;Number&gt;</b></p> <p><i>Note: In other pages (Commands/Control and Poll) in Explorer or under Configuration, additional Message &lt;Number&gt; fields will become available to further filter and specify the information you wish to monitor.</i></p> | <p>Click the <b>Edit</b> link to edit a specific message; this is where a command is entered. Four message fields will open to allow configuration of a specific command. When you begin entering information in these fields, additional <b>Message &lt;Number&gt;</b> options become available containing the four message fields which will also open upon clicking <b>Edit</b>. Complete the <b>Message &lt;Number&gt;</b> fields:</p> <ul style="list-style-type: none"> <li>◆ <b>Command:</b> enter the command in binary format (printable characters or binary string)</li> <li>◆ <b>End Character:</b> indicate as a single printable character or as a control character. Control characters may be input as &lt;control&gt;J, 0xA (hexadecimal) or \10 (decimal).</li> <li>◆ <b>Length:</b> set the length of the response.</li> <li>◆ <b>Timeout:</b> set the timeout length. Minimum timeout length is 100 milliseconds.</li> </ul> <p>Click <b>Submit</b> after making changes to get real time response displayed if you are utilizing Explorer.</p> |
| <b>Delay</b>  | Set the initial delay time in milliseconds before the monitor starts processing the initialization message. This field appears in <b>Step 1: Setup Initiation</b> .   |

Access the configuration options displayed in [Table 16-5](#) on the **Filter** page. These configuration fields are the same ones in **Step 3: Define Filters** if utilizing Explorer.

Table 16-5 Monitor Filter Settings

| Filter Settings | Description  |
|-----------------|--|
| Rule <Number>   | <p>Click the <b>Edit</b> link to edit a specific rule. Two rule configuration fields will open for this rule. When you begin entering information in these fields, additional <b>Rule &lt;Number&gt;</b> options become available containing the two rule configuration fields which will also open upon clicking <b>Edit</b>. Complete the <b>Rule &lt;Number&gt;</b> fields:</p> <ul style="list-style-type: none"> <li>◆ <b>Source:</b> indicate the input of the filter. For example, if the source of this filter is the second trunk of data created by filter 1, the source should be set to 1.2. A Source of 0 indicates the raw response.</li> <li>◆ <b>Mode:</b> select filter mode (All, Delimiters or Binary)</li> <li>◆ <b>Delimiter &lt;Number&gt; Binary String:</b> Enter the filter breaks input up to 8 trunks separated by binary string. Each trunk will not contain the delimiters. This field appears when Delimiter Mode is selected.</li> <li>◆ <b>Start index:</b> set to indicate when delimiters filter start breaking input into trunks, if the Delimiter Mode is selected.</li> <li>◆ <b>Offset:</b> set the size of the first trunk of data created by the binary filter, if selected.</li> <li>◆ <b>Length:</b> set the size of the second trunk of data created by the binary filter, if selected. The third trunk of data created by the binary filter will contain the rest of the input.</li> </ul> |

Access the configuration options displayed in [Table 16-6](#) on the Data page. These configuration fields are the same ones in **Step 4: Pick Data** if utilizing Explorer.

Table 16-6 Monitor Data Settings

| Data Settings     | Description  |
|-------------------|--|
| Selector <Number> | <p>Click the <b>Edit</b> link to edit a specific selector. Three selector configuration fields will open for this selector. When you begin entering information in these fields, additional <b>Selector &lt;Number&gt;</b> options become available containing the three selector configuration fields which will also open upon clicking <b>Edit</b>. Complete the <b>Selector &lt;Number&gt;</b> fields:</p> <ul style="list-style-type: none"> <li>◆ <b>Name:</b> define the data name as it will display.</li> <li>◆ <b>Response:</b> set the response instance source of data. Response instance corresponds to poll or control message instance.</li> <li>◆ <b>Reference:</b> select the output of the monitor filter. For instance, if data should select the second trunk of data created by filter 1, the reference must be set to 1.2. A Reference of 0 indicates the raw response.</li> </ul> |

## To Configure Monitor

The easiest way to view monitor status or modify monitor settings is through Web Manager, however you can also utilize the CLI and XML.

### Using Web Manager

- ◆ To view monitor status or modify monitor settings, go to **Monitor** on the menu.

### Using CLI

- ◆ To enter the Monitor command level: `config -> Monitor`

### Using XML

- ◆ Include in your file: `<configgroup name = "Monitor Initialization">`
- ◆ Include in your file: `<configgroup name = "Monitor Control">`
- ◆ Include in your file: `<configgroup name = "Monitor Poll">`
- ◆ Include in your file: `<configgroup name = "Monitor Filter">`
- ◆ Include in your file: `<configgroup name = "Monitor Data">`

## Example: Data Capture on a Serial Device

Connect the xPico Wi-Fi serial port to a serial device, then query and capture desired information periodically, presenting this information on a Web page.

### Sample Configuration

- ◆ Connect to the Command Line Interface (CLI) on the EDS2100. The CLI has menu levels, so we will send commands to exit through multiple levels, knowing that an exit at the top level will just return us to the top level. Then we can enter the "enable" command level.
- ◆ Use a null modem cable to connect xPico Wi-Fi unit Line 1 to a Lantronix EDS2100 Line 1.
- ◆ Set both devices to 115200 bits per second, no parity, 8 data bits, 1 stop bit, hardware flow control.
- ◆ Set the first three message Commands to send "exit[0x0d]", the fourth "enable[0x0d]"

## Initialization

Upon xPico Wi-Fi power-up, the state of the external serial device is not known. Monitor will send one or more messages to bring the serial device into a known state.

### STEP 1 - STRATEGY

Explore your serial device and determine your strategy for bringing it to the desired starting state.

### STEP 2 - CONNECTION

Connect your serial device to your xPico Wi-Fi unit.

### STEP 3 - LINE SETTINGS

Set serial line speed, flow control, and character options on both devices so they are compatible. On xPico Wi-Fi unit, select "Monitor" under Line Protocol.

### STEP 4 - MONITOR INITIALIZATION

Use Monitor Explorer or directly configure settings in Monitor Initialization Configuration. In [Figure 16-7 Monitor Initialization](#) the example configuration is typed into the Monitor Explorer web page.

**Note:** Non-printable characters are placed in the Command within square brackets. The "Enter" key on your PC is an ASCII Carriage Return, code 0x0d.

**Note:** After each message Command is sent, the Monitor may wait for a response. You may set the Timeout for each message. If the Timeout is too short, your device may become out of sync with Monitor. So make your timeout comfortably high, and then if applicable define an End Character or Length so it will move on without waiting further.

## Polling

Periodically your xPico Wi-Fi will send commands to query information from your serial device.

### STEP 1 - STRATEGY

Explore your serial device and determine your strategy for eliciting all of the desired data with the fewest message Commands.

### STEP 2 - SETUP

Use Monitor Explorer or directly configure settings in Monitor Poll Configuration. For each message Command, determine an appropriate Timeout and possibly shorten it via a Length and/or End Character.

Figure 16-7 Monitor Initialization

Figure 16-8 Monitor Polling (1 of 2)

### STEP 3 - TEST

Testing is rapid and simplified using Monitor Explorer. You can see the serial device response right in your browser window.

#### Sample Configuration

- ◆ Use a single "show" command to elicit the EDS2100 device status.
- ◆ In Monitor Poll Configuration, set Message 1 Command to "show[0x0d]".
- ◆ Testing with this, notice that the default Timeout of 100 milliseconds is too fast—we sometimes poll before all the data comes out. So we set Timeout to 200 milliseconds for stable operation.

**Note:** It is possible to poll with more than one message Command. They will be sent sequentially, and you will define distinct filtering and data mining steps for each.

### Filtering

The response to each poll will be sliced up according to your filter rules. The objective is to simply slice enough so you can subsequently point to the data fields you want to mine.

Note the raw data in the grey box above; it reflects what was received from the serial device. See "Uptime" in the top right region—that's our target for the example.

### STEP 1 - STRATEGY

Carefully examine the form of the response you received from a particular poll. Look for cues in the response to locate your desired information. Consider if the form of the response might have variations depending on the serial device state.

### STEP 2 - SETUP

Use Monitor Explorer or directly configure settings in Monitor Filter Configuration. Rules are performed sequentially, but note that you can point each Rule to either the raw source (0) or a result of a previous rule (R.f). Each rule (R) slices the raw input into multiple fields (f), so with a dot between them (R.f) you are selecting a particular sliced result from a Rule.

Figure 16-9 Monitor Polling (2 of 2)

Status **Explorer** Configuration

Monitor Explorer

< Prev Step 2: Setup commands. Next >

|                |                            |              |
|----------------|----------------------------|--------------|
| Message 1:     | show[0x0d], <None>, 0, 200 | [ Hide ]     |
| Command:       | show[0x0d]                 |              |
| End Character: | <None>                     |              |
| Length:        | 0                          | bytes        |
| Timeout:       | 200                        | milliseconds |
| Message 2:     | <None> [ Edit ]            |              |
| Delay:         | 2 seconds                  |              |

Submit

Figure 16-10 Monitor Filtering (1 of 2)

Status **Explorer** Configuration

Monitor Explorer

< Prev Step 3: Define filters. Next >

Rule 1: <None> [ Edit ]

Display: Response 1 [v] All Filter Rules [v]  Data

```
0: show[0x0d, 0x0a]Product Information:[0x0d, 0x0a] Product
Type : Lantronix EDS2100 (EDS2100)[0x0d, 0x0a] FW Version
/ Date : 5.2.0.3B2 / Aug 8 2012 (17:26:30)[0x0d, 0x0a] Serial
Number : 07101017G6KROD[0x0d, 0x0a] Uptime : 8
days 00:08:30[0x0d, 0x0a] Perm. Config : saved[0x0d,
0x0a]Network Status:[0x0d, 0x0a] Interface : eth0[0x0d,
0x0a] Link : Auto 10/100 Mbps Auto Half/Full (100 Mbps
Half)[0x0d, 0x0a] MAC Address : 00:20:4a:a8:8b:bd[0x0d,
0x0a] Hostname : <None> [[<DHCP>]][0x0d, 0x0a]
Domain : eng.lantronix.com (DHCP) [[<DHCP>]][0x0d,
0x0a] IP Address : 172.19.100.17/16 (DHCP) [[<DHCP>]]
[0x0d, 0x0a] Default Gateway : 172.19.0.1 [[<DHCP>]][0x0d,
0x0a] Primary DNS : 172.19.1.1 (DHCP)[0x0d, 0x0a]
Secondary DNS : 172.19.1.2 (DHCP)[0x0d, 0x0a]
MTU : 1500 [[<DHCP>]][0x0d, 0x0a] VIP Conduit :
Disabled[0x0d, 0x0a]Line 1:[0x0d, 0x0a] RS232, 115200, None, 8,
1, Hardware [[CL]][0x0d, 0x0a] Tunnel Connect Mode: Waiting,
Accept Mode: Waiting[0x0d, 0x0a]Line 2:[0x0d, 0x0a] RS232,
115200, None, 8, 1, Hardware[0x0d, 0x0a][enable]#
```

**STEP 3 - TEST**

Testing is rapid and simplified using Monitor Explorer. You can see the response data sliced into pieces right in your browser windows.

**Sample Configuration**

- ◆ First slice the response into lines, point to the one containing Uptime, then slice between the caption and the time value.
- ◆ Setup as follows:
  - We could see the Carriage Return / Line Feed sequence in our raw source.
  - Rule 1 points to the raw source (Source 0), Mode = Delimiters, Delimiter 1 Binary String = "[0x0d 0x0a]".
  - We can see our Uptime is in the sixth field.
  - Rule 2 dices that field (Source 1.6) further, to split the caption from the value.
  - We see that a colon (:) separates the caption from the data, but the data also contains colons.
  - Rule 2 Mode - Delimiters, Delimiter 1 Binary String = " ." (that's a space followed by a colon). We use the space so it will match the transition from caption to value, but not match within the Uptime value itself.
- ◆ Testing with this, confirm that the desired data is contained in a single field.

**Note:** Some devices might use a variable number of lines to display status depending on the device state. If so, slicing first by lines will not consistently point to the desired data. Instead, consider a different strategy:

- ◆ Rule 1 can use Mode = Delimiters, but set the Delimiter 1 Binary String = caption.
- ◆ Its field 2 contains all of the response following the caption.
- ◆ Use Rule 2 or more to further slice 1.2 (Rule 1 field 2) in order to separate the value from anything following the caption and from the rest of the response.

**Figure 16-11 Monitor Filtering (2 of 2)**

The screenshot shows the Monitor Explorer configuration interface. At the top, there are tabs for 'Status', 'Explorer', and 'Configuration'. Below that, the title 'Monitor Explorer' is displayed. The main area shows 'Step 3: Define filters.' with navigation buttons for '< Prev' and 'Next >'. A table lists three filter rules:

|         |                                       |          |
|---------|---------------------------------------|----------|
| Rule 1: | 0, Delimiters, [0x0d 0x0a], , 0, 0, 0 | [ Edit ] |
| Rule 2: | 1.6, Delimiters, . , 0, 0, 0          | [ Edit ] |
| Rule 3: | <None>                                | [ Edit ] |

Below the table, the 'Display' section shows 'Response 1' selected in a dropdown, 'Filter Rule 2' selected in another dropdown, and an unchecked 'Data' checkbox. The resulting filtered data is shown in a list:

- 1.6: Uptime : 8 days 00:08:30 ...<Summarized>
- 2.1: Uptime
- 2.2: 8 days 00:08:30

## Data Mining

You have already sliced the raw data multiple ways using the Filter Steps. Now you will select the data to be mined.

### STEP 1 - STRATEGY

You can have multiple Poll messages, and different Filter Steps will generally apply to each, but some Filter Steps may be shared. Here is where you put it all together. The neat thing is that all the slicing of the raw data is virtual, so all of your Filter Rules overlay raw data from each response, but you need only care about some of them on a particular Poll message.

### STEP 2 - SETUP

Use Monitor Explorer or directly configure settings in Monitor Data Configuration. Each Selector picks out a distinct data item you wish to subsequently present. The Selector Name will be presented as the caption for your data. Selector Response is a Message number; it selects the response from that Message. Selector Reference is a Rule number, dot, and a field number; it selects the desired data field.

Bottom line, you have placed a stake in the ground naming a result, identifying which poll response it comes from, and which field to pick up.

### STEP 3 - TEST

Testing is rapid and simplified using Monitor Explorer. You can see the selected field contents right in your browser window.

#### Sample Configuration

- ◆ We'll name our result "Up time". It goes in Monitor Data Configuration under "Name".
- ◆ We only used one Poll message, so "Response" is just "1".
- ◆ Our desired data is from Rule 2, field 2. So "Reference" is "2.2".

Figure 16-12 Monitor Data Mining (1 of 2)

Status Explorer Configuration

Monitor Explorer

< Prev Step 4: Pick data. Next >

Selector 1: <None> [Edit]

Display: Response 1 Filter Rule 2

No data available.

1.6: Uptime : 8 days 00:08:30 ...<Summarized>

2.1: Uptime

2.2: 8 days 00:08:30

Figure 16-13 Monitor Data Mining (2 of 2)

Status Explorer Configuration

Monitor Explorer

< Prev Step 4: Pick data. Next >

|             |                  |        |
|-------------|------------------|--------|
| Selector 1: | Up time, 1, 2, 2 | [Hide] |
| Name:       | Up time          |        |
| Response:   | 1                |        |
| Reference:  | 2.2              |        |
| Selector 2: | <None>           | [Edit] |

Display: Response 1 Filter Rule 2

Data 1 Up time,1,2,2 8 days 00:08:30

1.6: Uptime : 8 days 00:08:30 ...<Summarized>

2.1: Uptime

2.2: 8 days 00:08:30

## Presenting

### STEP 1 - STRATEGY

Here you consider your options for sharing the data you have mined. For human users, a Web page presentation is simplest. For machine-to-machine communication, XML might be best. Command Line could be used for either.

### STEP 2 - SETUP

Automatically your data is available under status on the Web Manager, XML, and CLI.

Advanced Web customization can be done with HTML and JavaScript files dropped into the xPico Wi-Fi unit.

### STEP 3 - TEST

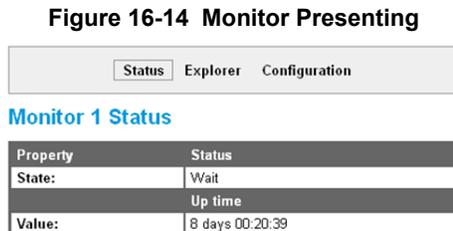
With the Web Manager, view all of your data under Monitor Status.

In the Command Line Interface (CLI), first type "status" to enter the status menu level, then type "monitor" for the Monitor menu level. From there, type "show" for the data.

In the XML status dump, find statusgroup name = "Monitor", then statusitem name = "data" instance = "<the name you gave your data>", and value contains the data received.

### Sample Configuration

- ◆ We visit our device Web Manager, select the "Monitor" tab at the left of the display, the select "Status" at the top of the display. Our "Up time" and the present value appear there.



**Figure 16-15 Monitor CLI Command Level**

```

COM20:115200baud - Tera Term VT
File Edit Setup Control Window Help

>status
status>monitor
status Monitor>show
Monitor Status:
  State: Wait
  Data Up time
  Value: 8 days 00:21:55
status Monitor>

```

- ◆ Visiting the Command Line Interface, we type "status", then "monitor", then "show". We see "Up time" presented there.

Figure 16-16 Monitor XML Commands

```

COM1:115200baud - Tera Term VT
File Edit Setup Control Window Help
>xml
xml>xsr dump monitor
<?xml version="1.0" standalone="yes"?>
<!-- Automatically generated XML -->
<!DOCTYPE statusrecord I
  <?ELEMENT statusrecord (statusgroup+)>
  <?ELEMENT statusgroup (statusitem+,statusgroup*)>
  <?ELEMENT statusitem (value+)>
  <?ELEMENT value (#PCDATA)>
  <?ATTLIST statusrecord version CDATA #IMPLIED>
  <?ATTLIST statusgroup name CDATA #IMPLIED>
  <?ATTLIST statusgroup instance CDATA #IMPLIED>
  <?ATTLIST statusitem name CDATA #IMPLIED>
  <?ATTLIST statusitem instance CDATA #IMPLIED>
  <?ATTLIST value name CDATA #IMPLIED>
]
<statusrecord version = "0.1.0.1">
  <statusgroup name = "Monitor">
    <statusitem name = "State">
      <value>Wait</value>
    </statusitem>
    <statusitem name = "Data" instance = "Uptime">
      <value name = "Value">0 days 00:05:54</value>
    </statusitem>
  </statusgroup>
</statusrecord>
xml>

```

- ◆ For XML we start at the root Command Line Interface, type "xml", then "xsr dump monitor". We see a statusitem name = "data", instance = "Up time", with value containing the present data.

## Data Capture on SPI

Connect xPico Wi-Fi SPI port to peripheral device, query and capture desired information periodically, present on Web page.

## 17: Branding the xPico Wi-Fi Unit

This chapter describes how to customize the Web Manager user interface of your xPico Wi-Fi embedded device server.

### Customizing Web Manager Appearance

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

The Web Manager files are hidden and are incorporated directly into the firmware image but may be overridden by placing the appropriate file in the appropriate directory within the xPico Wi-Fi file system.

#### To upload alternative Web Manager branding instructions:

1. Either create a file from scratch, or edit a copy of the existing Lantronix file. To edit a copy of the original file, do the following:
  - a. Obtain the file by entering the following path in a browser:  
`http://<hostname>/embedded/main/http/web_manager/<filename>`  
(or `http://<hostname>/embedded/main/http/web_manager/img/<filename>` for some files – see below).
  - b. Then save the file (in the case of *index.html*, you may need to set the browser to view the page source).
  - c. Modify the file as required.
2. Create a path in the file system (the entire path can be created in a single step via either the Web Manager or CLI). The path is the same as that for the hidden files, except for the top-level */embedded* directory: `/main/http/web_manager/`
3. Upload your file into the directory in step 2.
4. Restart the browser to view the changes.

To go back to the default files in the firmware image, simply delete the overriding files in the file system (the directories can be left intact if so desired).

#### Path Format

As mentioned above, the root directory for hidden files built into the firmware is */embedded*. When overriding these hidden files by placing your own copies in the file system, the path is identical but for the */embedded* top directory. For example, the built-in hidden file `/embedded/main/http/web_manager/index.html` is overridden by the real file system file `/main/http/web_manager/index.html`.

If you need to refer to an overridden file within your own web files, the path follows the same format, except the */embedded* top directory of the hidden file path is replaced by */.overlay*. So, to refer to *style.css* from within *index.html*, the path in *index.html* is `/.overlay/main/http/web_manager/style.css`. This format allows the system to look first for an overriding copy of the file before using the built-in copy.

## Other Overridable Files

In addition to `index.html`, and `style.css`, a few other presentation-related files can be overridden. The complete list is as follows:

- ◆ `/main/http/web_manager/index.html` – Main file controlling text and graphics
- ◆ `/main/http/web_manager/style.css` – Style sheet
- ◆ `/main/http/web_manager/img/bg.gif` – Main background
- ◆ `/main/http/web_manager/img/company_logo.gif` – Company logo in header container
- ◆ `/main/http/web_manager/img/product_logo.gif` – Product logo in header container
- ◆ `/main/http/web_manager/img/favicon.ico` – Shortcut icon
- ◆ `/main/http/web_manager/img/header_bg.gif` – Head container background

Note that many of the embedded files are compressed to save space. When overriding files, the user-supplied files can be either compressed or uncompressed, but must indicate so by the file name extension.

For example, the `style.css` file is actually stored as `/embedded/main/http/web_manager/index/style.css.gz`. But it can be overridden with either an uncompressed version as `/main/http/web_manager/index/style.css`, or a compressed version as `/main/http/web_manager/index/style.css.gz`.

## Adding Your Own Web Files

Users can also add their own web files. These must be placed in the `/http` directory. This directory does not exist by default and must be created by the user.

## Creating Your Own Webpages

If instead of modifying the existing pages, you would like to create your own pages, you can do so easily by placing your source files in the `/http/` directory of the filesystem. You will need to create the directory first.

Any HTML file placed there will be served at the root of the web server. That is, if you create a file called `/http/test.html`, it will be seen at address:

```
http://<ip-address-of-xPico-gateway>/test.html
```

## OEM Configgroup Options

Please see Chapter 6: OEM Management for OEM configuration options available through the OEM configgroup.

## 18: Updating Firmware Over the Air

The xPico Wi-Fi embedded device server supports a robust over the air (OTA) firmware update capability. This can be performed either via the on-device web manager or by using WebAPI to support a scripted method. The Lantronix method is user friendly with no setup required, uses the existing WLAN configuration and preserves the device configuration through the updater process. Updates are protected against failure so that if anything should happen to interrupt the process the device is not made inoperable. OTA updates are stored on the device internal Flash simplifying the integration of this capability into a final product.

### Obtaining Firmware

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

### Loading New Firmware through Web Manager

Upload the firmware using the device Web Manager **Device** page.

#### *To upload new firmware:*

1. Select **Device** in the menu bar. The **Device Status** page appears.

**Note:** See *Device Settings (on page 79)* for options to restore factory defaults or reboot the device.

Figure 18-1 Uploading New Firmware

The screenshot shows the xPico Wi-Fi web interface. The top header includes the xPico Wi-Fi logo and the LANTRONIX logo. A navigation menu on the left lists various settings categories, with 'Device' highlighted. The main content area is titled 'Device Status' and contains a table of device properties and their current status. To the right of the table, there is a note stating 'This displays the current status of the Device.' and a '[Logout]' link. At the bottom of the table, there are four buttons: '[ Save ]', '[ Reboot ]', '[ Factory Defaults ]', and '[ Firmware Upload ]'.

| Property             | Status                 |
|----------------------|------------------------|
| Product Type:        | xPicoWifi              |
| Product ID:          | Y1                     |
| Product SKU:         | XPW1001                |
| Antenna:             | External               |
| Serial Number:       | 0080A3A00382           |
| Firmware Version:    | 1.5.0.0R42             |
| Build Date:          | Feb 13 2018 (10:34:15) |
| Bootloader Version:  | 1.0.0.0R7              |
| Bootloader Date:     | Apr 2 2014 17:55:26    |
| OTA Upgrade Version: | 1.2.0.0R1              |
| Uptime:              | 12 days 19:15:58       |
| Permanent Config:    | saved                  |
|                      | [ Save ]               |
|                      | [ Reboot ]             |
|                      | [ Factory Defaults ]   |
|                      | [ Firmware Upload ]    |

Copyright © Lantronix, Inc. 2007-2018. All rights reserved.

2. Click **Firmware Upload**.
3. Click **Okay** to confirm uploading a new firmware image. You will be redirected to the Firmware Upgrade page.
4. Click **Browse...** to browse to the firmware file.
5. Select the file and click **Open**.
6. Click **Upgrade** to install the firmware on the xPico Wi-Fi embedded device server.
7. Click **OK** in the confirmation pop-up which appears. The firmware will be installed and the device will automatically reboot afterwards.
8. Close and reopen the Web Manager Internet browser to view the device's updated web pages.

## Loading New Firmware without Web Manager

Firmware can be uploaded without using the Web Manager. It is possible to use a client like cURL as part of a scriptable upgrade.

The following is an example of how to use cURL to perform an OTA firmware upload.

```
#
# Example script for xPicoWifi OTA firmware upgrade
#
curl--digest -u admin:PASSWORD -X POST -d "group=Device&action=Firmware
Upload" http://<hostname>/action/status

# The system will take some time to reboot and start the OTA firmware
curl -X POST -F
datafile=@xPicoWifi_1.5.0.0R43.rom http://<hostname>/upgrade
curl -X POST http://<hostname>/reboot
```

## Importing WLAN Configuration with XML

WLAN configuration can be exported and imported between devices.

1. Export an xml wlan configuration from a device.
2. Manually replace the "&lt;Configured>" placeholder for each secret field in the XML with the actual secret value.

**Note:** Five special characters must be replaced as follows:

|   |          |
|---|----------|
| & | &amp;    |
| < | &lt;&gt; |
| > | &gt;     |
| ' | &apos;   |
| " | &quot;.  |

3. Import the configuration to the desired device.

## Appendix A: Command Reference

The xPico Wi-Fi embedded device server supports four convenient configuration methods: Extensible Markup Language (XML), Web Manager, Command Line Interface (CLI), and WebAPI. This chapter describes how to configure the xPico Wi-Fi embedded device server using Extensible Markup Language (XML). This appendix describes how to configure the xPico Wi-Fi embedded device server using the Command Line Interface (CLI). CLI provides an interactive mode for accessing the device configuration and management interface. It is most suited for system and network administrators comfortable with using similar interfaces on Enterprise IT and Networking products. It is also helpful as a quick tool for access via the product's serial ports or console/management ports. XML provides an extensible mode for software developers.

**Note:** For more information about the Web Manager, see [Chapter 4: Configuration Using Web Manager](#). For more information about using XML to access device configuration and management interface, see [Configuration Using Serial Port on page 110](#). For more information about using Web API to configure and manage the xPico Wi-Fi device, see [Chapter 5: WebAPI](#).

### Conventions

The table below lists and describes the conventions used in this book.

| Convention                       | Description  |
|----------------------------------|--|
| <b>Bold text</b>                 | Default parameters.  |
| <i>Italic text</i>               | Required values for parameters   |
| <b>Brackets [ ]</b>              | Optional parameters.   |
| <b>Angle Brackets &lt; &gt;</b>  | Possible values for parameters.  |
| <b>Pipe  </b>                    | Choice of parameters.  |
| <b>Warning</b>                   | <b>Warning:</b> Means that you are in a situation that could cause equipment damage or bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents. |
| <b>Note</b>                      | <b>Note:</b> Means take notice. Notes contain helpful suggestions, information, or references to material not covered in the publication.  |
| <b>Caution</b>                   | <b>Caution:</b> Means you might do something that could result in faulty equipment operation, or loss of data.   |
| <b>Screen Font (Courier New)</b> | CLI terminal sessions and examples of CLI input.   |

## Configuration Using Serial Port

### Serial Command Mode

The serial port can be configured to operate in command mode permanently or to be triggered under specified conditions. See [Line Settings \(Serial\) \(on page 50\)](#) for more information.

### Boot to CLI

Regardless of the configured settings, the CLI can be accessed via Line 1 using fixed settings and the "back door" procedure. The original configured line settings will be restored once the user exits the "back door" CLI, unless any Line 1 settings are changed within the "back door" CLI.

To configure the Lantronix xPico Wi-Fi embedded device server locally using a serial port:

**Note:** *The xPico Wi-Fi embedded device server requires that flow control be used on the serial port to ensure the best performance when importing XML.*

1. Connect a terminal or a PC running a terminal emulation program to one of the xPico Wi-Fi embedded device server's serial ports.
2. Configure the terminal to the following settings:
  - ◆ 9600 baud
  - ◆ 8-bit
  - ◆ No parity
  - ◆ 1 stop bit
  - ◆ No flow control
3. Power off the device.
4. Get into the serial backdoor as follows:
  - a. While asserting the defaults signal,
  - b. Reset the device while sending X, Y, or Z characters.
  - c. When the incoming characters are recognized, a prompt in the following form will be seen:  
`xPicoWifi <MAC ADDRESS>`

**Note:** *It is important to release the defaults signal as soon as possible after the prompt is seen; continuing to hold it down may result in a reset to factory defaults.*

### OR

- a. While asserting the defaults signal,
- b. Reset the device while sending ! character until it is echoed back.
- c. Then release the defaults line, and enter xyz.

## Navigating the CLI Hierarchy

The CLI is organized into a hierarchy of levels. Each level has a group of commands for a specific purpose. For example, to view diagnostic or device status, one would navigate to the `status` level where they could then navigate to `diagnostics` or `device`.

- ◆ To move to a different level—Enter the name of the level from within its parent level. For example, to enter the file system level, type `file system` at the enable prompt.
- ◆ To exit and return to one level higher—Type `exit` and press the **Enter** key.
- ◆ To view the current configuration, enter the config level by typing `config`.
- ◆ To view the list of commands available at the current level—Type the question mark `?`. Items within `< >` (e.g. `<string>`) are required parameters.
- ◆ To view the available commands and explanations—Type the asterisk `*`.
- ◆ To view the list of commands available for a partial command—Type the partial command followed by the question mark `"?"`. For example: `config>?` displays a list of all config commands at the config level.
- ◆ To view available commands and their explanations for a partial command—Type an asterisk `*`. For example: `config Access Point>*` displays a list of all access point commands and descriptions at the config > access point level.
- ◆ To view SPI configurations, enter the config level by typing `config` at the root level, and then the SPI level by typing `SPI`.
- ◆ To view the tlog, type `tlog` or `t` at the root level.

## Using Keyboard Shortcuts and CLI

One useful shortcut built into xPico Wi-Fi embedded device server is that the complete text of a command does not have to be entered to issue a command. Typing just enough characters to uniquely identify a command, then hitting enter, can be used as a short cut for a command. For example, at the enable level, "sh" can be used for the "show" command.

Tab Completion is also available using the **Tab** and **Enter** keys on the keyboard. Typing the first few characters of a command, then hitting the **Tab** key displays the first command that begins with those characters. Hitting the **Tab** key again displays the next command that begins with the original characters typed. You can press **Enter** to execute the command or you can backspace to edit any parameters.

The following key combinations are allowed when configuring the Pico Wi-Fi embedded device server using the CLI:

**Table A-1 Keyboard Shortcuts**

| Key Combination | Description                              |
|-----------------|--|
| <b>Ctrl + a</b> | Places cursor at the beginning of a line |
| <b>Ctrl + b</b> | Backspaces one character                 |
| <b>Ctrl + d</b> | Deletes one character                    |
| <b>Ctrl + e</b> | Places cursor at the end of the line     |
| <b>Ctrl + f</b> | Moves cursor forward one character       |

| Key Combination (continued) | Description  |
|-----------------------------|--|
| Ctrl + k                    | Deletes from the current position to the end of the line |
| Ctrl + l                    | Redraws the command line                                 |
| Ctrl + n                    | Displays the next line in the history                    |
| Ctrl + p                    | Displays the previous line in the history                |
| Ctrl + u                    | Deletes entire line and places cursor at start of prompt |
| Ctrl + w                    | Deletes one word back                                    |
| Ctrl + z                    | Exits the current CLI level                              |

## Understanding the CLI Level Hierarchy

The CLI hierarchy is a series of levels. Arranging commands in a hierarchy of levels provides a way to organize and group similar commands, provide different levels of security, and reduce the complexity and number commands and options presented to a user at one time.

When you start a command line session, you begin at the root level. This level can be password protected and provides access to high level status, a few diagnostic commands, and the file system level. Further device information and configuration are accessed via the enable level.

The enable level can also be password protected and is the gateway to full configuration and management of the xPico Wi-Fi embedded device server. There are commands for gathering and effecting all elements of device status and configuration, as well as commands that take you to additional levels. For instance, tunnel specific status and configuration is found under the "tunnel" level, and network specific status and configuration commands are found under the "configuration" level.

Commands at the root level (see [Figure A-2 Root Level Commands](#) below) do not affect current configuration settings and are not displayed initially. If you type ?, you will see the login sub-commands. These commands provide diagnostic and status information only.

**Figure A-2 Root Level Commands**

```
Command Line started.

>?
config                documentation
file system           help
status                tlog
wlan scan [network-name]  xml
exit

>
```

---

## XML for xPico Wi-Fi Embedded Device Server

### **configgroup Access Point**

These settings pertain to the **Access Point** in the device. **Changes take effect immediately.** After saving the changes, re-establish any connections to the Access Point.

#### **configitem SSID**

value

**SSID** may contain up to 32 characters.

**SSID** may contain one or more **Directives** of the form %<option>.

Blank the value to restore the default.

**Directives:**

%s (serial number)

%<n>s (first <n> characters of serial number)

%-<n>s (last <n> characters of serial number)

%% %

#### **configitem Guest**

value

**Guest** may be "Enabled" or "Disabled".

"Enabled" allows clients to discover our SSID via a passive scan.

"Disabled" causes this device to ignore probe requests with the wildcard SSID.

In either case this device responds to directed scans that contain our SSID.

#### **configitem Channel**

value

**Channel** configured here is applicable only if wlan0 is down or disabled.

If wlan0 is up, its associated Access Point will set the channel, and ap0 must also operate on that same channel.

#### **configitem Suite**

value

**Suite** may be "None", "WPA" or "WPA2".

#### **configitem Encryption**

value

**Encryption** may contain combinations of "CCMP" or "TKIP".

### **configitem Passphrase**

value

**Passphrase** may contain up to 63 characters.

The value is `HIDDEN`.

### **configitem Mode**

value

**Mode** may be "Always Up", "Triggered" or "Initial Trigger".

"Always Up" brings ap0 up unconditionally.

"Triggered" waits for CPM Role "AP Trigger" to become active. Then ap0 stays up according to **Uptime**.

"Initial Trigger" waits for CPM Role "AP Trigger" to become active. Then ap0 stays up indefinitely.

### **configitem Uptime**

value

**Uptime** has units of seconds, minutes, and/or hours.

**Uptime** designates the time that ap0 will remain up after it has been triggered.

### **configitem DNS Redirect**

value

**DNS Redirect** may contain up to 128 characters.

The **DNS Redirect** name will map to the IP address of the Interface. It may contain upper case, but note that DNS names are case insensitive.

Blank to restore the default.

### **configgroup Clock**

These settings pertain to the **Clock** settings for keeping time.

### **configitem Source**

value

**Source** may be "Manual" or "NTP".

### **configitem UTC Offset**

value

**UTC Offset** may contain up to 5 characters.

**UTC Offset** must be in the range of -1440 to 1440, and be a multiple of 15 minutes.

Lists of common time zones and corresponding **UTC Offset** can be found at several websites, including "<http://www.iana.org/time-zones>".

## configgroup CPM

These settings pertain to the Configurable Pin Manager (**CPM**). Changes take effect immediately.

### configitem Role

"AP Trigger" turns on ap0 if **Mode** is "Triggered" or "Initial Trigger".

"HTTP Server Trigger" turns on HTTP Server if **Mode** is "Triggered".

"Line 1 DSR" read by application.

"Line 1 DTR" set by application.

"Line 2 DSR" read by application.

"Line 2 DTR" set by application.

"Line 2 Flow.CTS" allows send if **Flow Control** is "Hardware".

"Line 2 Flow.RTS" active says can receive if **Flow Control** is "Hardware".

"Radio Trigger" turns on radio if **Mode** is "Triggered".

"SPI.CS" pin is used when SPI **State** is "Enabled".

"SPI.MISO" pin is used when SPI **State** is "Enabled".

"SPI.MOSI" pin is used when SPI **State** is "Enabled".

"SPI.SCK" pin is used when SPI **State** is "Enabled".

"User Data Updated" is active when user data changes, till **Acknowledge** action.

"WLAN Active" is active while wlan0 is up.

value CP

Blank the value for "<No CP Selected>".

This is the number of the Configurable Pin (**CP**) assigned to the role.

value State

**State** may be "Enabled" or "Disabled".

"Enabled" allows the application to use the designated Configurable Pin.

Note that some Roles (those containing a ".") are bundled into a group. Enabling / Disabling any one of them also Enables / Disables the rest of the Roles in the same Group.

value Assert

**Assert** may be "High" or "Low".

**Assert** reflects the logical polarity of this Configurable Pin.

"High" means that a logical "1" corresponds to a voltage high condition on the pin.

"Low" means that a logical "1" corresponds to a voltage low condition on the pin.

value Mode

**Mode** may be "Push-Pull" or "Weak Pullup".

**5-Volt tolerance NOTE:** In order to sustain a voltage higher than VDD+0.3, the Mode must be set to "Push-Pull".

## configgroup HTTP Server

These settings pertain to the **HTTP Server**. **Changes will take effect after reboot.**

### configitem Mode

value

**Mode** may be "Disabled", "Enabled" or "Triggered".

"Disabled" prevents HTTP from operating on any port.

"Enabled" allows the HTTP Server to operate.

"Triggered" waits for CPM Role "HTTP Server Trigger" to become active. Then the HTTP Server stays up indefinitely.

### configitem Port

value

Enter 0 for "<None>".

The default **Port** can be overridden.

### configitem Authentication Timeout

value

**Authentication Timeout** has units of minutes.

The **Authentication Timeout** applies only if Digest authentication is being used.

### configitem Inactivity Timeout

value

**Inactivity Timeout** has units of seconds, minutes, and/or hours.

The **Inactivity Timeout** applies only if the Application "HTTP Server" is enabled in the Power settings.

The HTTP Server will hold power on this long after it completes a request.

## configgroup HTTP Server Security

These settings pertain to the **HTTP Server Security**. **Changes take effect immediately.**

### configitem Access Control

The XML **instance** may range from 1 to 5.

value URI

**URI** may contain up to 255 characters.

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

The **URI** must begin with /.

For example, create URI "/Welcome", then place your "hello.html" file in directory "/http/Welcome/", finally point your browser to "<device IP address>/Welcome/hello.html" to experiment with the authorization levels.

The following **URIs** are built in to the server:

"/ajax" Web Manager

"/logout" Digest authentication

"/mux\_http" Mux HTTP listener

"/tlog" Trouble log

value AuthType

**AuthType** may be "None", "Basic" or "Digest".

"None" requires no authentication.

"Basic" encodes passwords using Base64.

"Digest" hashes passwords using MD5.

value User Level

**User Level** may be "User", "Tech", "Admin" or "None".

"User" provides access to all users.

"Tech" provides users with **Privilege** "Tech" access only if one or more of their **Zones** are configured here. Users with **Privilege** "Admin" also have access.

"Admin" provides access only to users with **Privilege** "Admin".

"None" provides access to no users.

value Zones

**Zones** may contain combinations of "A", "B", "C", "D" or "E".

Select the **Zones** to be provided Tech access to this URI.

The meaning of the zones is determined by how you define them here. For example, say you define zones A and B via **Access Controls**:

/Toasters Tech A

/Blenders Tech B

Then over in **Users** you may reference zones:

admin Admin (has access to everything)

barry Tech A (has access to Toasters)

cindy Tech B (has access to Blenders)

david Tech A B (has access to Toasters and Blenders)

edwin User (has access to neither)

## configgroup Interface

The XML **instance** may be "ap0" or "wlan0".

These settings pertain to the **Network Interface** on the device. To see the effect of these selections after a reboot, view the corresponding **Status**. **Changes will take effect after reboot or wake from sleep or standby.**

When ap0 is enabled, **DHCP Server** will assign IP addresses to ap0's clients. DHCP Server manages up to 4 simultaneous clients. (Only 3 if wlan0 is enabled.)

### configitem State

value

**State** may be "Enabled" or "Disabled".

"Enabled" allows the Interface to operate.

### configitem DHCP Client

value

**DHCP Client** may be "Enabled" or "Disabled".

When "Enabled", any configured IP Address or Default Gateway will be ignored. DHCP Client will auto-discover and eclipse those configuration items. Hostname is sent to the remote DHCP Server and may figure into the address assignment.

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

This setting is not applicable to ap0.

### configitem IP Address

value

**IP Address** may contain up to 31 characters.

**IP Address** may be entered alone, in CIDR form, or with an explicit mask:

192.168.1.1 (default mask)

192.168.1.1/24 (CIDR)

192.168.1.1 255.255.255.0 (explicit mask)

The IP Address will be displayed always in CIDR, the canonical form.

### configitem Default Gateway

value

**Default Gateway** may contain up to 15 characters.

The **Default Gateway** is used only if DHCP Client is disabled, and provides the IP Address of the router.

This setting is not applicable to ap0.

### configitem Hostname

value

**Hostname** may contain up to 63 characters.

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

If **DHCP Client** is "Enabled", the Hostname is sent to the remote DHCP Server and may figure into the address assignment.

This setting is not applicable to ap0.

#### **configitem Primary DNS**

value

**Primary DNS** may contain up to 15 characters.

The **Primary DNS** is the first choice when performing a Domain Name lookup.

This setting is not applicable to ap0.

#### **configitem Secondary DNS**

value

**Secondary DNS** may contain up to 15 characters.

The **Secondary DNS** is the second choice when performing a Domain Name lookup.

This setting is not applicable to ap0.

#### **configitem MSS**

value

**MSS** has units of bytes.

The **Maximum Segment Size (MSS)** applies to TCP connections on the Interface. This can be useful to avoid fragmentation over the network, which may be required because this device does not perform reassembly.

#### **configgroup Line**

The XML **instance** may be "1" or "2".

These settings pertain to the Serial **Line**. Changes take effect immediately.

#### **configitem Name**

value

**Name** may contain up to 25 characters.

The **Name** is for display purposes only.

#### **configitem State**

value

**State** may be "Enabled" or "Disabled".

"Enabled" allows the Serial Line to operate.

### ***configitem Protocol***

value

**Protocol** may be "Command Line", "Modem Emulation", "Monitor", "Mux", "None", "Trouble Log" or "Tunnel".

**Protocol** selects the application to connect to the Line.

"Command Line" sets up a user interface containing commands to show device status and to change configuration. Simply paste in **XML** configuration to apply its settings to the device.

"Modem Emulation" implements legacy AT commands.

"Monitor" captures selected data.

"Mux" provides commands for sending / receiving data on multiple network connections.

"None" enables Line action commands.

"Trouble Log" sets up an output-only message log on the device.

"Tunnel" sets up the Line to work with the Tunnel application. See the Tunnel configuration options for details.

### ***configitem Baud Rate***

value

**Baud Rate** has units of bits per second.

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

### ***configitem Parity***

value

**Parity** may be "None", "Even" or "Odd".

### ***configitem Data Bits***

value

**Data Bits** may be "7" or "8".

### ***configitem Stop Bits***

value

**Stop Bits** may be "1" or "2".

### ***configitem Flow Control***

value

**Flow Control** may be "None", "Hardware" or "Software".

### ***configitem Xon Char***

value

**Xon Char** may contain one byte.

A control character <control>J, for example, counts as one.

A control character can be input in alternate forms:

\17 (decimal)

0x11 (hexadecimal)

<control>Q (control)

### **configitem Xoff Char**

value

**Xoff Char** may contain one byte.

A control character <control>J, for example, counts as one.

A control character can be input in alternate forms:

\17 (decimal)

0x11 (hexadecimal)

<control>Q (control)

### **configitem Gap Timer**

value

**Gap Timer** has units of milliseconds.

Blank the value for "<Four Character Periods>".

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

### **configitem Threshold**

value

**Threshold** has units of bytes.

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

## **configgroup Power**

These settings pertain to **Power** levels required by the device. Changes take effect immediately.

### **configitem Dynamic Power Mode**

value

**Dynamic Power Mode** may be "Disabled", "Sleep" or "Standby".

"Disabled" prevents the device from powering down.

"Sleep" powers down the radio and the system clocks, while preserving the system state. Wake up time is quick, and applications will pick up where they left off. This provides good power savings.

"Standby" powers down as much as is possible, including the CPU. System runtime state is not preserved. Wake up time is slower, as the entire system must be re-initialized. This provides the best power savings.

### **configitem Time Powered Up**

value

**Time Powered Up** has units of seconds, minutes, hours, and/or days.

The device holds power on for **Time Powered Up** duration.

After the **Time Powered Up** duration, power might continue to be held on for other reasons:

If **WKUP Pin** is "Level High", power will be held on as long as the WKUP level is high.

Any enabled **Application** can hold power on.

### **configitem Application**

If any **Application** is "Enabled", the application may hold power on longer or wake up sooner. This provides a mechanism to allow an application to be in an appropriate state for graceful shutdown.

"Command Line" holds power on till the last CLI user exits.

"HTTP Server" holds power up during each HTTP client operation and for a configurable time afterward.

"Tunnel Accept" holds power up while any Tunnel Accept connection is open.

"Tunnel Connect" holds power up while any Tunnel Connect connection is open.

value State

**State** may be "Enabled" or "Disabled".

"Enabled" allows this Application to hold power on.

### **configitem WKUP Pin**

value

**WKUP Pin** may be "Disabled", "Rising Edge" or "Level High".

**WKUP Pin** selects the role of the WKUP pin in powering up or staying up.

"Disabled" means the **WKUP Pin** is ignored. Power up will happen after **Maximum Time Powered Down** or earlier if called for by an enabled **Application**.

"Rising Edge" means the system will power up on the rising edge of **WKUP**. Power up can also happen after **Maximum Time Powered Down** or earlier if called for by an enabled **Application**.

"Level High" means the system will power up on the rising edge of **WKUP** and will stay up while **WKUP** remains high. Power up can also happen after **Maximum Time Powered Down** or earlier if called for by an enabled **Application**.

### **configitem Maximum Time Powered Down**

value

**Maximum Time Powered Down** has units of seconds, minutes, hours, and/or days.

Blank the value for "<Infinite>".

The device wakes up after being down **Maximum Time Powered Down**.

The device may wake up earlier if **WKUP Pin** is "Rising Edge" or "Level High".

The device may also wake up earlier if called for by an enabled **Application**.

### **configgroup Radio**

These settings pertain to the **Radio**.

Any change to these settings requires a reboot to take effect.

#### **configitem Mode**

value

**Mode** may be "Disabled", "Enabled" or "Triggered".

"Disabled" holds the Radio in low power.

"Enabled" allows the Radio to operate.

"Triggered" waits for CPM Role "Radio Trigger" to become active. Then the Radio stays up indefinitely.

**NOTE:** If Radio is disabled or not yet triggered, this inhibits both ap0 and wlan0 from operating.

#### **configitem Keep Alive**

value

**Keep Alive** may be "Enabled" or "Disabled".

"Enabled" causes a Null-Function Data frame to be sent on wlan0 once per second to keep the link up.

#### **configitem Max Volley Delay**

value

**Max Volley Delay** has units of seconds and/or minutes.

While wlan0 is Disconnected, it scans in turn for each WLAN Profile. One scan per profile comprises a volley. The interval delay is doubled after failure to join, subject to the **Max Volley Delay**.

**WARNING:** Short delay will compromise ap0 performance; ap0 cannot communicate while the radio is scanning.

#### **configitem Roaming**

value Scan Period

**Scan Period** has units of seconds and/or minutes.

**Scan Period** is the time between scans looking for a roaming candidate.

value Trigger Delta

**Trigger Delta** has units of dBm.

A device with RSSI **Trigger Delta** higher than the current Access Point is a roaming candidate.

value RSSI Floor

**RSSI Floor** has units of dBm.

When the signal drops below the **RSSI Floor**, the radio attempts to roam.

### **configgroup SPI**

These settings pertain to the **Serial Peripheral Interface (SPI)** Bus Master device. Changes take effect immediately.

#### **configitem Name**

value

**Name** may contain up to 25 characters.

The **Name** is for display purposes only.

#### **configitem State**

value

**State** may be "Enabled" or "Disabled".

"Enabled" enables the SPI.

"Disabled" disables the SPI.

#### **configitem Protocol**

value

**Protocol** may be "Monitor" or "None".

**Protocol** selects the application to connect to the SPI.

"Monitor" captures selected data.

#### **configitem Target Speed**

value

**Target Speed** has units of Hz.

Blank the value for "<Minimum>".

**Target Speed** selects the target clock speed of the SPI.

The **Target Speed** may be lowered to the closest **Operating Speed** capability of the device. If so, a warning will be noted.

#### **configitem Idle Clock Level**

value

**Idle Clock Level** may be "Low" or "High".

**Idle Clock Level**, also known as Clock Polarity or CPOL, selects the level of the clock when idle:

"Low" means the idle clock is at a low level. This is equivalent to CPOL=0.

"High" means the idle clock is at a high level. This is equivalent to CPOL=1.

### **configitem Clock Edge**

value

**Clock Edge** may be "First" or "Second".

**Clock Edge**, also known as Clock Phase or CPHA, selects the clock edge for latching data:

"First" means each bit is latched on the first edge of the clock. This is equivalent to CPHA=0. When **Idle Clock Level** is "Low", data is latched on the rising edge. When **Idle Clock Level** is "High", data is latched on the falling edge.

"Second" means each bit is latched on the second edge of the clock. This is equivalent to CPHA=1. When **Idle Clock Level** is "Low", data is latched on the falling edge. When **Idle Clock Level** is "High", data is latched on the rising edge.

### **configitem Bits Per Word**

value

**Bits Per Word** may be "8" or "16".

**Bits Per Word** selects the number of bits per word of transfer.

### **configitem First Transfer**

value

**First Transfer** may be "Most Significant Bit" or "Least Significant Bit".

**First Transfer** selects the first transfer bit of each word.

## **configgroup User**

These settings pertain to each **User** on the device.

### **configitem Password**

value

**Password** may contain up to 32 characters.

The value is HIDDEN.

### **configitem Privilege**

value

**Privilege** may be "User", "Tech" or "Admin".

Sets the user **Privilege** which governs what they can do.

"User" has access only to areas with **User Level** set to "User".

"Tech" has access only to areas with **User Level** set to "User" or with **User Level** set to "Tech" within the designated **Zones**.

"Admin" has access to all except areas with **User Level** set to "None".

### **configitem Zones**

value

**Zones** may contain combinations of "A", "B", "C", "D" or "E".

**Zones** designate areas that a "Tech" has access to.

The meaning of the zones is determined by how you define them over in **HTTP Server Security Access Controls**. For example, say you define zones A and B via **Access Controls**:

```
/Toasters Tech A
```

```
/Blenders Tech B
```

Then here you may reference zones:

```
admin Admin (has access to everything)
```

```
barry Tech A (has access to Toasters)
```

```
cindy Tech B (has access to Blenders)
```

```
david Tech A B (has access to Toasters and Blenders)
```

```
edwin User (has access to neither)
```

### **configgroup WLAN Profile**

These settings pertain to a WLAN Profile on the device.

If wlan0 connects to an access point on a different wireless channel, a current connection to ap0 may be dropped due to the channel change. Reconnect to ap0 in order to continue access to the device.

### **configitem Basic**

value Network Name

**Network Name** may contain up to 32 characters.

value State

**State** may be "Enabled" or "Disabled".

"Enabled" allows this profile to be used.

"Disabled" prevents this profile from being used.

### **configitem Security**

value Suite

**Suite** may be "None", "WEP", "WPA" or "WPA2".

value WEP Key Size

**Key Size** may be "40" or "104".

**Key Size** is in bits.

value WEP TX Key Index

**TX Key Index** may be "1", "2", "3" or "4".

value WEP Key Key

**Key** may contain up to 13 bytes.

The value is HIDDEN.

Set the **Key** value in hex, 5 or 13 bytes according to **Key Size** 40 or 104 bits respectively.

value WPAx Key Type

**Key Type** may be "Passphrase" or "Hex".

value WPAx Passphrase

**Passphrase** may contain up to 63 characters.

The value is HIDDEN.

value WPAx Key

**Key** may contain up to 32 bytes.

The value is HIDDEN.

Set the **Key** value in hex.

value WPAx Encryption

**Encryption** may contain combinations of "CCMP" or "TKIP".

"WPA" requires "TKIP", and only "TKIP".

"WPA2" requires "CCMP" and/or "TKIP".

### ***configitem Advanced***

value TX Power Maximum

**TX Power Maximum** has units of dBm.

**TX Power Maximum** governs the power output of the WLAN radio.

value Power Management

**Power Management** may be "Enabled" or "Disabled".

value PM Interval

**PM Interval** has units of beacons (100 ms each).

### **configgroup XML Import Control**

#### ***configitem Restore Factory Configuration***

value

**Restore Factory Configuration** may be "Enabled" or "Disabled".

#### ***configitem Reboot***

value

**Reboot** may be "Enabled" or "Disabled".

**configitem Missing Values**

value

**Missing Values** may be "Unchanged" or "Set to Default".

**configitem Delete WLAN Profiles**

value

**Delete WLAN Profiles** may be "Enabled" or "Disabled".

**configitem WLAN Profile delete**

value name

**name** may contain up to 35 characters.

**configgroup AES Credential**

Each **AES Credential** holds a secret Encrypt Key and Decrypt Key for secure communication.

**configitem Encrypt Key**

value

**Encrypt Key** may contain up to 32 bytes.

The value is **HIDDEN**.

The **Encrypt Key** is used for encrypting outgoing data.

The Key is 16, 24, or 32 bytes in length. Any Key entered that is less than one of these is padded with zeroes. A byte specification comprises two nibble specifications with no intervening space. A nibble specification is a single digit from 0 to 9 or from "a" to "f" (representing 10 through 15).

Example Hexadecimal key:

```
12 34 56 78 9a bc de f0 01 02 03 04 05 06 07 08
```

To **remove** the Key, set it blank.

Note that the Key is a **shared secret** so it must be known by both sides of the connection and kept secret.

**configitem Decrypt Key**

value

**Decrypt Key** may contain up to 32 bytes.

The value is **HIDDEN**.

The **Decrypt Key** is used for decrypting incoming data.

The Key is 16, 24, or 32 bytes in length. Any Key entered that is less than one of these is padded with zeroes. A byte specification comprises two nibble specifications with no intervening space. A nibble specification is a single digit from 0 to 9 or from "a" to "f" (representing 10 through 15).

Example Hexadecimal key:

```
12 34 56 78 9a bc de f0 01 02 03 04 05 06 07 08
```

To **remove** the Key, set it blank.

Note that the Key is a **shared secret** so it must be known by both sides of the connection and kept secret.

### **configgroup CLI Server**

These settings pertain to the **CLI Server**. **Changes take effect immediately.**

#### **configitem Inactivity Timeout**

value

**Inactivity Timeout** has units of minutes.

Enter 0 for "<None>".

After this time period with no activity, the **CLI Server** will close the connection.

#### **configitem Telnet**

value Mode

**Mode** may be "Enabled" or "Disabled".

value Port

The **CLI Server** listens on this port for incoming Telnet connections.

### **configgroup Discovery**

The XML **instance** may be "ap0" or "wlan0".

These settings pertain to **Discovery**. Changes take effect immediately.

**Query Port** is a Lantronix discovery protocol server. It implements a simple proprietary discovery service on port 0x77FE (30718).

#### **configitem Query Port**

value State

**State** may be "Enabled" or "Disabled".

"Enabled" allows the device to be discovered.

"Disabled" prevents discovery from finding the device.

### **configgroup Modem Emulation**

The XML **instance** may be "1" or "2".

Connections can be initiated and accepted using **Modem** "AT" commands incoming from the Serial Line.

#### **configitem Listen Port**

value

Blank the value for "<None>".

Specify a **Listen Port** to accept connections on.

#### ***configitem*** Echo Pluses

value

**Echo Pluses** may be "Enabled" or "Disabled".

"Enabled" means pluses will be echoed back during a "pause +++ pause" escape sequence on the Serial Line.

#### ***configitem*** Echo Commands

value

**Echo Commands** may be "Enabled" or "Disabled".

"Enabled" (ATE1) means characters read on the Serial Line will be echoed while the Line is in Modem Command Mode.

#### ***configitem*** Verbose Response

value

**Verbose Response** may be "Enabled" or "Disabled".

"Enabled" (ATQ0) means Modem Response Codes are sent out on the Serial Line.

#### ***configitem*** Response Type

value

**Response Type** may be "Text" or "Numeric".

Either "Text" (ATV1) or "Numeric" (ATV0) representation for the Modem Response Codes are sent out on the Serial Line.

#### ***configitem*** Error Unknown Commands

value

**Error Unknown Commands** may be "Enabled" or "Disabled".

"Enabled" (ATU0) means ERROR is returned on the Serial Line for unrecognized AT commands.

"Disabled" (ATU1) means OK is returned for unrecognized AT commands.

#### ***configitem*** Incoming Connection

value

**Incoming Connection** may be "Disabled", "Automatic" or "Manual".

"Disabled" (ATS0=0) will refuse to answer.

"Automatic" (ATS0=1) will answer immediately.

"Manual" (ATS0=2 or higher) may be answered via the ATA command after an incoming RING.

### ***configitem Connect String***

value

**Connect String** may contain up to 30 characters.

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

### ***configitem Display Remote IP***

value

**Display Remote IP** may be "Enabled" or "Disabled".

"Enabled" means the incoming RING sent on the Serial Line is followed by the IP address of the caller.

### ***configgroup Monitor Initialization***

These settings pertain to **Monitor Initialization** in the device.

Monitor will process any initialization message before it starts polling or process any control message. Response captured during initialization will be overwritten by any poll or control response.

### ***configitem Initial Delay***

value

**Initial Delay** has units of milliseconds.

Sets **Initial Delay** waited before monitor start processing any initialization message.

### ***configitem Message***

The XML **instance** may range from 1 to 4.

value Command

**Command** may contain up to 32 bytes.

Sets the **Command** in binary format.

Binary format takes printable characters (e.g. 'abc' for characters 'a', 'b' and 'c') or binary string (e.g. [0xa, 0xd] for line feed and carriage return).

value End Character

**End Character** may contain one byte.

A control character <control>J, for example, counts as one.

A control character can be input in alternate forms:

\17 (decimal)

0x11 (hexadecimal)

<control>Q (control)

Sets the **End Character** to indicate end of response.

Response is ended by any configured **End Character**, **Length** OR **Timeout**.

value Length

**Length** has units of bytes.

Sets the **Length** of response.

Response is ended by any configured **End Character**, **Length** OR **Timeout**.

value Timeout

**Timeout** has units of milliseconds.

Blank the value for "<Minimum>".

Sets the **Timeout** to receive response.

Response is ended by any configured **End Character**, **Length** OR **Timeout**.

### configgroup Monitor Control

These settings pertain to **Monitor Control** in the device.

Control Message will be processed after receiving status action **Send**. Response will overwrite any response captured during initialization or poll. Response must be read before sending another status action **Send** or buffer will be reset.

#### configitem Message

The XML **instance** may range from 1 to 4.

value Command

**Command** may contain up to 32 bytes.

Sets the **Command** in binary format.

Binary format takes printable characters (e.g. 'abc' for characters 'a', 'b' and 'c') or binary string (e.g. [0xa, 0xd] for line feed and carriage return).

value End Character

**End Character** may contain one byte.

A control character <control>J, for example, counts as one.

A control character can be input in alternate forms:

\17 (decimal)

0x11 (hexadecimal)

<control>Q (control)

Sets the **End Character** to indicate end of response.

Response is ended by any configured **End Character**, **Length** OR **Timeout**.

value Length

**Length** has units of bytes.

Sets the **Length** of response.

Response is ended by any configured **End Character**, **Length** OR **Timeout**.

value Timeout

**Timeout** has units of milliseconds.

Blank the value for "<Minimum>".

Sets the **Timeout** to receive response.

Response is ended by any configured **End Character, Length OR Timeout**.

### configgroup Monitor Poll

These settings pertain to **Monitor Poll** in the device.

Poll Message will be processed periodically. Response will overwrite any response captured during initialization or poll.

#### configitem Message

The XML **instance** may range from 1 to 4.

value Command

**Command** may contain up to 32 bytes.

Sets the **Command** in binary format.

Binary format takes printable characters (e.g. 'abc' for characters 'a', 'b' and 'c') or binary string (e.g. [0xa, 0xd] for line feed and carriage return).

value End Character

**End Character** may contain one byte.

A control character <control>J, for example, counts as one.

A control character can be input in alternate forms:

\17 (decimal)

0x11 (hexadecimal)

<control>Q (control)

Sets the **End Character** to indicate end of response.

Response is ended by any configured **End Character, Length, OR Timeout**.

value Length

**Length** has units of bytes.

Sets the **Length** of response.

Response is ended by any configured **End Character, Length OR Timeout**.

value Timeout

**Timeout** has units of milliseconds.

Blank the value for "<Minimum>".

Sets the **Timeout** to receive response.

Response is ended by any configured **End Character, Length OR Timeout**.

### **configitem Delay**

value

**Delay** has units of seconds, minutes, hours, and/or days.

Sets **Delay** waited before monitor starts processing all poll messages again. 0 means poll messages are sent only once.

### **configgroup Monitor Filter**

These settings pertain to **Monitor Filter** in the device.

Filter settings will be applied to all received response. Filter results can be used to feed another filter or use as Data Reference.

### **configitem Rule**

The XML **instance** may range from 1 to 4.

value Source

**Source** may contain up to 6 characters.

Sets the **Source** in dot number format.

**Source** defines the input of a filter. E.g. If the source of this Filter is the second trunk of data created by filter 1, **Source** must be set to "1.2". A **Source** of "0" indicates the raw response.

Dot number format could be "0" or two numbers separated by a dot (e.g. "1.2").

value Mode

**Mode** may be "All", "Delimiters" or "Binary".

"All" makes filter output to be a duplicate of input.

"Delimiters" filter breaks input up to 8 trunks separated by **Binary String**. Each trunk will not contain the delimiters.

"Binary" filter breaks input into 3 trunks according to **Offset** and **Length**.

value Delimiter Binary String

**Binary String** may contain up to 6 bytes.

Sets **Binary String** delimiter in binary format.

Delimiters break input up to 8 trunks separated by (but not containing) delimiters. A delimiter is recognized if any of the **Binary String** is completely matched.

Binary format takes printable characters (e.g. 'abc' for characters 'a', 'b' and 'c') or binary string (e.g. [0xa, 0xd] for line feed and carriage return).

value Start Index

Sets **Start Index** to indicate when **Delimiters** filter starts breaking input into trunks.

value Offset

**Offset** has units of bytes.

Sets **Offset** for the size of the first trunk of data created by **Binary** Filter.

value Length

**Length** has units of bytes.

Sets **Length** for the size of the second trunk of data created by **Binary** Filter. The third trunk of data created by **Binary** Filter will contain the rest of input.

### **configgroup Monitor Data**

These settings pertain to **Monitor Data** in the device.

Data configured here will be accessible through the status of **Monitor**.

#### **configitem Selector**

The XML **instance** may range from 1 to 8.

value Name

**Name** may contain up to 16 characters.

Sets **Name** to enable the data selector.

value Response

Blank the value for "<None>".

Sets **Response** instance to select the source of data. Response instance corresponds to Poll or Control Message instance.

value Reference

**Reference** may contain up to 6 characters.

Sets the **Reference** in dot number format.

**Reference** selects the output of **Monitor Filter**. E.g. If data should select the second trunk of data created by filter 1, **Reference** must be set to "1.2". A **Reference** of "0" indicates the raw response.

Dot number format could be "0" or two numbers separated by a dot (e.g. "1.2").

### **configgroup NTP**

The **xPico Wi-Fi** implements Simple **NTP** (SNTP).

#### **configitem Server Hostname**

value

**Server Hostname** may contain up to 128 characters.

The **Server Hostname** is the name or IP address of an NTP server.

#### **configitem Sync Time**

value

**Sync Time** has units of seconds, minutes, and/or hours.

The NTP client waits **Sync Time** after successful update before querying again.

## configgroup Tunnel Accept

**Tunnel Accept** controls how a tunnel behaves when a connection attempt originates from the network.

### configitem Mode

value

**Mode** may be "Disable", "Always", "Any Character", "Start Character" or "Modem Control Asserted".

An Accept Tunnel can be started in a number of ways, according to its **Mode**:

"Disabled": never started.

"Always": always started.

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

"Start Character": started when the Start Character is read on the Serial Line.

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

### configitem Local Port

value

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

Blank the value to restore the default.

### configitem Protocol

value

**Protocol** may be "TCP" or "TCP AES".

### configitem Credential

value

**Credential** may contain up to 30 characters.

The **Credential** named here must belong to the selected **Protocol**.

Configure the named Credential on its separate page. A Credential typically contains whatever keys, certificates, passwords, or usernames that are required for connection using the selected **Protocol**.

### configitem Start Character

value

**Start Character** may contain one byte.

A control character <control>J, for example, counts as one.

A control character can be input in alternate forms:

\17 (decimal)

0x11 (hexadecimal)

<control>Q (control)

When the **Start Character** is received on the Serial Line, it enables the tunnel to listen for a network connection.

#### ***configitem Flush Start Character***

value

**Flush Start Character** may be "Enabled" or "Disabled".

"Enabled" prevents forwarding of a start character from the Line into the network.

"Disabled" allows forwarding of a start character from the Line into the network.

#### ***configitem Flush Line***

value

**Flush Line** may be "Enabled" or "Disabled".

**Flush Line** applies at the time when a connection is accepted from the network.

"Enabled" means any buffered characters from the Serial Line will be discarded when a connection is accepted.

"Disabled" means any characters received on the Serial Line will be buffered and sent after a connection is accepted.

#### ***configitem Block Line***

value

**Block Line** may be "Enabled" or "Disabled".

"Enabled" (the debug setting) means incoming characters from the Serial Line will NOT be forwarded to the network. Instead, they will be buffered and will eventually flow off the Serial Line if hardware or software flow control is configured.

"Disabled" (the normal setting) means incoming characters from the Serial Line are sent on into the network. Any buffered characters are sent first.

#### ***configitem Block Network***

value

**Block Network** may be "Enabled" or "Disabled".

"Enabled" (the debug setting) means incoming characters from the network will NOT be forwarded to the Serial Line. Instead, they will be buffered and will eventually flow off the network side.

"Disabled" (the normal setting) means incoming characters from the network are sent on into the Serial Line. Any buffered characters are sent first.

#### ***configitem Password***

value

**Password** may contain up to 31 characters.

The value is HIDDEN.

The **Password** must contain only alphanumeric characters and punctuation. When set, clients must send the correct password string to the unit within 30 seconds from opening network connection in order to enable data transmission. The password sent to the unit must be terminated with one of the following:

0A (Line Feed)

00 (Null)

0D 0A (Carriage Return / Line Feed)

0D 00 (Carriage Return / Null)

If **Prompt for Password** is "Enabled", the user will be prompted for the password upon connection.

### **configitem Prompt for Password**

value

**Prompt for Password** may be "Enabled" or "Disabled".

### **configgroup Tunnel Line**

The **Line** Configuration applies to the Serial Line interface.

### **configitem DTR**

value

**DTR** may be "Asserted while connected", "Continuously asserted" or "Unasserted".

The **DTR** options select the conditions in which the **Data Terminal Ready** control signal on the Serial Line is asserted.

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

### **configgroup Tunnel Connect**

**Tunnel Connect** controls how a tunnel behaves when a connection attempt originates locally.

### **configitem Mode**

value

**Mode** may be "Disable", "Always", "Any Character", "Start Character" or "Modem Control Asserted".

A Connect Tunnel can be started in a number of ways, according to its **Mode**:

"Disabled": never started.

"Always": always started.

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

"Start Character": started when the Start Character is read on the Serial Line.

---

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

### ***configitem Start Character***

value

**Start Character** may contain one byte.

A control character <control>J, for example, counts as one.

A control character can be input in alternate forms:

\17 (decimal)

0x11 (hexadecimal)

<control>Q (control)

When the **Start Character** is received on the Serial Line, it connects the tunnel.

### ***configitem Flush Start Character***

value

**Flush Start Character** may be "Enabled" or "Disabled".

"Enabled" prevents forwarding of a start character from the Line into the network.

"Disabled" allows forwarding of a start character from the Line into the network.

### ***configitem Local Port***

value

Blank the value for "<Random>".

The **Local Port** is by default random but can be overridden.

### ***configitem Host***

The XML **instance** may range from 1 to 2.

value Address

**Address** may contain up to 50 characters.

The **Host Address** is required to enable a Connect Tunnel.

It designates the address of the remote host to connect to.

Either a DNS address or an IP address may be provided.

If your **Protocol** is UDP based and you want to listen rather than connect: Leave **Host Port** set to **<None>** and set **Host Address** to the Interface name you want to listen to ("ap0" or "wlan0").

value Port

Blank the value for "<None>".

The **Host Port** is required to enable a Connect Tunnel.

It designates the TCP or UDP port on the remote host to connect to.

value Protocol

**Protocol** may be "TCP", "TCP AES" or "UDP".

---

value Credential

**Credential** may contain up to 30 characters.

The **Credential** named here must belong to the selected **Protocol**.

Configure the named Credential on its separate page. A Credential typically contains whatever keys, certificates, passwords, or usernames that are required for connection using the selected **Protocol**.

value Initial Send

**Initial Send** may contain up to 32 characters.

The **Initial Send** string, if present, is sent out the network before any other data when the connection is established.

value Reception

**Reception** may be "Restricted" or "Unrestricted".

"Restricted" will discard any received UDP packets whose from address and port do not match the designated **Host Address** and **Port**. In UDP listen mode, the remote address and port of the first received packet are taken as designated until the socket is closed.

"Unrestricted" accepts any UDP packets directed to the **Local Port** regardless of where they came from.

### **configitem Connections**

value

**Connections** may be "Sequential", "Simultaneous" or "Round-Robin".

**Connections** controls how multiple hosts shall be used with a Connect Tunnel.

"Sequential" means the tunnel will start with host 1 and attempt each host in sequence until a connection is accepted.

"Simultaneous" means the tunnel will connect to all of the hosts that accept a connection.

"Round-Robin" means the tunnel connection attempts start with the host after whichever host had previously connected.

### **configitem Reconnect Time**

value

**Reconnect Time** has units of seconds, minutes, and/or hours.

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

Blank the display field to restore the default.

### **configitem Flush Line**

value

**Flush Line** may be "Enabled" or "Disabled".

**Flush Line** applies at the time when a connection is established to the network.

---

"Enabled" means any buffered characters from the Serial Line will be discarded when a connection is established.

"Disabled" means any characters received on the Serial Line will be buffered and sent after a connection is established.

### ***configitem Block Line***

value

**Block Line** may be "Enabled" or "Disabled".

"Enabled" (the debug setting) means incoming characters from the Serial Line will NOT be forwarded to the network. Instead, they will be buffered and will eventually flow off the Serial Line if hardware or software flow control is configured.

"Disabled" (the normal setting) means incoming characters from the Serial Line are sent on into the network. Any buffered characters are sent first.

### ***configitem Block Network***

value

**Block Network** may be "Enabled" or "Disabled".

"Enabled" (the debug setting) means incoming characters from the network will NOT be forwarded to the Serial Line. Instead, they will be buffered and will eventually flow off the network side.

"Disabled" (the normal setting) means incoming characters from the network are sent on into the Serial Line. Any buffered characters are sent first.

## **configgroup Tunnel Disconnect**

These settings relate to Disconnecting a Tunnel.

### ***configitem Stop Character***

value

**Stop Character** may contain one byte.

A control character <control>J, for example, counts as one.

A control character can be input in alternate forms:

\17 (decimal)

0x11 (hexadecimal)

<control>Q (control)

When the **Stop Character** is received on the Serial Line, it disconnects the tunnel.

Disable the **Stop Character** by blanking the field to set it to < None>.

### ***configitem Flush Stop Character***

value

**Flush Stop Character** may be "Enabled" or "Disabled".

---

"Enabled" prevents forwarding of a stop character from the Line into the network.

"Disabled" allows forwarding of a stop character from the Line into the network.

### ***configitem Modem Control***

value

**Modem Control** may be "Enabled" or "Disabled".

"Enabled" means disconnect when the Modem Control pin is not asserted on the Serial Line.

### ***configitem Timeout***

value

**Timeout** has units of milliseconds.

Blank the value for "<Disabled>".

**Timeout** enables disconnect after the tunnel is idle for a specified number of milliseconds.

### ***configitem Flush Line***

value

**Flush Line** may be "Enabled" or "Disabled".

"Enabled" means flush the Serial Line when the Tunnel is disconnected.

### ***configgroup Tunnel Packing***

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

### ***configitem Mode***

value

**Mode** may be "Disable", "Timeout" or "Send Character".

"Disable" means data is not packed.

"Timeout" means data is sent only after a timeout occurs.

"Send Character" means data is sent when the **Send Character** is read on the Serial Line.

### ***configitem Timeout***

value

**Timeout** has units of milliseconds.

If the oldest byte of queued data has been waiting for **Timeout** milliseconds, the queued data will be sent on the network immediately.

### ***configitem Threshold***

value

---

**Threshold** has units of bytes.

If the number of bytes of queued data reaches the **Threshold**, the queued data will be sent on the network immediately.

#### ***configitem Send Character***

value

**Send Character** may contain one byte.

A control character <control>J, for example, counts as one.

A control character can be input in alternate forms:

\17 (decimal)

0x11 (hexadecimal)

<control>Q (control)

If used, the **Send Character** is a single printable character or a control character that, when read on the Serial Line, forces the queued data to be sent on the network immediately.

#### ***configitem Flush Send Character***

value

**Flush Send Character** may be "Enabled" or "Disabled".

"Enabled" means the **Send Character** will NOT be sent from the Serial Line to the network.

"Disabled" means the **Send Character** WILL be forwarded from the Serial Line to the network.

#### ***configitem Trailing Character***

value

**Trailing Character** may contain one byte.

A control character <control>J, for example, counts as one.

A control character can be input in alternate forms:

\17 (decimal)

0x11 (hexadecimal)

<control>Q (control)

The **Trailing Character** is an optional single printable character or control character that is injected into the outgoing data stream right after the **Send Character**.

Disable the **Trailing Character** by blanking the field to set it to < None>.

### **configgroup Custom**

User custom configuration values are stored under this group.

#### ***configitem Item***

value Value

---

**Value** may contain up to 63 characters.

Sets a custom configurable text **Value** of an Item. The Item <instance> is the name of this value.

## Appendix B: Technical Support

Lantronix offers many resources to support our customers and products at <http://www.lantronix.com/support>. For instance, ask a question, find firmware downloads, access the FTP site and search through tutorials, FAQs, bulletins, warranty information, extended support services, and product documentation.

To contact technical support or sales, look up your local office at <http://www.lantronix.com/about/contact.html>. When you report a problem, please provide the following information:

- ◆ Your name, company name, address, and phone number
- ◆ Lantronix product and model number
- ◆ Lantronix MAC address or serial number
- ◆ Firmware version and current configuration
- ◆ Description of the problem
- ◆ Status of the unit when the problem occurred (please try to include information on user and network activity at the time of the problem).

## Appendix C: Compliance

(According to ISO/IEC Guide and EN 45014)

### Manufacturer's Name & Address:

Lantronix, Inc.  
7535 Irvine Center Drive  
Suite 100  
Irvine, CA 92618 USA

Declares that the following product:

### Product Name Models:

xPico® Wi-Fi® Embedded Device Server, xPico Wi-Fi SMT Embedded Device Server

Conforms to the following standards or other normative documents:

**Table C-1 Country Certifications**

| Country  | Specifications for Models xPico Wi-Fi, xPico W1002, and xPico W1003   |
|--|---|
| USA                                 | <ul style="list-style-type: none"><li>◆ FCC Part 15, Subpart B, Class B</li><li>◆ ICES-003:2012 Issue 5, Class B</li><li>◆ ANSI C63.4-2009</li></ul>  |
| USA  | <ul style="list-style-type: none"><li>◆ FCC Part 15, Subpart C (Section 15.247)</li><li>◆ ANSI C63.10-2009</li><li>◆ FCC Part 2 (Section 2.1091)</li><li>◆ FCC OET Bulletin 65, Supplement C (01-01)</li><li>◆ IEEE C95.1</li></ul> |
| Canada   | <ul style="list-style-type: none"><li>◆ Canada RSS-210 Issue 8 (2010-12)</li><li>◆ Canada RSS-Gen Issue 3 (2010-12)</li><li>◆ ANSI C63.10-2009</li><li>◆ RSS-102 Issue 4 (2010-12)</li></ul>  |
| Australia,<br>New Zealand  N11206 | <ul style="list-style-type: none"><li>◆ AS/NZS 4268: 2012</li></ul>   |
| Japan  | <ul style="list-style-type: none"><li>◆ ARIB STD-T66, MIC notice 88 Appendix 43</li><li>◆ RCR STD-33, MIC notice 88 Appendix 44</li></ul>   |

**Figure C-2 EU Declaration of Conformity**

The xPico Wi-Fi embedded device server has been so constructed that the product complies with the requirement of with Article 10(2) as it can be operated in at least one Member State as examined and the product is compliant with Article 10(10) as it has no restrictions on putting into service in all EU member states.



7535 Irvine Center Drive, Suite 100, Irvine, CA 92618

**EU DECLARATION OF CONFORMITY**

This declaration of conformity is issued under the sole responsibility of the manufacturer.

|  |             |  |            |
|--|-------------|--|------------|
| Object of the declaration  |             |  |            |
| Product Information  |             | Product Name: xPico Wireless Device Server |            |
|  | Model       | SW Version                                 | HW Version |
|  | xPico Wi-Fi | 1.4.0.0R28                                 | 11         |
|  | xPico W1002 | 1.4.0.0R28                                 | 13         |
|  | xPico W1003 | 1.4.0.0R28                                 | 13         |
| <p>The object of the declaration described above is in conformity with the relevant Union harmonisation legislation:</p> <ul style="list-style-type: none"> <li>•References to the relevant harmonised standards used or references to the technical specifications in relation to which conformity is declared</li> </ul> |             |  |            |
| <b>Radio Equipment Directive 2014/53/EU</b>  |             |  |            |
| EN 300 328 V2.1.1  |             |  |            |
| EN 301 489-1 V2.1.1  |             |  |            |
| EN 301 489-17 V3.1.1   |             |  |            |
| EN 62311:2008  |             |  |            |
| EN 60950-1:2006 + A1:2010 +A12:2011 +A2:2013   |             |  |            |

The notified body, TUV SUD BABT, performed a conformity assessment of the technical construction file and issued certificate BABT-RED000186 i01.

Signature:       Date: 6-26-17

Name: Daryl R. Miller  
Title: VP of Engineering, Lantronix, Inc.

**Table C-3 Country Transmitter IDs**

| Country      | Specifications for Models xPico Wi-Fi, xPico W1002, and xPico W1003 |
|--------------|---|
| USA FCC ID   | R68XPICOW   |
| Canada IC ID | 3867A-XPICOW  |
| Japan ID     | 201-135275  |

**Table C-4 Safety**

| Country  | Specifications for Models xPico Wi-Fi, xPico W1002, and xPico W1003  |
|--|--|
| World Wide  | CB<br>EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011<br>In accordance with the council directive 2006/95/EC |
| US, Canada   | UL 60950-1 (2nd Edition)   |

Hereby, Lantronix, declares that this xPico Wi-Fi and xPico Wi-Fi SMT embedded device server is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

**Table C-5 Europe – EU Declaration of Conformity**

|  |  |
|--|--|
|  Český [Czech]        | <i>Lantronix, Inc.</i> tímto prohlašuje, že tento <i>xPico Wi-Fi, xPico Wi-Fi SMT</i> je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice RED 2014/53/EU.  |
|  Dansk [Danish]     | Undertegnede <i>Lantronix, Inc.</i> erklærer herved, at følgende udstyr <i>xPico Wi-Fi, xPico Wi-Fi SMT</i> overholder de væsentlige krav og øvrige relevante krav i direktiv RED 2014/53/EU.  |
|  Deutsch [German]   | Hiermit erklärt <i>Lantronix, Inc.</i> , dass sich das Gerät <i>xPico Wi-Fi, xPico Wi-Fi SMT</i> in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie RED 2014/53/EU befindet. |
|  Eesti [Estonian]   | Käesolevaga <i>Lantronix, Inc.</i> seadme <i>xPico Wi-Fi, xPico Wi-Fi SMT</i> vastavust direktiivi RED 2014/53/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.                                     |
|  English            | Hereby, <i>Lantronix, Inc.</i> , declares that this <i>xPico Wi-Fi, xPico Wi-Fi SMT</i> is in compliance with the essential requirements and other relevant provisions of Directive RED 2014/53/EU.  |
|  Español [Spanish]  | Por medio de la presente <i>Lantronix, Inc.</i> declara que el <i>xPico Wi-Fi, xPico Wi-Fi SMT</i> cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva RED 2014/53/EU.          |
|  Ελληνική [Greek]   | ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ <i>Lantronix, Inc.</i> ΔΗΛΩΝΕΙ ΟΤΙ <i>xPico Wi-Fi, xPico Wi-Fi SMT</i> ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ RED 2014/53/EU.  |
|  Français [French]  | Par la présente <i>Lantronix, Inc.</i> déclare que l'appareil <i>xPico Wi-Fi, xPico Wi-Fi SMT</i> est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive RED 2014/53/EU.                           |
|  Italiano [Italian] | Con la presente <i>Lantronix, Inc.</i> dichiara che questo <i>xPico Wi-Fi, xPico Wi-Fi SMT</i> è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva RED 2014/53/EU.                          |
| Latviski [Latvian]   | Ar šo <i>Lantronix, Inc.</i> deklarē, ka <i>xPico Wi-Fi, xPico Wi-Fi SMT</i> atbilst Direktīvas RED 2014/53/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.   |

**Table C-5 Europe – EU Declaration of Conformity (continued)**

|  |   |
|--|---|
| Lietuvių [Lithuanian]  | Šiuo Lantronix, Inc. deklaruoja, kad šis xPico Wi-Fi, xPico Wi-Fi SMT atitinka esminius reikalavimus ir kitas RED 2014/53/EU Direktyvos nuostatas.  |
|  Nederlands [Dutch]     | Hierbij verklaart Lantronix, Inc. dat het toestel xPico Wi-Fi, xPico Wi-Fi SMT in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn RED 2014/53/EU.            |
|  Malti [Maltese]        | Hawnhekk, Lantronix, Inc., jiddikjara li dan xPico Wi-Fi, xPico Wi-Fi SMT jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva RED 2014/53/EU.               |
|  Magyar [Hungarian]     | Alulírott, Lantronix, Inc. nyilatkozom, hogy a xPico Wi-Fi, xPico Wi-Fi SMT megfelel a vonatkozó alapvető követelményeknek és az RED 2014/53/EU irányelv egyéb előírásainak.                            |
|  Polski [Polish]        | Niniejszym Lantronix, Inc. oświadcza, że xPico Wi-Fi, xPico Wi-Fi SMT jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy RED 2014/53/EU.                         |
|  Português [Portuguese] | Lantronix, Inc. declara que este xPico Wi-Fi, xPico Wi-Fi SMT está conforme com os requisitos essenciais e outras disposições da Directiva RED 2014/53/EU.  |
|  Slovensko [Slovenian]  | Lantronix, Inc. izjavlja, da je ta xPico Wi-Fi, xPico Wi-Fi SMT v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive RED 2014/53/EU.   |
| Slovensky [Slovak]   | Lantronix, Inc. týmto vyhlasuje, že xPico Wi-Fi, xPico Wi-Fi SMT spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice RED 2014/53/EU.  |
|  Suomi [Finnish]        | Lantronix, Inc. vakuuttaa täten että xPico Wi-Fi, xPico Wi-Fi SMT tyyppinen laite on direktiivin RED 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.          |
|  Svenska [Swedish]    | Härmed intygar Lantronix, Inc. att denna xPico Wi-Fi, xPico Wi-Fi SMT står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv RED 2014/53/EU. |

**Table C-1 RF Output Power**

| Characteristics                            | Rate    | Type | Criteria | Unit |
|--|---------|------|----------|------|
| RF Average Output Power, 802.11b CCK Mode  | 1 Mbps  | 16.5 | ±1.5     | dBm  |
|  | 11 Mbps | 16.5 | ±1.5     | dBm  |
| RF Average Output Power, 802.11g OFDM Mode | 6 Mbps  | 15   | ±1.5     | dBm  |
|  | 54 Mbps | 13   | ±1.5     | dBm  |
| RF Average Output Power, 802.11n OFDM Mode | MCS0    | 14.5 | ±1.5     | dBm  |
|  | MCS7    | 12   | ±1.5     | dBm  |

**Note:** Frequency band supported is between 2.412 to 2.472 Ghz.

---

## Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- ◆ Reorient or relocate the receiving antenna.
- ◆ Increase the separation between the equipment and receiver.
- ◆ Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- ◆ Consult the dealer or an experienced radio/TV technician for help.

***FCC Caution:*** Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

**This device is intended only for OEM integrators under the following conditions:**

1. The antenna must be installed such that 20 cm is maintained between the antenna and users, and
2. The transmitter module may not be co-located with any other transmitter or antenna.

As long as 2 conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed

**IMPORTANT NOTE:** *In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.*

## End Product Labeling

This transmitter module is authorized only for use in device where the antenna may be installed such that 20 cm may be maintained between the antenna and users. The final end product must be labeled in a visible area with the following: "Contains FCC ID: R68XPICOW". The grantee's FCC ID can be used only when all FCC compliance requirements are met.

## Manual Information To the End User

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the user's manual of the end product which integrates this module.

The end user manual shall include all required regulatory information/warning as show in this manual.

## Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

## Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

## Déclaration d'exposition aux radiations

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

### **This device is intended only for OEM integrators under the following conditions: (For module device use)**

1. The antenna must be installed such that 20 cm is maintained between the antenna and users, and
2. The transmitter module may not be co-located with any other transmitter or antenna.

As long as 2 conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed.

### **Cet appareil est conçu uniquement pour les intégrateurs OEM dans les conditions suivantes: (Pour utilisation de dispositif module)**

L'antenne doit être installée de telle sorte qu'une distance de 20 cm est respectée entre l'antenne et les utilisateurs, et

Le module émetteur peut ne pas être coïmplanté avec un autre émetteur ou antenne.

Tant que les 2 conditions ci-dessus sont remplies, des essais supplémentaires sur l'émetteur ne seront pas nécessaires. Toutefois, l'intégrateur OEM est toujours responsable des essais sur son produit final pour toutes exigences de conformité supplémentaires requis pour ce module installé.

**IMPORTANT NOTE:** *In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the Canada authorization is no longer considered valid and the IC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate Canada authorization.*

**NOTE IMPORTANTE:** *Dans le cas où ces conditions ne peuvent être satisfaites (par exemple pour certaines configurations d'ordinateur portable ou de certaines co-localisation avec un autre émetteur), l'autorisation du Canada n'est plus considéré comme valide et l'ID IC ne peut pas être utilisé sur le produit final. Dans ces circonstances, l'intégrateur OEM sera chargé de réévaluer le produit final (y compris l'émetteur) et l'obtention d'une autorisation distincte au Canada.*

### End Product Labeling

This transmitter module is authorized only for use in device where the antenna may be installed such that 20 cm may be maintained between the antenna and users.

- ◆ The final end xPico Wi-Fi product must be labeled in a visible area with the following: "Contains IC: 3867A-XPICOW".
- ◆ The final end xPico Wi-Fi SMT product must be labeled in a visible area with the following: "Contains IC: 3867A-XPICOW".

### Plaque signalétique du produit final

Ce module émetteur est autorisé uniquement pour une utilisation dans un dispositif où l'antenne peut être installée de telle sorte qu'une distance de 20cm peut être maintenue entre l'antenne et les utilisateurs.

- ◆ Le produit final xPico Wi-Fi doit être étiqueté dans un endroit visible avec l'inscription suivante: "Contient des IC: 3867A-XPICOW".
- ◆ Le produit final xPico Wi-Fi SMT doit être étiqueté dans un endroit visible avec l'inscription suivante: "Contient des IC: 3867A-XPICOW".

### Manual Information To the End User

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the user's manual of the end product which integrates this module.

The end user manual shall include all required regulatory information/warning as show in this manual.

### Manuel d'information à l'utilisateur final

L'intégrateur OEM doit être conscient de ne pas fournir des informations à l'utilisateur final quant à la façon d'installer ou de supprimer ce module RF dans le manuel de l'utilisateur du produit final qui intègre ce module.

Le manuel de l'utilisateur final doit inclure toutes les informations réglementaires requises et avertissements comme indiqué dans ce manuel.

---

## Antenna Requirement

This device has been designed to operate with a PIFA antenna have a maximum gain of 2.5dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

This radio transmitter xPico Wi-Fi or xPico Wi-Fi SMT has been approved by Industry Canada to operate with the antenna type, maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this user's manual, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Ce dispositif a été conçu pour fonctionner avec une antenne ayant un gain maximal de PIFA antenne avec dBi 2.5. Une antenne à gain plus élevé est strictement interdite par les règlements d'Industrie Canada. L'impédance d'antenne requise est de 50 ohms.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Le présent émetteur radio xPico Wi-Fi o xPico Wi-Fi SMT a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

**Table C-6 Approved Antenna(s) List**

| Type   | Gain    | Brand        |
|--------|---------|--------------|
| PIFA   | 2.5 dBi | Ethertronics |
| Dipole | 2.38    | Wanshih      |

### Manufacturer's Contact:

Lantronix, Inc.  
7535 Irvine Center Drive, Suite 100  
Irvine, CA 92618 USA  
Tel: 949-453-3990  
Fax: 949-453-3995

## RoHS, REACH and WEEE Compliance Statement

Please visit <http://www.lantronix.com/legal/rohs/> for Lantronix's statement about RoHS, REACH and WEEE compliance.