



PremierWave® EN Embedded System on Module User Guide

Intellectual Property

© 2017 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 *PremierWave* are registered trademarks of Lantronix, Inc. in the United States and other countries. *DeviceInstaller* is a trademark of Lantronix, Inc.

Patented: patents.lantronix.com; additional patents pending.

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

Open Source Software

Some applications are Open Source software licensed under the Berkeley Software Distribution (BSD) license, the GNU General Public License (GPL) as published by the Free Software Foundation (FSF), or the Python Software Foundation (PSF) License Agreement for Python 2.7.3 (Python License). Lantronix grants you no right to receive source code to the Open Source software; however, in some cases, rights and access to source code for certain Open Source software may be available directly from Lantronix' licensors. Your use of each Open Source component or software is subject to the terms of the applicable license. The BSD license is available at <http://opensource.org/licenses>. The GNU General Public License is available at <http://www.gnu.org/licenses/>. The Python License is available at <http://cmpt165.csil.sfu.ca/Python-Docs/license.html>. Your use of each Open Source component or software is subject to the terms of the applicable license.

OPEN SOURCE SOFTWARE IS DISTRIBUTED WITHOUT ANY WARRANTY, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SEE THE APPLICABLE LICENSE AGREEMENT FOR ADDITIONAL INFORMATION.

Warranty

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

Contacts

Lantronix, Inc.

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

Sales Offices

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

Disclaimer

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
January 2011	A	Initial document.
July 2011	B	Updated document to firmware release 7.2.0.0. Includes the new Bridging feature.
July 2011	C	Added chapter on OEM branding capabilities.
February 2013	D	Updated document to firmware release 7.3.0.1R7.
January 2015	E	Updated document to firmware release 7.9.0.1.
August 2015	F	Updated restriction information related to the line 3 tunnel, the tunnel 3 connect mode, and AdHoc mode connection. Updated SPI interface support information.
March 2017	G	Updated document to firmware release 8.0.0.0. Changes include adding Modbus, IPv6, TCP Keep Alive, IKEv2, and updating log verbosity, network settings, system setup, email setup, settings for WLAN Quick Connect and WLAN profile settings, and compliance updates.

Table of Contents

Intellectual Property	2
Open Source Software	2
Warranty	2
Contacts	2
Disclaimer	3
Revision History	3
List of Figures	11
List of Tables	12
1: Using This Guide	15
Purpose and Audience	15
Summary of Chapters	15
Additional Documentation	16
2: Introduction	17
Key Features	17
Applications	18
Protocol Support	18
Troubleshooting Capabilities	18
Configuration Methods	19
Addresses and Port Numbers	19
Hardware Address	19
IP Address	19
Port Numbers	19
Product Information Label	20
3: Using DeviceInstaller	21
Accessing PremierWave EN Using DeviceInstaller	21
Device Detail Summary	22
4: Configuration Using Web Manager	24
Accessing Web Manager	24
Device Status Page	25
Web Manager Components	26
Navigating Web Manager	27
5: Network Settings	30
Network 1 Status	30
Network 1 (eth0) Interface Settings	30

To Configure Network 1 Interface Settings _____	32
Network 1 (eth0) Link Settings _____	33
Network 1 (eth0) QoS _____	33
To Configure Network 1 QoS Settings _____	34
Network 1 (eth0) Failover _____	35
To Configure Network 1 Failover Settings _____	35
Network 2 Status _____	35
Network 2 (wlan0) Interface Settings _____	36
To Configure Network 2 Interface Settings _____	37
SmartRoam _____	37
Network 2 (wlan0) Link Settings _____	38
To Configure Network 2 Link Settings _____	38
Network 2 (wlan0) QoS _____	39
To Configure Network 2 QoS Settings _____	40
WLAN Link Status and Scan Commands _____	40
To View WLAN Link Scan and Status Information _____	42
Network 2 (wlan0) Failover _____	42
To Configure Network 2 Failover Settings _____	43
WLAN Profiles _____	43
To Configure WLAN Profiles _____	43
To Configure WLAN Profile Basic Settings _____	44
To Configure WLAN Profile Advanced Settings _____	45
WLAN Profile Security Settings _____	46
To Configure WLAN Profile Security Settings _____	47
WLAN Profile WEP Settings _____	47
To Configure WLAN Profile WEP Settings _____	49
WLAN Profile WPA and WPA2/IEEE802.11i Settings _____	49
To Configure WLAN Profile WPA and WPA/IEEE802.11i Settings _____	51
WLAN Quick Connect _____	51
To Configure WLAN Quick Connect _____	52
Gateway _____	52
Status _____	52
WAN _____	53
WAN MAC Address Filters _____	53
To Configure Gateway WAN Settings _____	53
Port Forwarding _____	54
To Configure Gateway Port Forwarding Settings _____	55
Static Routes _____	55
To Configure Gateway Static Route Settings _____	55
DHCP Server _____	56
To Configure Gateway DHCP Server Settings _____	56
Static Lease Listing _____	56
Routing Protocols _____	57

To Configure Gateway Routing Protocol Settings	58
Virtual IP	58
To Configure Gateway Virtual IP	58
DDNS	59
To Configure Gateway WAN Settings	59
VPN	60
To Configure VPN Settings	61
GRE Settings	62
To Configure Tunnel Serial Settings	62

6: Action Settings **63**

Alarms and Reports	63
Actions	63
To Configure Action Settings	64
Python	65
IDE	65
Applications	65
To Configure Application Settings	66

7: Line and Tunnel Settings **67**

Line Statistics	67
USB-CDC-ACM	67
Line Settings	68
To Configure Line Settings	68
To Configure Line Command Mode	70
Tunnel Statistics	71
To View Tunnel Statistics	71
Tunnel Settings	71
Serial Settings	71
To Configure Tunnel Serial Settings	72
Packing Mode	72
To Configure Tunnel Packing Mode Settings	73
Accept Mode	73
To Configure Tunnel Accept Mode Settings	76
Connect Mode	76
Connecting Multiple Hosts	79
Host List Promotion	80
Disconnect Mode	80
To Configure Tunnel Disconnect Mode Settings	80
Modem Emulation	81
To Configure Tunnel Modem Emulation Settings	82

8: Terminal and Host Settings	83
Terminal Settings _____	83
To Configure the Terminal Network Connection _____	84
To Configure the Terminal Line Connection _____	84
Host Configuration _____	84
To Configure Host Settings _____	85
9: Configurable Pin Manager	86
CPM: Configurable Pins _____	86
CPM: Groups _____	87
To Configure CPM Settings _____	88
10: Network Services	89
DNS Settings _____	89
To View or Configure DNS Settings: _____	89
FTP Settings _____	90
To Configure FTP Settings _____	90
Syslog Settings _____	90
To View or Configure Syslog Settings _____	91
HTTP Settings _____	91
To Configure HTTP Settings _____	92
To Configure HTTP Authentication _____	93
RSS Settings _____	93
To Configure RSS Settings _____	94
SNMP Settings _____	94
To Configure SNMP Settings _____	95
Discovery _____	95
To Configure Discovery _____	95
SMTP Settings _____	96
To Configure SMTP Settings _____	96
Email Settings _____	96
To View, Configure, and Send Email _____	97
11: Security Settings	98
Public Key Infrastructure _____	98
TLS (SSL) _____	98
Digital Certificates _____	99
Trusted Authorities _____	99
Obtaining Certificates _____	99
Self-Signed Certificates _____	99
Certificate Formats _____	99
OpenSSL _____	100

Steel Belted RADIUS _____	100
Free RADIUS _____	100
SSH Settings _____	101
SSH Server Host Keys _____	101
SSH Client Known Hosts _____	102
SSH Server Authorized Users _____	102
SSH Client Users _____	103
To Configure SSH Settings _____	104
SSL Settings _____	104
Create a New Credential _____	104
To Create a New Credential _____	105
Upload Certificate _____	105
Certificate and Key Generation _____	106
To Configure an Existing SSL Credential _____	107
Trusted Authorities _____	107

12: Maintenance and Diagnostics Settings 109

Filesystem Settings _____	109
Statistics _____	109
To View Statistics _____	109
File Display _____	109
To Display Files _____	110
File Modification _____	110
File Transfer _____	110
To Transfer or Modify Filesystem Files _____	111
Protocol Stack Settings _____	111
IP Settings _____	111
To Configure IP Protocol Stack Settings _____	112
ICMP Settings _____	112
To Configure ICMP Protocol Stack Settings _____	112
To View ICMP Protocol Stack Settings _____	112
ARP Settings _____	113
To Configure ARP Network Stack Settings _____	113
Diagnostics _____	114
Hardware _____	114
To View Hardware Information _____	114
IP Sockets _____	114
To View the List of IP Sockets _____	114
Ping _____	114
To Ping a Remote Host _____	115
Traceroute _____	115
To Perform a Traceroute _____	115
Log _____	116

To Configure the Diagnostic Log Output	116
Memory	116
To View Memory Usage	116
Processes	117
To View Process Information	117
Threads	117
To View Thread Information	117
Clock	117
To Specify Clock Setting Method	118
System Settings	118
To Reboot or Restore Factory Defaults	119

13: Management Interface Settings **120**

Command Line Interface Settings	120
Basic CLI Settings	120
To View and Configure Basic CLI Settings	120
Telnet Settings	121
To Configure Telnet CLI Settings	121
SSH CLI Settings	121
To Configure SSH Settings	122
XML Settings	122
XML: Export Configuration	122
To Export Configuration in XML Format	123
XML: Export Status	123
To Export in XML Format	123
XML: Import Configuration	124
To Import Configuration in XML Format	125

14: Bridging **126**

Bridging Configuration	126
To configure and enable bridging:	126
Bridging Operation	127
Bridge Configuration	127
To View or Configure Bridge Settings	127

15: Security in Detail **129**

Public Key Infrastructure	129
TLS (SSL)	129
Digital Certificates	129
Trusted Authorities	129
Obtaining Certificates	130
Self-Signed Certificates	130

Certificate Formats _____	130
OpenSSL _____	130
Steel Belted RADIUS _____	131
Free RADIUS _____	131
16: Updating Firmware	132
Obtaining Firmware _____	132
Loading New Firmware through Web Manager _____	132
Loading New Firmware through FTP _____	134
17: Branding the PremierWave EN Device	135
Web Manager Customization _____	135
Short and Long Name Customization _____	136
To Customize Short or Long Names _____	136
Appendix A: Lantronix Technical Support	137
Appendix B: Binary to Hexadecimal Conversions	138
Converting Binary to Hexadecimal _____	138
Conversion Table _____	138
Scientific Calculator _____	138
Appendix C: Compliance	140
Appendix D: USB-CDC-ACM Device Driver File for Windows Hosts	142
Creating a USB-CDC-ACM Device Driver File _____	142
Installing the USB-CDC-ACM Device Driver File _____	145

List of Figures

Figure 2-1 PremierWave EN Unit Product Label	20
Figure 4-1 Device Status Page	25
Figure 4-2 Components of the Web Manager Page	26
Figure 16-1 Uploading New Firmware	133

List of Tables

Table 4-3 Web Manager Pages _____	27
Table 5-1 Network Interface Settings _____	30
Table 5-2 Network 1 (eth0) Link Settings _____	33
Table 5-3 Network 1 (eth0) QoS Settings _____	34
Table 5-4 Adding or Deleting Network 1 (eth0) QoS Settings _____	34
Table 5-5 Network 1 (eth0) Failover Settings _____	35
Table 5-6 Network 2 (wlan0) Interface Settings _____	36
Table 5-7 Network 2 (wlan0) Link Settings _____	38
Table 5-8 Network 2 (wlan0) QoS Settings _____	39
Table 5-9 Adding or Deleting Network 2 (wlan0) QoS Settings _____	39
Table 5-10 Network 2 Link Scan _____	40
Table 5-11 Network 2 Link Scan Results on Web Manager _____	40
Table 5-12 Network 2 Link Status _____	41
Table 5-13 Network 2 (wlan0) Failover Settings _____	42
Table 5-14 Creating, Deleting or Enabling WLAN Profiles _____	44
Table 5-15 WLAN Profile Basic Settings _____	44
Table 5-16 WLAN Profile Advanced Settings _____	45
Table 5-17 WLAN Profile Security Settings _____	46
Table 5-18 Additional WEP Settings for WLAN Profile. _____	48
Table 5-19 WLAN Profile WPA and WPA2/IEEE802.11i Settings _____	49
Table 5-20 WLAN Quick Connect _____	51
Table 5-21 WAN Configuration _____	53
Table 5-22 Adding a New MAC Address Filters _____	53
Table 5-23 Port Forwarding Rules List _____	54
Table 5-24 Adding a New Port Forwarding Rule _____	54
Table 5-25 Static Route Setting Routes _____	55
Table 5-26 Adding a New Static Route _____	55
Table 5-27 DHCP Settings _____	56
Table 5-28 Static Lease Listing _____	57
Table 5-29 Add a Static Lease _____	57
Table 5-30 Routing Protocol Settings _____	57
Table 5-31 Virtual IP Settings _____	58
Table 5-32 Adding a Virtual IP _____	58
Table 5-33 DDNS Configuration _____	59
Table 5-34 VPN Configuration _____	60

Table 5-35 GRE Settings _____	62
Table 6-1 Action Settings _____	63
Table 6-2 Script Settings _____	66
Table 7-1 Line Configuration Settings _____	68
Table 7-2 Line Command Mode Settings _____	70
Table 7-3 Tunnel Serial Settings _____	71
Table 7-4 Tunnel Packing Mode Settings _____	72
Table 7-5 Tunnel Accept Mode Settings _____	74
Table 7-6 Tunnel Connect Mode Settings _____	77
Table 7-7 Tunnel Disconnect Mode Settings _____	80
Table 7-8 Tunnel Modem Emulation Settings _____	81
Table 8-1 Terminal on Network and Line Settings _____	83
Table 8-2 Host Configuration _____	84
Table 9-1 Current Configurable Pins _____	86
Table 9-2 CP Status _____	86
Table 9-3 CPM Group Current Configuration _____	87
Table 9-4 CPM Group Status _____	87
Table 10-1 DNS Settings _____	89
Table 10-2 FTP Settings _____	90
Table 10-3 Syslog Settings _____	90
Table 10-4 HTTP Settings _____	91
Table 10-5 HTTP Authentication Settings _____	93
Table 10-6 RSS Settings _____	93
Table 10-7 SNMP Settings _____	94
Table 10-8 Discovery Settings _____	95
Table 10-9 SMTP Settings _____	96
Table 10-10 Email Configuration _____	96
Table 11-1 SSH Server Host Keys _____	101
Table 11-2 SSH Client Known Hosts _____	102
Table 11-3 SSH Server Authorized Users _____	102
Table 11-4 SSH Client Users _____	103
Table 11-5 Create New Keys _____	103
Table 11-6 Create a New Credentials _____	105
Table 11-7 Upload Certificate Settings _____	105
Table 11-8 Certificate and Key Generation Settings _____	106
Table 12-1 File Statistics _____	109
Table 12-2 File Display Settings _____	109
Table 12-3 File Modification Settings _____	110

Table 12-4 File Transfer Settings _____	110
Table 12-5 IP Protocol Stack Settings _____	111
Table 12-6 ICMP Protocol Stack Settings _____	112
Table 12-7 ARP Protocol Stack Settings _____	113
Table 12-8 Ping Settings _____	114
Table 12-9 Traceroute Settings _____	115
Table 12-10 Log Settings _____	116
Table 12-11 Clock Settings _____	117
Table 12-12 System Settings _____	118
Table 13-1 CLI Configuration Settings _____	120
Table 13-2 Telnet Settings _____	121
Table 13-3 SSH Settings _____	121
Table 13-4 XML Exporting Configuration _____	122
Table 13-5 Exporting Status _____	123
Table 13-6 Import Configuration from Filesystem Settings _____	124
Table 14-1 Bridge Settings _____	127
Table 17-1 Short and Long Name Settings _____	136

1: Using This Guide

Purpose and Audience

This guide provides the information needed to configure, use, and update the Lantronix® PremierWave® EN embedded system on module (SOM). 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
2: Introduction	Main features of the product and the protocols it supports. Includes technical specifications.
3: Using DeviceInstaller	Instructions for viewing the device and configuration using UPnP and the DeviceInstaller utility.
4: Configuration Using Web Manager	Instructions for accessing Web Manager and using it to configure settings for the device.
5: Network Settings	Instructions for configuring network settings.
6: Action Settings	Instructions for configuring alarm settings.
7: Line and Tunnel Settings	Instructions for configuring line and tunnel settings.
8: Terminal and Host Settings	Instructions for configuring terminal and host settings.
9: Configurable Pin Manager	Information about the Configurable Pin Manager (CPM) including how to set the configurable pins to work with a device and instructions for accessing Web Manager and using it to configure settings for the device.
10: Network Services	Instructions for configuring DNS, FTP, HTTP and Syslog settings.
11: Security Settings	Instructions for configuring SSL security settings.
12: Maintenance and Diagnostics Settings	Instructions to view statistics, files, and diagnose problems.
13: Management Interface Settings	Instructions for configuring CLI and XML settings.
14: Bridging	Instructions for bridging configuration.
15: Security in Detail	
16: Updating Firmware	Instructions for obtaining and updating the latest firmware for the PremierWave device.
17: Branding the PremierWave EN Device	Instructions on how to brand your device.
Appendix A: Lantronix Technical Support	Instructions for contacting Lantronix Technical Support.
Appendix B: Binary to Hexadecimal Conversions	Instructions for converting binary values to hexadecimal.
Appendix C: Compliance	Lantronix compliance information.
Appendix D: USB-CDC-ACM Device Driver File for Windows Hosts	Information about the device driver file for windows host.

Additional Documentation

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

Document	Description
PremierWave EN Embedded System on Module Integration Guide	Information about the PremierWave hardware, testing the device server using the demonstration board, and integrating the unit into your product.
PremierWave Embedded EN System on Module Command Reference	Instructions for accessing Command Mode (the command line interface) using a Telnet connection, SSH connection or through the serial port. Detailed information about the commands. Also provides details for XML configuration and status.
PremierWave EN Embedded System on Module Quick Start	Instructions for getting the PremierWave evaluation board device up and running.
PremierWave Embedded System on Module Evaluation Board User Guide	Information needed to use the PremierWave on the evaluation board.
DeviceInstaller™ Utility Online Help	Instructions for using the Windows® operating system-based utility to locate the embedded device server and to view its current settings.
Com Port Redirector Quick Start and Online Help	Instructions for using the Windows operating system-based utility to create virtual com ports.
Secure Com Port Redirector User Guide	Instructions for using the Windows operating system-based utility to create secure virtual com ports.

2: Introduction

The PremierWave EN embedded system on module is a complete network-enabling solution in a 30 (1.181) X 55 (2.165) X 6.45 (0.248) package. This compact system on module empowers original equipment manufacturers (OEMs) to go to market quickly and easily with Ethernet and/or wireless networking and web page serving capabilities built into their products. [DIMS = mm (in.)]

Key Features

- ◆ **Power Supply:** Regulated 3.3V input required. There are internal step down regulators to convert to processor core and memory required voltages: a step-down converter to 1.5V for the processor core and 1.8V for the memory subsystem. All voltages have LC filtering to minimize noises and emissions.
- ◆ **Controller:** 32-bit ARM9 microprocessor running at 400 megahertz (Mhz) with 32 KB Data Cache and 32 Kilobytes (KB). Instruction Cache
- ◆ **Memory:** Up to 64 MB SDRAM, 256 MB NAND Flash (64 MB default). Up to 16 MB serial SPI Flash (8 MB default).
- ◆ **Ethernet:** 10/100 megabits per second (Mbps) Ethernet transceiver.
- ◆ **Wireless:** Dual Band 802.11 a/b/g/n with an on-board antenna and option for external antennas and diversity.
- ◆ **Serial Ports:** Two high speed RS232/RS422/RS485* serial ports with all hardware handshaking signals. Baud rate is software selectable (300 bps to 921600 bps). One emulated serial port on the USB Device Port (up to Full Speed 12 Mbps), using standard CDC/ACM protocol.
- ◆ **USB Ports:** Two USB 2.0 full speedOne USB 2.0 Full Speed (12 Mbps) host device port
- ◆ Master/Slave high speed SPI interface
- ◆ I2C interface
- ◆ Configurable I/O Pins (CPs): Up to nine pins are configurable as general purpose I/Os if no DTR or DCD is used on serial ports. Not 5V tolerant.
- ◆ Interface Signals: 3.3V-level interface signals.
- ◆ Configuration via CLI, XML and HTTP
- ◆ Ethernet to wireless tunneling
- ◆ Lantronix® SmartRoam™ technology
- ◆ **Temperature Range:** Operates over a temperature range of -40°C to +85°C (-40°F to 158°F). The storage temperature range is -40°C to 85°C (-40°F to 185°F).

Applications

The PremierWave EN embedded system on module is suitable for these application scenarios:

- ◆ ATM machines
- ◆ CNC controllers
- ◆ Data collection devices
- ◆ Universal Power Supply (UPS) management unit
- ◆ Telecommunications equipment
- ◆ Data display devices
- ◆ Security alarms and access control devices
- ◆ Handheld instruments
- ◆ Modems
- ◆ Time/attendance clocks and terminals
- ◆ Patient Monitoring Devices
- ◆ Glucose Analyzers
- ◆ Infusion Pumps

Protocol Support

The PremierWave EN embedded system on module contains a full-featured IP networking stack:

- ◆ ARP, SNMP v1/v2c/v3, IPv4, UDP, TCP, ICMP, BOOTP, DHCP, Auto IP, Telnet, FTP, FTPS, DNS, TFTP, SSH, SSL/TLS, and Syslog for network communications and management.
- ◆ TCP, UDP, SSH, SSL and Telnet tunneling to the serial port.
- ◆ TFTP for uploading/downloading files.
- ◆ FTP and HTTP/HTTPS for firmware upgrades and uploading/downloading files.
- ◆ SMTP AUTH, HTTP/HTTPS Post, FTP/FTPS Put and SNMP Traps

Troubleshooting Capabilities

The PremierWave EN device server offers a comprehensive diagnostic toolset that lets you troubleshoot problems quickly and easily. Available from the CLI or Web Manager, the diagnostic tools let you:

- ◆ View critical hardware, memory, buffer pool, IP socket information and routing table
- ◆ Perform ping and traceroute operations
- ◆ Conduct forward or reverse DNS lookup operations
- ◆ View all processes currently running on the PremierWave EN embedded system on module including CPU utilization
- ◆ View system log messages

Configuration Methods

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

- ◆ **Web Manager:** View and configure all settings easily through a web browser using the Lantronix Web Manager. (See [Configuration Using Web Manager on page 24.](#))
- ◆ **DeviceInstaller:** Configure the IP address and related settings and view current settings on the PremierWave EN embedded system on module using a Graphical User Interface (GUI) on a PC attached to a network. You will need the latest version of the Lantronix® DeviceInstaller™ utility. (See [Accessing the PremierWave XC HSPA+ Device Using DeviceInstaller on page 30.](#))
- ◆ **Command Mode:** There are a few methods for accessing Command Mode (CLI): making a Telnet or SSH connection, or connecting a PC or other host running a terminal emulation program to the unit's serial port. (See the *PremierWave EN Embedded System on Module Command Reference* for instructions and available commands.)
- ◆ **XML:** The PremierWave EN embedded system on module supports XML-based configuration and setup records that make device configuration transparent to users and administrators. XML is easily editable with a standard text or XML editor. (See the *PremierWave EN Embedded System on Module Command Reference* for instructions and commands).

Addresses and Port Numbers

Hardware Address

The hardware address is also referred to as the Ethernet address, physical address, or MAC address. The first three bytes of the Ethernet address are fixed and identify the unit as a Lantronix product. The fourth, fifth, and sixth bytes are unique numbers assigned to each unit. Sample hardware address:

- ◆ 00-80-A3-14-1B-18
- ◆ 00:80:A3:14:1B:18

IP Address

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

Port Numbers

Every TCP connection and every UDP datagram is defined by a destination and source IP address, and a destination and source port number. For example, a Telnet server commonly uses TCP port number 23.

The following is a list of the default server port numbers running on the PremierWave EN embedded system on module:

- ◆ TCP Port 22: SSH Server (Command Mode configuration)
- ◆ TCP Port 23: Telnet Server (Command Mode configuration)

- ◆ TCP Port 80: HTTP (Web Manager Configuration)
- ◆ TCP Port 21: FTP
- ◆ UDP Port 30718: LDP (Lantronix Discovery Protocol) port
- ◆ TCP/UDP Port 10001: Tunnel 1 (see note below)

Note: Additional TCP/UDP ports and tunnels will be available, depending on the product type. The default numbering of each additional TCP/UDP port and corresponding tunnel will increase sequentially (i.e., TCP/UDP Port 1000X: Tunnel X).

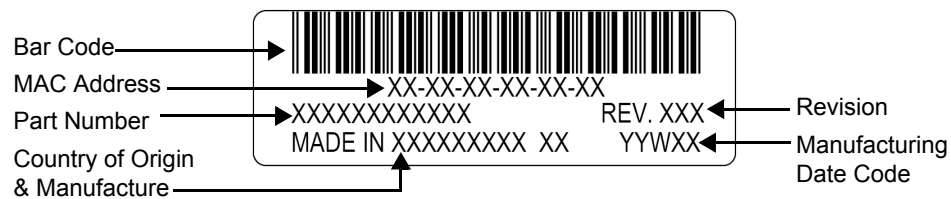
Product Information Label

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

- ◆ Part Number
- ◆ Hardware Address (MAC Address)
- ◆ Country of Origin
- ◆ Product Revision
- ◆ Manufacturing Date Code

Note: The hardware address on the label is also the product serial number. The hardware address on the label is the address for the Ethernet (eth0) interface. The WLAN (wlan0) interface uses the Ethernet address "+1". For example, if the product label hardware address is 00-80-A3-14-1B-18, then the Ethernet address is 00-80-A3-14-1B-18 and the WLAN address is 00-80-A3-14-1B-19.

Figure 2-1 PremierWave EN Unit Product Label



3: Using DeviceInstaller

This chapter covers the steps for locating an PremierWave EN unit and viewing its properties and device details. The Lantronix® DeviceInstaller™ application is a free utility program provided by Lantronix that discovers, configures, upgrades and manages Lantronix device servers.

Notes:

- ◆ For instructions on using the DeviceInstaller utility to configure the IP address and related settings or for more advanced features, see the DeviceInstaller Online Help.
- ◆ Auto IP generates a random IP address in the range of 169.254.0.1 to 169.254.255.254, with a netmask of 255.255.0.0, if no BOOTP or DHCP server is found. These addresses are not routable.

Accessing PremierWave EN Using DeviceInstaller

Note: Make note of the MAC address. It may be needed to perform various functions in the DeviceInstaller application.

To use the DeviceInstaller utility, first install the latest version from the downloads page on the Lantronix web site www.lantronix.com/downloads.

1. Run the executable to start the installation process and respond to the installation wizard prompts. (If prompted to select an installation type, select **Typical**.)
2. Click **Start -> All Programs -> Lantronix -> DeviceInstaller 4.3 -> DeviceInstaller**.
3. When DeviceInstaller starts, it will perform a network device search. To perform another search, click **Search**.
4. Expand the PremierWave folder by clicking the + symbol next to the folder icon. The list of available Lantronix PremierWave EN devices appears.
5. Select the PremierWave EN unit by expanding its entry and clicking on its IP address to view its configuration.
6. On the right page, click the **Device Details** tab. The current PremierWave EN device configuration appears. This is only a subset of the full configuration; the full configuration may be accessed via Web Manager, CLI or XML.

Device Detail Summary

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

Current Settings	Description
Name	Shows "PremierWave EN".
DHCP Device Name	Displays one of the names the PremierWave EN device will send to the DHCP server if it is configured to obtain an address in this manner.
Group	Configurable field. Enter a group to categorize the PremierWave EN unit. Double-click the field, type in the value, and press Enter to complete. This group name is local to this PC and is not visible on other PCs or laptops using DeviceInstaller.
Comments	Configurable field. Enter comments for the PremierWave EN device. Double-click the field, type in the value, and press Enter to complete. This description or comment is local to this PC and is not visible on other PCs or laptops using DeviceInstaller.
Device Family	Shows the PremierWave EN device family type as "PremierWave".
Short Name	Shows "premierwave_en" by default.
Long Name	Shows "Lantronix PremierWave EN" by default.
Type	Shows the device type as "PremierWave".
ID	Shows the PremierWave EN ID embedded within the unit.
Hardware Address	Shows the PremierWave EN hardware (MAC) address.
Firmware Version	Shows the firmware currently installed on the PremierWave EN.
Extended Firmware Version	Provides additional information on the firmware version.
Online Status	Shows the PremierWave EN status as Online , Offline , Unreachable (the PremierWave EN device is on a different subnet), or Busy (the PremierWave EN is currently performing a task).
IP Address	Shows the PremierWave EN current IP address. To change the IP address, click the Assign IP button on the DeviceInstaller menu bar.
IPv6 Link Local Address	Shows the current PremierWave IPv6 link local address.
IPv6 Global Address	Shows the current PremierWave IPv6 global address.
IP Address was Obtained	Appears "Dynamically" if the PremierWave EN unit automatically received an IP address (e.g., from DHCP). Appears "Statically" if the IP address was configured manually. If the IP address was assigned dynamically, the following fields appear: <ul style="list-style-type: none"> ◆ Obtain via DHCP with values of True or False. ◆ Obtain via BOOTP with values of True or False.
Subnet Mask	Shows the subnet mask specifying the network segment on which the PremierWave EN device resides.
Gateway	Shows the IP address of the router of this network. There is no default.
Interfaces	Shows information about the Ethernet (eth0) and wireless (wlan0) interfaces for your PremierWave unit. Click the + sign beside eth0 or wlan0, and then the Status and Configuration subcategories to view status and configuration information on these interfaces.
Number of Serial Ports	Shows the number of serial ports on this PremierWave EN embedded device serverdevice server.

Current Settings	Description
Supports Configurable Pins	Shows True, indicating configurable pins are available on the PremierWave EN embedded device server device server.
Supports Email Triggers	Shows True , indicating email triggers are available on the PremierWave embedded device serverdevice server.
Telnet Supported	Indicates whether Telnet is enabled on this PremierWave EN embedded device serverdevice server.
Telnet Port	Shows the PremierWave EN port for Telnet sessions.
Web Port	Shows the PremierWave EN port for Web Manager configuration (if Web Enabled field is True).
Firmware Upgradable	Shows True , indicating the PremierWave firmware is upgradable as newer versions become available.

4: Configuration Using Web Manager

This chapter describes how to configure the PremierWave EN embedded system on module using Web Manager, the Lantronix browser-based configuration tool. The unit's configuration is stored in non-volatile memory and is retained without power. All changes take effect immediately, unless otherwise noted. It contains the following sections:

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

Accessing Web Manager

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

To access Web Manager, perform the following steps:

1. Open a standard web browser. Lantronix supports the latest versions of Internet Explorer, Mozilla Firefox, Safari or Chrome web browsers.
2. Enter the IP address or hostname of the PremierWave EN unit in the address bar. The IP address may have been assigned manually using DeviceInstaller (see the *PremierWave EN Embedded System on Module Quick Start Guide*) or automatically by DHCP.
3. Enter your username and password. The factory-default username is “**admin**” and “**PASS**” is the default password. The Device Status web page displays configurations including network settings, line settings, tunneling settings, and product information.

Device Status Page

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

Figure 4-1 Device Status Page

PremierWave EN LANTRONIX

Status [Logout](#)

Device Status

Product Information		
Product Type:	Lantronix PremierWave EN (premierwave_en)	
Firmware Version:	8.0.0.0R12	
Radio Firmware Version:	3.2.12.0/1.1.6.71/6.134	
Build Date:	Feb 6 18:13:11 PST 2017	
Serial Number:	0080A3956D9C	
Uptime:	3 days 10:41:52	
Current Date/Time:	Fri Feb 10 07:10:45 UTC 2017	
Permanent Config:	Saved	
Region:	United States	
Network Settings		
Name servers		
Primary DNS:	172.19.1.1	
Secondary DNS:	172.19.1.2	
Interface eth0		
Link:	Auto 10/100 Mbps Auto Half/Full (100 Mbps Full)	
MAC Address:	00:80:A3:95:6D:9C	
Hostname:	<None>	
MTU:	1500	
IP Address:	172.19.100.43/16 <DHCP>	
Network Mask:	255.255.0.0 <DHCP>	
Default Gateway:	172.19.0.1 <DHCP>	
Domain:	eng.lantronix.com <DHCP>	
IPv6 Global Address:	2001:db80:ac13:d91e:280:a3ff:fe95:6d9c/64 <DHCP>	
IPv6 Global Address:	2001:db80:ac13:d91e:ab0:7af8:763c:7778/64 <DHCP>	
IPv6 Link-local Address:	fe80::280:a3ff:fe95:6d9c/64	
IPv6 Default Gateway:	fe80::6600:f1ff:feb6:586e fe80::20c:29ff:fe5f:dab <DHCP>	
IPv6 Domain:	patdomain.local	
Interface wlan0		
Link:	ESTABLISHED	
MAC Address:	00:80:A3:95:6D:9D	
Hostname:	<None>	
MTU:	1500	
IP Address:	172.19.100.83/16 <DHCP>	
Network Mask:	255.255.0.0 <DHCP>	
Default Gateway:	172.19.0.1 <DHCP>	
Domain:	eng.lantronix.com <DHCP>	
IPv6 Global Address:	2001:db80:ac13:d91e:280:a3ff:fe95:6d9d/64 <DHCP>	
IPv6 Global Address:	2001:db80:ac13:d91e:90bf:ade:60fd:2ed0/64 <DHCP>	
IPv6 Link-local Address:	fe80::280:a3ff:fe95:6d9d/64	
IPv6 Default Gateway:	fe80::6600:f1ff:feb6:586e fe80::20c:29ff:fe5f:dab <DHCP>	
IPv6 Domain:	patdomain.local	
Line Settings		
Line 1:	RS232, 9600, None, 8, 1, None	
Line 2:	RS232, 9600, None, 8, 1, None	
Line 3:	USB-CDC-ACM	
Tunneling	Connect Mode	Accept Mode
Tunnel 1:	Disabled	Waiting
Tunnel 2:	Disabled	Waiting
Tunnel 3:	Disabled	Waiting
VPN		
Status:	Disabled	
IP Address:	<None>	

Copyright © Lantronix, Inc. 2007-2017. 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

Note: The **Logout** button is available on any web page. Logging out of the web page forces re-authentication the next time the web page is accessed.

The screenshot displays the PremierWave EN Web Manager interface. The header shows the product name and the Lantronix logo. A menu bar on the left lists various system components. The main content area is titled "Network 1 (eth0) Interface Configuration" and contains a configuration table. A warning message is displayed above the table. The right side of the page contains help text and a [Logout] button. The footer includes copyright information.

Items to configure (Network 1, Network 2)

Links to subpages (Interface, Link, QoS, Failover)

Logout button ([Logout])

Configuration and/or Status Area

Information and Help Area

State:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
IPv4 State:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
BOOTP Client:	<input type="radio"/> On <input checked="" type="radio"/> Off
DHCP Client:	<input checked="" type="radio"/> On <input type="radio"/> Off
Priority:	1
IP Address:	<None>
Default Gateway:	<None>
Hostname:	
Domain:	
DHCP Client ID:	
Primary DNS:	<None>
Secondary DNS:	<None>
MTU:	1500
IPv6 State:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
IPv6 DHCP Client:	<input checked="" type="radio"/> On <input type="radio"/> Off
IPv6 Address:	<None>
IPv6 Default Gateway:	<None>
IPv6 Domain:	
IPv6 Primary DNS:	<None>
IPv6 Secondary DNS:	<None>

WARNING: Priority for interface eth0 and wlan0 are the same. Default priorities will be applied for all interfaces.

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

State: Enable or Disable the interface.

The following items require a reboot to take effect:

- State
- BOOTP Client On/Off
- DHCP Client On/Off
- Priority
- IP Address
- DHCP Client ID

If BOOTP or DHCP is turned on, any configured IP Address, Network Mask, Gateway, Hostname, or Domain will be ignored. BOOTP/DHCP will auto-discover and eclipse those configuration items.

If both BOOTP and DHCP are turned on, DHCP will run, but not BOOTP.

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

Each interface can be assigned a Priority from 0-10.

Note: Lower priority number means higher preference.

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)

IPv6 Address may be entered alone. IPv6 Address and IPv6 Default Gateway may be entered with scope id. IPv6 DNS entries can also be entered here.

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

Copyright © Lantronix, Inc. 2007-2017. All rights reserved.

Web Manager pages have these sections:

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

The main area of the page has these additional sections:

- ◆ Links near the top of many pages, such as the one in the example above, enable you to link to additional subpages. On some pages, you must also select the item you are configuring, such as a tunnel.
- ◆ In the middle of many pages, you can select or enter new configuration settings. Some pages show status or statistics in this area rather than allow you to enter settings.
- ◆ At the bottom of most pages, the current configuration is displayed. In some cases, you can reset or clear a setting.
- ◆ When a parameter is changed on the page, a **Submit** button will appear. Click on this button to save the change.
- ◆ The information or help area shows information or instructions associated with the page.
- ◆ A **Logout** link is available at the upper right corner of every page. In Chrome or Safari, it is necessary to close out of the browser to completely logout. If necessary, reopen the browser to log back in.
- ◆ The footer appears at the very bottom of the page. It contains copyright information and a link to the Lantronix home page.

Navigating Web Manager

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

Note: *There may be times when you must reboot the PremierWave EN device 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 25-30 seconds after rebooting the unit before attempting to make any subsequent connections.*

Table 4-3 Web Manager Pages

Web Manager Page	Description	See Page
Status	Shows product information, network, line, and tunneling settings.	25
Actions	Allows you to view and configure the actions for a specific alarm or report.	63
Applications	Allows you to view and configure Application settings.	65
Bridge	Allows you to configure a bridge and shows the current operational state of the bridge.	126
CLI	Shows Command Line Interface (CLI) statistics and lets you change the current CLI configuration settings.	120

Web Manager Page (continued)	Description	See Page
Clock	Allows you to view and configure the current date, time and time zone as it displays in web manager.	118
CPM	Shows information about the Configurable Pins Manager (CPM) and how to set the configurable pins and pin groups to work with a device.	86
Diagnostics	Lets you perform various diagnostic procedures.	114
Discovery	Allows you to view and modify the configuration and statistics for device discovery.	95
DDNS	Allows you to view and configure DDNS settings.	59
DNS	Shows the current configuration of the DNS subsystem and the DNS cache.	89
Email	Shows email statistics and lets you clear the email log, configure email settings, and send an email.	96
Filesystem	Shows file system statistics and lets you browse the file system to view a file, create a file or directory, upload files using HTTP, copy a file, move a file, or perform TFTP actions.	109
FTP	Shows statistics and lets you change the current configuration for the File Transfer Protocol (FTP) server.	90
Gateway	Shows statistics and lets you change the current configuration for the gateway.	52
GRE	Allows you to view and configure GRE settings.	62
Host	Lets you view and change settings for a host on the network.	84
HTTP	Shows HyperText Transfer Protocol (HTTP) statistics and lets you change the current configuration and authentication settings.	91
Line	Shows statistics and lets you change the current configuration and Command mode settings of a serial line.	68
Modbus	Shows the current connection status of the Modbus servers listening on the TCP ports and configure Modbus TCP server.	122
Network	Shows status and lets you configure the network interface.	30
Protocol Stack	Lets you perform lower level network stack-specific activities.	111
RSS	Lets you change current Really Simple Syndication (RSS) settings.	93
SmartRoam	Lets you configure SmartRoam options through Network Link Settings.	37
SMTP	Shows and allows modification of the current configuration of SMTP.	96
SNMP	Shows and allows modification of the current configuration of SNMP.	96
SSH	Lets you change the configuration settings for SSH server host keys, SSH server authorized users, SSH client known hosts, and SSH client users.	101
SSL	Lets you upload an existing certificate or create a new self-signed certificate.	104
Syslog	Lets you specify the severity of events to log and the server and ports to which the syslog should be sent.	90
System	Lets you reboot device, restore factory defaults, upload new firmware, and change the device long and short names.	118
Terminal	Lets you change current settings for a terminal.	83

Web Manager Page (continued)	Description	See Page
Tunnel	Lets you change the current configuration settings for an incoming tunnel connection.	71
VPN	Lets you view and configure VPN settings.	60
WLAN Profiles	Lets you view, edit, delete and create a WLAN profile on a device.	43
WLAN Quick Connect	Lets you change configuration settings for the Quick Connect.	51
XML	Lets you export XML configuration and status records, and import XML configuration records.	122

5: Network Settings

The Network Settings show the status of the PremierWave EN device interface/link and lets 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.

The PremierWave EN device server contains two interfaces. The Ethernet interface is called Network 1 or eth0, and the WLAN interface is called Network 2 or wlan0.

Notes:

- ◆ Some settings require a reboot to take effect. These settings are noted below.
- ◆ Wait a minimum of 25-30 seconds after rebooting the unit before attempting to make any subsequent connections.
- ◆ The blue text in the XML command strings of this chapter are to be replaced with a user-specified name.

Network 1 Status

In the Network 1 status pages, you can view both the current interface operational settings as well as the settings that would take effect upon a device reboot, as well as Link, QoS and Failover status information.

- ◆ To view Ethernet (eth0) Interface status, click **Network** on the menu and select **Network 1 -> Interface -> Status**.
- ◆ To view Ethernet (eth0) Link status, click **Network** on the menu and select **Network 1 -> Link -> Status**.
- ◆ To view Ethernet (eth0) QoS status, click **Network** on the menu and select **Network 1 -> QoS -> Status**.
- ◆ To view Ethernet (eth0) Failover status, click **Network** on the menu and select **Network 1 -> Failover -> Status**.

Network 1 (eth0) Interface Settings

Table 5-1 shows the network interface settings that can be configured.

These settings apply to both the Network 1 Ethernet (eth0) and the Network 2 WLAN (wlan0) interfaces, but are configured independently for each interface.

Table 5-1 Network Interface Settings

Network Interface Settings	Description
State	Select to enable or disable the interface.
IPv4 State	Select to enable or disable the IPv4 state.

Network Interface Settings (continued)	Description
BOOTP Client	<p>Select to turn On or Off. At boot up, after the physical link is up, the PremierWaveEN device will attempt to obtain IPv4 settings from a BOOTP server.</p> <p>Note: Overrides the configured IPv4 address/mask, gateway, hostname, and domain. When DHCP is Enabled, the system automatically uses DHCP, regardless of whether BOOTP is Enabled. Changing this value requires you to reboot the device.</p>
DHCP Client	<p>Select to turn On or Off. At boot up, after the physical link is up, the PremierWave EN unit will attempt to obtain IPv4 settings from a DHCP server and will periodically renew these settings with the server.</p> <p>Note: Overrides BOOTP, the configured IPv4 address/mask, gateway, hostname, and domain. Changing this value requires you to reboot the device.</p> <p>Note: Within Web Manager, click Renew to renew the DHCP lease.</p>
Priority	<p>Priority ranges from 0-10.</p> <p>Note: Lower priority number means higher preference.</p>
IP Address	<p>Enter the static IPv4 address to use for the interface. You may enter it alone or in CIDR format.</p> <p>Note: This setting will be used if Static IP is active (both DHCP and BOOTP are Disabled). Changing this value requires you to reboot the device. When DHCP or BOOTP is enabled, the PremierWave EN device tries to obtain an IPv4 address from a DHCP or BOOTP server. If it cannot, the PremierWave EN unit generates and uses an Auto IP address in the range of 169.254.xxx.xxx, with a network mask of 255.255.0.0.</p>
Default Gateway	<p>Enter the IPv4 address of the router for this network.</p> <p>Note: This setting will be used if Static IP is active (both DHCP and BOOTP are Disabled).</p>
Hostname	<p>Enter the hostname for the interface. It must begin with a letter or number, continue with a sequence of letters, numbers, or hyphens, and end with a letter or number. This setting will take effect immediately, but will not register the hostname with a DNS server until the next reboot.</p>
Domain	<p>Enter the domain name suffix for the interface.</p> <p>Note: This setting will be used when either Static IP or Auto IP is active, or if DHCP/BOOTP is active and no Domain Suffix was acquired from the server.</p>
DHCP Client ID	<p>Enter the ID if the DHCP server requires a DHCP Client ID option. The DHCP server's lease table shows IP addresses and MAC addresses for devices. The lease table shows the Client ID, in hexadecimal notation, instead of the PremierWave EN embedded system on module MAC address.</p>
Primary DNS	<p>Enter the IP address of the primary Domain Name Server.</p> <p>Note: This setting will be used when either Static IP or Auto IP is active, or if DHCP/BOOTP is active and no DNS server was acquired from the server.</p>
Secondary DNS	<p>Enter the IP address of the secondary Domain Name Server.</p> <p>Note: This setting will be used when either Static IP or Auto IP is active, or if DHCP/BOOTP is active and no DNS server was acquired from the server.</p>
MTU	<p>When DHCP is enabled, the MTU size is (usually) provided with the IP address. When not provided by the DHCP server, or using a static configuration, this value is used. The MTU size can be from 576 to 1500 bytes, the default being 1500 bytes.</p>

Network Interface Settings (continued)	Description
IPv6 State	Select to enable or disable the IPv6 state.
IPv6 DHCP Client	Select to turn On or Off . At boot up, after the physical link is up, the PremierWave unit will attempt to obtain IPv6 settings from a DHCPv6 server and will periodically renew these settings with the server.
IPv6 Address	Enter the static IPv6 address to use for the interface. <i>Note: This setting is used if Static IPv6 is active (DHCPv6 is Disabled). Changing this value requires a reboot. When DHCPv6 is enabled, the PremierWave EN tries to obtain an IPv6 address from a DHCPv6 server.</i>
IPv6 Default Gateway	Enter the default IPv6 Default Gateway.
IPv6 Domain	Enter the IPv6 domain name suffix for the interface. <i>Note: This setting will be used when Static IP is active, or if IPv6 DHCP client is active and no Domain Suffix was acquired from the server.</i>
IPv6 Primary DNS	Enter the IPv6 address of the primary Domain Name Server. <i>Note: This setting will be used when Static IP is active, or if IPv6 DHCP client is active and no Domain Suffix was acquired from the server.</i>
IPv6 Secondary DNS	Enter the IPv6 address of the secondary Domain Name Server. <i>Note: This setting will be used when Static IP is active, or if IPv6 DHCP client is active and no Domain Suffix was acquired from the server.</i>

To Configure Network 1 Interface Settings

Using Web Manager

- ◆ To modify Ethernet (eth0) settings, click **Network** on the menu and select **Network 1 -> Interface -> Configuration**.

Using the CLI

- ◆ To enter the eth0 command level: `enable -> config -> if 1`

Using XML

- ◆ Include in your file: `<configgroup name="interface" instance="eth0">`

Network 1 (eth0) Link Settings

Physical link parameters can be configured for an Ethernet (eth0) Network Link (see [Table 5-2](#)) and a WLAN (wlan0) Link Interface (see [Table 5-7](#)).

Table 5-2 Network 1 (eth0) Link Settings

Network 1 Ethernet (eth0) Link Settings	Description
Speed	Select the Ethernet link speed. (Default is Auto) ◆ Auto = Auto-negotiation of Link Speed ◆ 10 Mbps = Force 10 Mbps ◆ 100 Mbps = Force 100 Mbps
Duplex	Select the Ethernet link duplex mode. (Default is Auto) ◆ Auto = Auto-negotiation of Link Duplex ◆ Half = Force Half Duplex ◆ Full = Force Full Duplex

Notes:

- ◆ When speed is **Auto**, duplex must be **Auto** or **Half**.
- ◆ When speed is not **Auto**, duplex must be **Half** or **Full**.
- ◆ Fixed speed Full duplex will produce errors connected to Auto, due to duplex mismatch.

Network 1 (eth0) QoS

QoS (Quality of Service) can be enabled and configured for both Network 1 (eth0) and Network 2 (wlan0). If enabled, the router will control the flow of outbound traffic according to the user-defined filters. In other words, QoS improves performance by allowing the user to prioritize applications. Filters can be defined to prioritize traffic based on the source or destination network, source or destination port, or the source MAC address. Up to 32 user-defined filters can be added. The following are predefined priority classes:

- ◆ Network Control and Internetwork Control are typically used for network control packets such as ICMP and have the highest priorities.
- ◆ Move bandwidth allocation is a minimum 5% each to Network control.
- ◆ Voice: Bandwidth allocation is minimum 30%.
- ◆ Video: Bandwidth allocation is minimum 20%.
- ◆ Critical Applications: Bandwidth allocation is minimum 15%.
- ◆ Excellent Effort: Bandwidth allocation is minimum 10%.
- ◆ Best Effort: Bandwidth allocation is minimum 10%.
- ◆ Background: Bandwidth allocation is minimum 5% and has the lowest priority.

[Table 5-3](#) shows the network QoS settings that can be configured including adding new filters.

Table 5-3 Network 1 (eth0) QoS Settings

Network 1 (eth0) Settings	Description
State	Click to enable or disable state.
Import filters	Click to enable or disable import filters to import configurations from other interfaces.
Uplink Speed	Enter the maximum uplink speed. Set 0 to set speed to default.
Delete	Click the checkbox to the left of any existing QoS filter to be deleted and click the Submit button.
Filter type	Select the filter type from the drop-down window: <ul style="list-style-type: none"> ◆ Network ◆ Port
Network	Enter the Network, if the Network filter type is selected.
Ports	Enter the Port, if the Port filter type is selected.
Priority	Select the priority of the filter from the drop-down menu.

Table 5-4 Adding or Deleting Network 1 (eth0) QoS Settings

Adding or Deleting Network 1 (eth0) Settings	Description
Delete	Click the checkbox to the left of any existing QoS filter to be deleted and click the Submit button.
Filter type	Select the filter type from the drop-down window: <ul style="list-style-type: none"> ◆ Network ◆ Port
Network	Enter the Network, if the Network filter type is selected.
Ports	Enter the Port, if the Port filter type is selected.
Priority	Select the priority of the filter from the drop-down menu.
Submit	Click Submit after adding information for a new filter.

To Configure Network 1 QoS Settings

Using Web Manager

- ◆ To modify Ethernet 1 (eth0) QoS information, click **Network** on the menu and select **Network 1 > QoS > Configuration**.

Using the CLI

- ◆ To enter the eth0 QoS command level: `enable -> config -> if 1 -> qos`

Using XML

- ◆ Include in your file: `<configgroup name="qos" instance="eth0">`

Network 1 (eth0) Failover

The PremierWave EN embedded system on module provides network failover, in the form of a "dead remote host reachability" mechanism (essentially a ping against a known host). If the remote host is determined to be not reachable, the device will failover to the Wi-Fi interface. If the remote host is determined to be reachable, the device will failback to the Ethernet interface.

Table 5-5 Network 1 (eth0) Failover Settings

Network 1 (Failover) Settings	Description
State	Click to enable or disable state.
Failover Interface	Always select wlan0 in the PremierWave EN embedded system on module.
Hostname	Enter the remote host to test reachability.
Method	Select ICMP or TCP based ping.
Timeout	Indicate the interval to wait for ping response from remote host.
Interval	Indicate the interval in which to test reachability
Failover Threshold	Indicate the allowed number of failed pings – after which the device will failover to the interface.
Failback Threshold	Indicate the number of successful pings – after which the device will failback to the Ethernet interface.

To Configure Network 1 Failover Settings

Using Web Manager

- ◆ To modify Failover settings, click **Network** on the menu and select **Network 1 > Failover > Configuration**.

Using the CLI

- ◆ To enter the eth0 link command level: `enable -> config -> if 1 -> failover`

Using XML

- ◆ Include in your file: `<configgroup name="network failover" instance="eth0">`

Network 2 Status

In the Network 2 status pages, you can view both the current interface operational settings as well as the settings that would take effect upon a device reboot, as well as Link, QoS and Failover status information.

- ◆ To view Ethernet (wlan0) Interface status, click **Network** on the menu and select **Network 2 -> Interface -> Status**.
- ◆ To view Ethernet (wlan0) Link status, click **Network** on the menu and select **Network 2 -> Link -> Status**.

- ◆ To view Ethernet (wlan0) QoS status, click **Network** on the menu and select **Network 2 -> QoS -> Status**.
- ◆ To view Ethernet (wlan0) Failover status, click **Network** on the menu and select **Network 2 -> Failover -> Status**.

Network 2 (wlan0) Interface Settings

This page is used to view the status of the wlan0 interface on the device.

Note: *Statistics are as measured by the device since bootup. Your service provider may account for data usage differently.*

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

Table 5-6 Network 2 (wlan0) Interface Settings

Network 2 (wlan0) Interface Settings	Description
State	Select to enable or disable the interface.
IPv4 State	Select to enable or disable the IPv4 state.
BOOTP Client	Select to turn on or off the BOOTP client.
DHCP Client	Select to turn on or off the DHCP client.
Priority	It ranges from 0-10. Note: <i>Lower priority number means higher preference.</i>
IP Address	Enter the IP address alone, in CIDR form, or with an explicit mask.
Default Gateway	Enter the default gateway.
Hostname	Enter the host name, beginning with a letter, continue with a letter, number or hyphen and end with a letter or a number.
Domain	Enter the domain for the interface.
DHCP Client ID	Enter the DHCP client ID.
Primary DNS	Enter the IP address of the primary Domain Name Server. Note: <i>This setting will be used when either Static IP or Auto IP is active, or if DHCP/BOOTP is active and no DNS server was acquired from the server.</i>
Secondary DNS	Enter the IP address of the secondary Domain Name Server. Note: <i>This setting will be used when either Static IP or Auto IP is active, or if DHCP/BOOTP is active and no DNS server was acquired from the server.</i>
MTU	Enter the maximum transmission unit (MTU) associated with the interface.
IPv6 State	Select to enable or disable the IPv4 state.
IPv6 DHCP Client	Select to turn On or Off . ◆ On: will provide an additional IPv6 address in addition to the displayed Link Local IPv6 address and DHCPv6 IPv6 address. This is the auto configuration address provided by the IPv6 router. ◆ Off: will not display auto configured IPv6 address in CLI or WebUI.

Network 2 (wlan0) Interface Settings	Description
IPv6 Address	Enter the static IPv6 address to use for the interface. <i>Note: This setting is used if Static IPv6 is active (DHCPv6 is Disabled). Changing this value requires a reboot. When DHCPv6 is enabled, the XPort Pro Lx6 tries to obtain an IPv6 address from a DHCPv6 server. If it cannot, then XPort Pro Lx6 generates and uses a Link local IPv6 address.</i>
IPv6 Default Gateway	Enter the default IPv6 Default Gateway.
IPv6 Domain	Enter the IPv6 domain name suffix for the interface. <i>Note: This setting will be used when Static IP is active, or if IPv6 DHCP client is active and no Domain Suffix was acquired from the server.</i>
IPv6 Primary DNS	Enter the IPv6 address of the primary Domain Name Server. <i>Note: This setting will be used when Static IP is active, or if IPv6 DHCP client is active and no Domain Suffix was acquired from the server.</i>
IPv6 Secondary DNS	Enter the IPv6 address of the secondary Domain Name Server. <i>Note: This setting will be used when Static IP is active, or if IPv6 DHCP client is active and no Domain Suffix was acquired from the server.</i>

To Configure Network 2 Interface Settings

Using Web Manager

- ◆ To modify network 2 wlan0 interface information, click **Network** on the menu and select **Network 2 > Interface > Configuration**.

Using the CLI

- ◆ To enter the wlan0 command level: `enable -> config -> if 2`

Using XML

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

SmartRoam

The SmartRoam utility monitors the signal strengths of all in-range access points belonging to the Extended Service Set (ESS) to which the PremierWave EN is currently connected. When an AP is found with a signal strength which is significantly greater than that of the currently associated AP, the SmartRoam utility automatically switches to the new AP. This reduces interruptions in wireless connectivity and ensures optimal signal strength. Roaming happens automatically and is completely transparent to the user; no loss of network connectivity should occur.

The SmartRoam utility periodically scans for access points which belong to the current ESS (having the same SSID and security settings at the currently associated AP.) The results are then searched for an AP with a 'stronger' signal (higher RSSI) than the current AP. If the search is successful, SmartRoam triggers a disconnection from the current AP and a connection to the one selected from the scan results.

Since moving between access points is a time-consuming process which can negatively impact throughput, SmartRoam employs a delta value to ensure that the move only occurs if there would

be a significant gain in signal strength. When searching the results of a scan, SmartRoam only considers the APs with RSSI exceeding that of currently associated AP by at least the delta value.

Note: RSSI is reported in two different ways. When displayed in scan results the RSSI is an instantaneous value obtained from a single beacon/probe response, and therefore may vary across scan results. When reported in the status of the current connection (for the associated access point) the value is averaged over time and is less prone to fluctuation.

Network 2 (wlan0) Link Settings

This page shows configuration of an wlan0 link on the device.

Table 5-7 Network 2 (wlan0) Link Settings

Network 2 Link Settings	Description
Choice 1 Profile Choice 2 Profile Choice 3 Profile Choice 4 Profile	<ul style="list-style-type: none"> Select up to four (4) WLAN Profiles for automatic connection to wireless networks. More information on wireless settings is available in the section, To Configure Network 2 Link Settings on page 38. Enter the name of the WLAN Profile desired for each choice.
Out of Range Scan Interval	Set the amount of time in seconds, between SmartRoaming scans.
Roaming	Click to Enable or Disable SmartRoaming.
RSSI Delta	The minimum difference (in dBm) between the current RSSI and the RSSI of any access point in the scan results before it will be considered as a roaming candidate. The configured value will actually be used for the high-power delta. The roaming delta is cut in half for RSSI below -50 dBm. The value for the low-power delta will be derived from the configured one by dividing it by two. Default value: 24 dBm, range: 14 - 24 dBm.
Debugging Level	Set the verbosity level for printing WLAN Link messages to the TLOG (Default is Info).
Active Channel Scan Time	Set the amount of time, in milliseconds, the radio will dwell on each individual channel when performing an active scan. During active scanning, the radio transmits probe requests and gathers probe responses from other devices. The range of values is 50 to 150 msec.
Passive Channel Scan Time	Set the amount of time, in milliseconds, the radio will dwell on each individual channel when performing a passive scan. During passive scanning the radio does not transmit probe requests, instead relying on beacons sent by other devices. The range of values is 100 to 400 msec.
Radio Band Selection	Select the band(s) on which the radio will operate. Options are 2.4 GHz only, 5 GHz only or Dual band.
WLAN Watchdog	Select to enable or disable.

To Configure Network 2 Link Settings

Using Web Manager

- To modify network 2 wlan0 interface information, click **Network** on the menu and select **Network 2 > Link > Configuration**.

Using the CLI

- ◆ To enter the link command level: `enable -> if 2 -> link`

Using XML

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

Network 2 (wlan0) QoS

QoS (Quality of Service) can be enabled and configured for both Network 1 (eth0) and Network 2 (wlan0). If enabled, the router will control the flow of outbound traffic according to the user-defined filters. In other words, QoS improves performance by allowing the user to prioritize applications. Filters can be defined to prioritize traffic based on the source or destination network, source or destination port, or the source MAC address. Up to 32 user-defined filters can be added. The following are predefined priority classes:

- ◆ Network Control and Internetwork Control are typically used for network control packets such as ICMP and have the highest priorities.
- ◆ Bandwidth allocation is a minimum 5% each.
- ◆ Voice: Bandwidth allocation is minimum 30%.
- ◆ Video: Bandwidth allocation is minimum 20%.
- ◆ Critical Applications: Bandwidth allocation is minimum 15%.
- ◆ Excellent Effort: Bandwidth allocation is minimum 10%.
- ◆ Best Effort: Bandwidth allocation is minimum 10%.
- ◆ Background: Bandwidth allocation is minimum 5% and has the lowest priority.

[Table 5-8](#) shows the network QoS settings that can be configured including adding new filters.

Table 5-8 Network 2 (wlan0) QoS Settings

Network 2 (QoS) Settings	Description
State	Click to enable or disable state.
Import filters	Click to enable or disable import filters to import configurations from other interfaces.
Uplink Speed	Enter the maximum uplink speed. Set 0 to set speed to default.

Table 5-9 Adding or Deleting Network 2 (wlan0) QoS Settings

Adding or Deleting Network 2 (QoS) Settings	Description
Delete	Click the checkbox to the left of any existing QoS filter to be deleted and click the Submit button.
Filter type	Select the filter type from the drop-down window: <ul style="list-style-type: none"> ◆ Mac Address ◆ Network ◆ Port

Adding or Deleting Network 2 (QoS) Settings	Description
MAC Address	Enter the MAC address, if the MAC Address filter type is selected.
Network	Enter the Network, if the Network filter type is selected.
Ports	Enter the Port, if the Port filter type is selected.
Priority	Select the priority of the filter from the drop-down menu.

To Configure Network 2 QoS Settings

Using Web Manager

- ◆ To modify Ethernet (eth0) QoS information, click **Network** on the menu and select **Network 2 > QoS > Configuration**.

Using the CLI

- ◆ To enter the eth0 QoS command level: `enable -> config -> if 2 -> qos`

Using XML

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

WLAN Link Status and Scan Commands

These commands display information about the current state of the wireless network.

Table 5-10 Network 2 Link Scan

WLAN Link Information Commands	Description
Scan "<network SSID>"	Perform a scan for devices within range of the PremierWave device server. 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. <i>Note: When omitting the network SSID it is still necessary to include the opening and closing quotation marks (scan ""). When the PremierWave unit is associated with an access point, scanning is only performed on the band on which the unit is connected.</i>
Refresh scan results every 60 seconds (checkbox)	<ul style="list-style-type: none"> ◆ Check this to auto update the list of networks every 60 seconds. ◆ Uncheck this to stop auto update.

The results of the **scan** command are presented in the following format in the table below:

Table 5-11 Network 2 Link Scan Results on Web Manager

WLAN Link Scan Results Field	Description
Network Name	The Service Set Identifier (network name) of the device.

WLAN Link Scan Results Field (continued)	Description
SSID	Service Set Identifier (network name) of the device. Clicking a specific SSID brings you to the specific WLAN profile of the device selected. See WLAN Profiles (on page 43) for more information.
BSSID	Basic Service Set Identifier. AdHoc mode is limited to four connections.
Ch (Channel)	The channel on which the device is operating.
RSSI	The instantaneous Received Signal Strength Indicator (RSSI) of the device measured in dBm. <i>Note: RSSI reported in scan results is a single sampling, while the RSSI reported in the 'status' command (showing the signal strength of the currently connected AP) is averaged over time.</i>
Security Suite	Indicates the security suite in use by the device as well as whether it is operating in Adhoc (IBSS) mode.

The results of the **status** command are presented in the following format:

Table 5-12 Network 2 Link Status

WLAN Link Status	Description
Connection State	Indicates the connection state.
BSSID	A unique identifier for the Basic Service Set corresponding to the MAC address of the Access Point in infrastructure mode, or a generated value in Adhoc mode. AdHoc mode is limited to four connections.
SSID	The Service Set Identifier of the connected network.
Topology	The type of wireless network in use for the current association (Adhoc or Infrastructure).
Active WLAN Profile	Indicates which WLAN profile created the current connection to the wireless network.
Pairwise Cipher	The standard used to encrypt a particular type of data in the current wireless association.
Group Cipher	The standard used to encrypt a particular type of data in the current wireless association.
Authentication	Indicates the method of distributing encryption key material.
Security Suite	Indicates the security suite used for the current association.
Channel	The channel used for the current association.
IP Address	The IP address assigned to the PremierWave device.
RSSI	A measure of the power level of the received radio signal in dBm, specifically the RSSI of the currently associated AP averaged over time. <i>Note: RSSI reported in scan results is a single sampling, while the RSSI reported in the 'status' command (showing the signal strength of the currently connected AP) is averaged over time.</i>
WPS Mode	Indicates whether WPS is activated.
Frequency	Frequency (in MHz) on which the current connection is operating.

WLAN Link Status (continued)	Description
IPv6 Link-local Address	Indicates the IPv6 link-local address.
IPv6 Global Address	Indicates the IPv6 global address.
IPv6 Global Address	Indicates the IPv6 global address.

To View WLAN Link Scan and Status Information

Using Web Manager

- ◆ To scan the wireless (wlan0) Link, click **Network** in the menu and select **Network 2 -> Link -> Scan**.
- ◆ To view the wireless (wlan0) Link status information, click **Network** in the menu and select **Network 2 -> Link -> Status**.

Using the CLI

- ◆ To enter the wlan0 Link command level: `enable -> config -> if 2 -> link`

Using XML

- ◆ Include in your file:


```
<statusgroup name=" status">
and
<statusgroup name=" scan">
```

Network 2 (wlan0) Failover

The PremierWave EN embedded system on module provides wlan0 failover, in the form of a "dead remote host reachability" mechanism (essentially a ping against a known host). If the remote host is determined to be not reachable, the device will failover to the Ethernet interface. If the remote host is determined to be reachable, the device will failback to the Wi-Fi interface.

Table 5-13 Network 2 (wlan0) Failover Settings

Network 1 (Failover) Settings	Description
State	Click to enable or disable state.
Failover Interface	Always select eth0 in the PremierWave EN embedded system on module.
Hostname	Enter the remote host to test reachability.
Method	Select ICMP or TCP based ping.
Timeout	Indicate the interval to wait for ping response from remote host.
Interval	Indicate the interval in which to test reachability
Failover Threshold	Indicate the allowed number of failed pings – after which the device will failover to the interface.

Network 1 (Failover) Settings	Description
Failback Threshold	Indicate the number of successful pings – after which the device will failback to the Ethernet interface.

To Configure Network 2 Failover Settings

Using Web Manager

- ◆ To modify Failover settings, click **Network** on the menu and select **Network 2 > Failover > Configuration**.

Using the CLI

- ◆ To enter the wlan0 link command level: `enable -> config -> if 2 -> failover`

Using XML

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

WLAN Profiles

A WLAN profile defines all of the settings necessary to establish a wireless connection with either an access point (in infrastructure mode) or another wireless client (in Adhoc mode, limited to four connections.) A maximum of eight profiles can exist on the PremierWave EN system on module at a time. All enabled profiles are active.

The PremierWave unit now supports dynamic profiles and prioritization of the profiles. Dynamic Profiles are the ones created via WPS or QuickConnect. Profiles are numbered based on priority. Dynamic profiles (in reversed order of creation), choice list profiles (Choice1, Choice2, Choice3, and Choice4), and then the remaining profiles. Use the number from output of 'show' command.

To Configure WLAN Profiles

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

Using WebManager

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

Using the CLI

- ◆ To enter the wlan0 Profile command level: `enable -> config -> wlan profiles`

Using XML

- ◆ Include in your file: `<configgroup name="wlan profile" instance="profile_name">`

Table 5-14 Creating, Deleting or Enabling WLAN Profiles

WLAN Profile Basic Settings	Description
Delete (checkbox)	Click the Delete checkbox beside the profile(s) to be deleted. Three buttons will appear: <ul style="list-style-type: none"> ◆ Click the Submit button to permanently delete profile(s). ◆ Click the Apply button to delete the profile for testing purposes. If the device reboots, this change will not be applied. ◆ Click the Cancel button to cancel this action, as desired.
Enabled (checkbox)	Click the Enabled checkbox beside the profile(s) to be enabled. Three buttons will appear: <ul style="list-style-type: none"> ◆ Click the Submit button to permanently enable profile(s). ◆ Click the Apply button to enable the profile for testing purposes. If the device reboots, this change will not be applied. ◆ Click the Cancel button to cancel this action, as desired.
View or Edit (link to specific profile)	Click on a specific WLAN Profile name to edit the WLAN profile basic settings (see Table 5-15).
Create new profile	Type in the name of the new profile to be created into the Create new profile field. Then, click the Submit button which appears to create the profile. Once created, the profile name may be clicked so you may edit profile settings (see Table 5-15).

Table 5-15 WLAN Profile Basic Settings

WLAN Profile Basic Settings	Description
Network Name (SSID)	Specify the name of the wireless network (SSID.) Warning: <i>Creating a new profile with a pre-existing network name will cause the original network name and associated profile to be overwritten.</i>
State	Select to Enable or Disable .
Topology	Specify Infrastructure (ESS) or Adhoc (IBSS) mode. <ul style="list-style-type: none"> ◆ Infrastructure: mode that communicates with access points. ◆ Adhoc: mode that communicates with other clients, limited to four connections.
Channel	Specify the channel for an Adhoc network. Note: <i>This setting only applies to the creation of an Adhoc network.</i>
Radio Mode	Select the radio mode for the WLAN profile.
Scan DFS Channels	Select to Enable or Disable scanning on the DFS (Dynamic Frequency Selection) channels in the 5 GHz band. Note: <i>This setting only applies if scanning in the 5 GHz band is enabled.</i>

To Configure WLAN Profile Basic Settings

Using Web Manager

- ◆ To view or edit an existing WLAN profile or to create a new profile, click **WLAN Profiles** on the menu and select an existing profile.

Using the CLI

- ◆ To enter the wlan0 Profile command level:
enable -> config -> wlan profiles -> edit <profile number>
or
enable -> config -> wlan profiles -> edit <profile name>

Using XML

- ◆ Include in your file:
<configgroup name="wlan profile" instance="profile name">
and
<configitem name="basic">

Table 5-16 WLAN Profile Advanced Settings

WLAN Profile Advanced Settings	Description
TX Data Rate Maximum	Specify the rate for data transmission. <i>Note: This setting only applies if 'TX Data Rate' is set to 'Fixed'.</i>
TX Data Rate	Specify the type of transmission data rate: ◆ Fixed = keeps the transmission rate at the configured value. ◆ Auto-reduction = allows the PremierWave EN system on module to reduce the data rate automatically, depending on link quality.
TX Power Maximum	Specify the maximum transmission output power in dBm.
Antenna Diversity	Select the antenna the radio will use or allow PremierWave EN unit to automatically make the selection. ◆ Enabled = allows the PremierWave EN unit to select the antenna. ◆ Antenna 1 = use the internal antenna. ◆ Antenna 2 = use the external antenna.
Max Missed Beacons	Enter the maximum number of missed beacons allowed.
Power Management	Select to Enable or Disable power management, which reduces the overall power consumption of the PremierWave EN system on module, but can increase latency. ◆ Enabled = allows the PremierWave EN unit to turn off the receiver when it is idling. ◆ Disabled = keeps the receiver on at all times.
Power Management Interval	Select number of beacons (100 msec interval) between 1 and 10. The above-mentioned latency can be up to this number "X" 100 msec. This field becomes available when power management is enabled.

To Configure WLAN Profile Advanced Settings

Using Web Manager

- ◆ To view or edit an existing WLAN Profile, click **WLAN Profiles** on the menu and select an existing profile.

Using the CLI

- ◆ To enter the wlan0 profile advanced command level: `enable -> config -> wlan profiles -> edit <profile name or number> -> advanced`

Using XML

- ◆ Include in your file:

```
<configgroup name="wlan profile" instance="profile name">
and
<configitem name="security">
```

WLAN Profile Security Settings

The PremierWave EN system on module supports WEP, WPA, and WPA2/IEEE 802.11i to secure all wireless communication. WPA and WPA2/IEEE 802.11i are not available for Adhoc topology.

The WPA2/IEEE 802.11i mode is compliant with the Robust Secure Network specified in the IEEE standard 802.11i.

Table 5-17 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"> ◆ None = no authentication or encryption method will be used. ◆ WEP = Wired Equivalent Privacy ◆ WPA = Wi-Fi Protected Access ◆ WPA2 /IEEE 802.11i = Robust Secure Network.
Authentication	Select the authentication of the security key when the WPA or the WPA2/IEEE802.11i suite is selected above. <ul style="list-style-type: none"> ◆ PSK ◆ IEEE 802.1X <p>- OR -</p> Select the authentication of the security key when the WEP suite is selected above. <ul style="list-style-type: none"> ◆ Open ◆ Shared
Key Type	Select the desired key type. <p>Note: This configuration option becomes available only when suites, WEP, WPA or WPA2/IEEE 802.11i are selected.</p>
Key Size	Select the key size: <ul style="list-style-type: none"> ◆ 40 bits ◆ 104 bits <p>Note: This configuration option becomes available only when the WEP suite is selected.</p>
Key	Enter the key. <p>Note: This configuration option becomes available only when the WPA or the WPA2/IEEE 802.11i suite and the Hex key type is selected.</p>

WLAN Profile Security Settings	Description
Passphrase	<p>Select the passphrase consists of up to 63 characters.</p> <p>Note: This configuration option becomes available only when suites, WEP, WPA or WPA2/IEEE 802.11i are selected.</p> <p>Note: Lantronix recommends using a passphrase of 20 characters or more for maximum security. Spaces and punctuation characters are permitted.</p> <p>Note: 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.</p>
TX Key Index	<p>Select TX Key Index from the drop-down menu.</p> <p>Note: This option is available when the WEP suite and Hex key type is selected above.</p>
Key 1 - 4	<p>Enter key information in the appropriate Key number field(s).</p> <p>Note: These options are available when the WEP suite and Hex key type is selected above.</p>
Encryption	<p>Select the encryption for the key:</p> <ul style="list-style-type: none"> ◆ CCMP ◆ TKIP ◆ WEP <p>Note: This configuration option becomes available only when suites WPA or WPA2/IEEE 802.11i are selected.</p>

To Configure WLAN Profile Security Settings

Using Web Manager

- ◆ To view or edit an existing WLAN Profile, click **WLAN Profiles** on the menu and select an existing profile.

Using the CLI

- ◆ To enter the wlan0 Profile Advanced Security Command level: `enable -> config -> wlan profiles -> edit 1 -> advanced -> security`

Using XML

- ◆ Include in your file:


```
<configgroup name="wlan profile" instance="profile name">
and
<configitem name="security">
```

WLAN Profile WEP Settings

WEP security is available in both **Infrastructure** and **AdHoc** modes. WEP is a simple and efficient security mode encrypting the data via the RC4 algorithm. However, WEP has become more vulnerable due to advances in hacking technology. State of the art equipment can find WEP keys in five minutes. For stronger security, please use WPA, or better, WPA2 with AES (CCMP).

Table 5-18 Additional WEP Settings for WLAN Profile.

WLAN Profile WEP Settings	Description
Suite	Specify the security suite to be used for this profile. <ul style="list-style-type: none"> ◆ None = no authentication or encryption method will be used. ◆ WEP = Wired Equivalent Privacy ◆ WPA = WiFi Protected Access ◆ WPA2 /IEEE 802.11i = Robust Secure Network.
Authentication	Select one of the following options: <ul style="list-style-type: none"> ◆ Shared = encryption keys of both parties are compared as a form of authentication. If mismatched, no connection is established. ◆ Open = a connection is established without first checking for matching encryption keys. However, mismatched keys will result in garbled data and thus a lack of connectivity on the IP level.
Key Type	Select the format of the security key. <ul style="list-style-type: none"> ◆ Passphrase ◆ Hex <p><i>Note:</i> This configuration option becomes available only when suites, WEP, WPA or WPA2/IEEE 802.11i are selected.</p>
Key Size	Select the key size in bits. Select 40 for WEP40 and WEP64; select 104 for WEP104 and WEP128.
TX Key Index	Select one of four index listing keys for transmitting data. Reception is allowed with all four keys. <p><i>Note:</i> For interoperability with some products that generate four identical keys from a passphrase, this index must be one. This field appears when the WEP suite type and the Hex key type are selected.</p>
Keys 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. This field appears when the WEP suite type and the Hex key type are selected.
Passphrase	Select the passphrase consists of up to 63 characters. <p><i>Note:</i> This configuration option becomes available only when suites, WEP, WPA or WPA2/IEEE 802.11i are selected.</p> <p><i>Note:</i> Lantronix recommends using a passphrase of 20 characters or more for maximum security. Spaces and punctuation characters are permitted.</p> <p><i>Note:</i> 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.</p>

To Configure WLAN Profile WEP Settings

Using Web Manager

- ◆ To view or edit an existing WLAN Profile WEP setting, click **WLAN Profiles** on the menu, select an existing profile and select **WEP** for the suite.

Using the CLI

- ◆ To enter the wlan0 Profile WEP command level: enable -> config -> wlan profiles -> edit <profile name or number> -> advanced -> security -> wep

Using XML

- ◆ Include in your file:

```
<configgroup name="wlan profile" instance="profile name">
```

and

```
<configitem name="security">
```

WLAN Profile WPA and WPA2/IEEE802.11i Settings

WPA and WPA2/IEEE802.11i security suites are available for **Infrastructure** mode only.

WPA is a security standard specified by Wi-Fi Alliance and is a close derivative of an early draft of the IEEE802.11i specification. WEP was becoming vulnerable and finalizing the IEEE802.11i standard was still far away. WPA2 is Wi-Fi's subset of the broad IEEE802.11i standard to enforce better interoperability. The PremierWave EN system on module is compliant with both WPA2 and IEEE802.11i.

Table 5-19 WLAN Profile WPA and WPA2/IEEE802.11i Settings

WLAN Profile WPA & WPA2 Settings	Description
Suite	Specify the security suite to be used for this profile. <ul style="list-style-type: none"> ◆ None = no authentication or encryption method will be used. ◆ WEP = Wired Equivalent Privacy ◆ WPA = WiFi Protected Access ◆ WPA2 /IEEE 802.11i = Robust Secure Network.
Authentication	Select the authentication method to be used. <ul style="list-style-type: none"> ◆ PSK = Pre-Shared Key. The same key needs to be configured on both sides of the connection. (On the PremierWave unit and on the Access Point.) ◆ IEEE 802.1X = This authentication method communicates with a RADIUS authentication server that is part of the network. The RADIUS server will match the credentials sent by the PremierWave unit with an internal database.
Key Type	If PSK authentication is selected, select the Hex key type.
Key Type	Select the format of the security key. <p>Note: This configuration option becomes available only when suites, WEP, WPA or WPA2/IEEE 802.11i are selected.</p>
Key	Enter 64 hexadecimal digits (32 bytes), if PSK authentication and Hex key type are selected.

WLAN Profile WPA & WPA2 Settings (continued)	Description
IEEE 802.1X	<p>Select the protocol to use to authenticate the WLAN client.</p> <ul style="list-style-type: none"> ◆ LEAP = Lightweight Extensible Authentication Protocol. A derivative of the original Cisco LEAP, which was a predecessor of 802.1X. Real Cisco LEAP uses a special MAC layer authentication (called Network EAP) and cannot work with WPA/WPA2. The PremierWave uses a more generic version to be compatible with other major brand Wi-Fi equipment. The authentication back end is the same. ◆ EAP-TLS = Extensible Authentication Protocol - Transport Layer Security. Uses the latest incarnation of the Secure Sockets Layer (SSL) standard and is the most secure because it requires authentication certificates on both the network side and the PremierWave side. ◆ EAP-TTLS = Extensible Authentication Protocol - Tunneled Transport Layer Security. ◆ PEAP = Protected Extensible Authentication Protocol. ◆ EAP-TTLS and PEAP have been developed to avoid the requirement of certificates on the client side (PremierWave unit), which makes deployment more cumbersome. Both make use of EAP-TLS to authenticate the server (network) side and establish an encrypted tunnel. This is called the outer-authentication. Then a conventional authentication method (MD5, MSCHAP, etc.) is used through the tunnel to authenticate the PremierWave device. This is called inner authentication. EAP-TTLS and PEAP have been developed by different consortia and vary in details, of which the most visible is the supported list of inner authentications. <p><i>Note: When using EAP-TLS, EAP-TTLS or PEAP authority, at least one authority certificate will have to be installed in the SSL configuration that is able to verify the RADIUS server's certificate. In case of EAP-TLS, also a certificate and matching private key need to be configured to authenticate the PremierWave EN device to the RADIUS server. For more information about SSL certificates see TLS (SSL) on page 129. The IEEE 802.1X options will be available only if the IEEE 802.1X authentication is selected.</i></p>
EAP-TTLS Option	<p>Select the inner authentication method to be used with EAP-TTLS, if the EAP-TTLS IEEE 802.1X is selected.</p> <ul style="list-style-type: none"> ◆ EAP-MSCHAPV2 ◆ MSCHAPV2 ◆ MSCHAP ◆ CHAP ◆ PAP ◆ EAP-MD5
PEAP Option	<p>Select the inner authentication method to be used with EAP-PEAP, if the PEAP IEEE 802.1X is selected.</p> <ul style="list-style-type: none"> ◆ EAP-MSCHAPV2 ◆ EAP-MD5
Username	User ID for identifying the PremierWave unit to the RADIUS server in the network
Password	Select the password for identifying the PremierWave to the RADIUS server in the network.
Validate Certificate	Select to Enable or Disable , if the EAP-TLS IEEE 802.1X is selected. If enabled, the PremierWave unit will attempt to validate the certificate received from the RADIUS server.

WLAN Profile WPA & WPA2 Settings (continued)	Description
Encryption	<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"> ◆ CCMP = Uses AES as basis and is the strongest encryption option. ◆ TKIP = Uses WEP as the basis, but adds extra checks and variations for added protection. ◆ WEP = Based on RC4. <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.</i></p>
Credentials	<p>Indicate the name of client certificate (required for EAP-TLS.) For more information about SSL certificates see sections, TLS (SSL) on page 129.</p>

To Configure WLAN Profile WPA and WPA/IEEE802.11i Settings

Using Web Manager

- ◆ To view or edit an existing WLAN Profile WPA setting, click **WLAN Profiles** on the menu, select an existing infrastructure profile and select **WPA** or **WPA2/IEEE802.11i** for the suite.

Using the CLI

- ◆ To enter the wlan0 Profile WPAX command level: `enable -> config -> wlan profiles -> edit <profile name or number> -> advanced -> security -> wpax` or `enable -> config -> wlan profiles -> edit <profile name or number> -> security -> wpax`

Using XML

- ◆ Include in your file:


```
<configgroup name="wlan profile" instance="profile name">
and
<configitem name="security">
```

WLAN Quick Connect

WLAN QuickConnect allows users to add a WLAN profile from a list of available networks auto-refreshed every 15 seconds. Details of the selected network are pre-populated, so little or no configuration is required by the user. Users can test the network connection before adding it to the pool of WLAN profiles.

Table 5-20 WLAN Quick Connect

WLAN Quick Connect Settings	Description
Network Name (search field)	Enter a network name and click Scan to search for a network.

WLAN Quick Connect Settings	Description
Scan “<network SSID>”	Perform a scan for devices within range of the PremierWave . 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. <i>Note:</i> When the PremierWave unit is associated with an access point, scanning is only performed on the band on which the unit is connected.
Refresh scan results every 60 seconds (checkbox)	<ul style="list-style-type: none"> ◆ Check this to auto update the list of networks every 15 seconds. ◆ Uncheck this to stop auto update.
SSID (link)	Network ID of a network. Click this link to display its configuration profile.
BSSID	Basic service set identifier. This is a unique 48-bits address that identifies the access point that creates the wireless network. AdHoc mode is limited to four connections.
CH	Channel number and frequency (MHz) of a network.
RSSI	An instantaneous value indicating the signal strength of the network. The best to worst signal strength is indicated by green, yellow and red respectively. <i>Note:</i> RSSI reported in scan results is a single sampling, while the RSSI reported in the 'status' command (showing the signal strength of the currently connected AP) is averaged over time.
Security Suite	Security suite of a network (e.g., WEP, WPA, WPA2, WPS, IBSS). <i>Note:</i> Although they are reported with the security flags, WPS and IBSS are not security settings. WPS indicates that an AP supports WPS and IBSS indicates a device operating in adhoc mode.

To Configure WLAN Quick Connect

Using Web Manager

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

Gateway

The PremierWave XEN intelligent gateway embedded system on module can be configured as a wireless router with DHCP server functionality.

Status

This page displays the current configuration and statistics information for the gateway.

- ◆ To view gateway status: click **Gateway** on the menu and select **Status**.

WAN

Table 5-21 WAN Configuration

Gateway Settings	Description
Operating Mode	Select the type of operating mode: <ul style="list-style-type: none"> ◆ Disabled: prevents the device to be used as a gateway; use the device normally. ◆ Gateway: allows the device to be used as a router with NAT. ◆ Router: allows the device to be used as a router without NAT.
Firewall	Select to enable or disable firewall: <ul style="list-style-type: none"> ◆ Enabled: enables the device firewall. ◆ Disabled: disable the device firewall.
MAC Address filter	Select to enable or disable the MAC address filter.
Interface	Specify the WAN interface. Generally wlan0 interface.
IP Address	Assign a static IP address to the gateway.
IPv6 Address	Assign a static IPv6 address to the gateway.
Primary DNS	Enter the IP address of the primary Domain Name Server. <i>Note: This setting will be used when either Static IP or Auto IP is active, or if DHCP/BOOTP is active and no DNS server was acquired from the server.</i>
Secondary DNS	Enter the IP address of the secondary Domain Name Server. <i>Note: This setting will be used when either Static IP or Auto IP is active, or if DHCP/BOOTP is active and no DNS server was acquired from the server.</i>

WAN MAC Address Filters

Accept or drop traffic from specified MAC addresses using the settings below.

Table 5-22 Adding a New MAC Address Filters

Adding or Deleting New MAC Address Filter Settings	Description
Delete	Click the checkbox to the left of any existing mac address filter to be deleted and click the Submit button.
MAC Address	Enter a new mac address to add a new filter.
Action	Select to ACCEPT or DROP above indicated MAC Address field.
Add	Click Add after adding new MAC address filter information.

To Configure Gateway WAN Settings

Using Web Manager

- ◆ To modify gateway WAN information, click **Gateway** on the menu and select **Configuration > WAN**.

Using the CLI

- ◆ To enter the gateway command level: `enable -> config -> gateway`

Using XML

- ◆ Include in your file: `<configgroup name="gateway"> <configitem name="wan">`

Port Forwarding

Port forwarding allows remote computers (for example, computers on the Internet) to connect to a specific computer or service within a private local-area network (LAN). Port Forwarding rules apply to inbound traffic and will not work if the device is not reachable or traffic to certain ports is blocked before it reaches the device.

If traffic is going through firewalls, all referenced ports on the gateway and LAN devices must be accessible.

Table 5-23 Port Forwarding Rules List

Port Forwarding Rule	Description
Enabled	Enables the port forwarding rule.
Delete	Deletes the port forwarding rule.
Name	User friendly name for the rule. Click on the [Edit] icon to make changes.
Ingress IP Address: Port Range	Port or Port range for the rule.
Protocol	Protocols for the rule: TCP, UDP, or Both.
IP Address: Target Port	Target for the port forwarding rule.

Table 5-24 Adding a New Port Forwarding Rule

Adding New Port Forwarding Rule Settings	Description
Name	Enter a user friendly name for the rule (optional).
Ingress IP Address (Optional)	Enter the destination address of the packets. This option can only be used with single ports and not with port range.
Start Port	Enter the starting port number
End Port	End port number (optional). If start port and end port are same it assumes a single port. If start port and end port are not the same – it is a port range.
Protocol	Select the protocol for the rule: TCP, UDP, or Both
IP Address	Enter the target for the port forwarding rule.
Target Port	Indicate the target port. This is the port which the packets are to be forwarded. This options can only be used with single ports andnot with port range. If this value is not specified. If this value is not specified, the packets are forwarded to same port or pot range. Optional field.
Add (button)	Click Add after adding new new forwarding rule information.

To Configure Gateway Port Forwarding Settings

Using Web Manager

- ◆ To modify gateway port forwarding information, click **Gateway** on the menu and select **Configuration > Port Forwarding**.

Using the CLI

- ◆ To enter the gateway command level: enable -> config -> gateway -> port forwarding rule <number>

Using XML

- ◆ Include in your file: <configgroup name="gateway"> <configitem name="port forwarding" instance="<number>">

Static Routes

Allows the user to add routes to the device routing table.

Table 5-25 Static Route Setting Routes

Static Route Settings	Description
Enabled	Enables the static route.
Delete	Deletes the static route.
Name	User friendly name for the route. Click on the [Edit] icon to make changes.
Route	Network or Host for the route.
Applied	If the route was successfully applied. Routing table updates require a reboot and route needs to be valid as per other device configurable.

Table 5-26 Adding a New Static Route

Adding New Static Route Settings	Description
Name	Enter the user friendly name for the route.
Network	Enter the Network or Host for the route.
Gateway	Enter the Gateway for the route.
Interface	Select the Interface for the route.
Metric	Enter the priority for the route. Lower metric means higher priority.
Add	Click Add after adding new route information.

To Configure Gateway Static Route Settings

Using Web Manager

- ◆ To modify gateway static route information, click **Gateway** on the menu and select **Configuration > Static Routes**.

Using the CLI

- ◆ To enter the gateway command level: `enable -> config -> gateway -> static route <number>`

Using XML

- ◆ Include in your file: `<configgroup name = "gateway"> <configitem name="static routes" instance="<number>"`

DHCP Server

Allows the user to configure the device as a DHCP server.

Table 5-27 DHCP Settings

DHCP Settings	Description
Lease time	Enter the duration for which lease is initially assigned. Clients must renew after this duration.
State	Enable or Disable the DHCP server for the DHCP settings. <ul style="list-style-type: none"> ◆ Enabled: DHCP server is enabled. ◆ Disabled: DHCP server is disabled.
Start IP Address	View or edit the Start IP Address of address pool.
End IP Address	View or edit the End IP Address of address pool.
State	Enable or Disable the DHCP server for the DHCPv6 settings. <ul style="list-style-type: none"> ◆ Enabled: DHCP server is enabled. ◆ Disabled: DHCP server is disabled.
Start IPv6 Address	Start IPv6 Address of address pool.
End IPv6 Address	End IPv6 Address of address pool.

To Configure Gateway DHCP Server Settings

Using Web Manager

- ◆ To modify gateway DHCP server information, click **Gateway** on the menu and select **Configuration > DHCP Server**.

Using the CLI

- ◆ To enter the gateway command level: `enable -> config -> gateway -> dhcp server`

Using XML

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

Static Lease Listing

The device also provides the ability to pre-assign specific IP addresses to connected devices using static leases. This would ensure that the connected device (identified by the MAC address) always gets the same IP address even while using DHCP.

Table 5-28 Static Lease Listing

Static Lease List Settings	Description
Delete	Click checkbox beside existing static lease MAC Address/IP Address to delete, if available and if desired.
MAC Address	MAC Address of existing static leases are listed here.
IP Address	Static IP Address of existing static leases are listed here.
IPv6 Address	Static IPv6 Address of existing static leases are listed here.

Table 5-29 Add a Static Lease

Add a Static Lease Settings	Description
MAC Address	Enter the MAC Address of the static lease to be added.
IP Address	Enter static IP address of the static lease to be added.
IPv6 Address	Enter static IPv6 address of the static lease to be added.
Add	Click Add after adding new static lease information.

Routing Protocols

The PremierWave EN system on module allows the configuration of routing protocols. Routing protocols specify how routers communicate with each other, disseminating information that enables the selection of routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. Each router has a prior knowledge of networks directly attached to it. A routing protocol shares this information among immediate neighbors first, then through the network. This way, routers gain knowledge of the topology of the network. The PremierWave device supports RIP and OSPF protocols.

Table 5-30 Routing Protocol Settings

Routing Settings	Description
State (RIP)	Select to enable or disable the RIP state.
Version	Select how the RIP is to be configured. It can accept Version 1 , Version 2 , or Version 1 and 2 .
Update Interval	Indicate the number of seconds for the Update Interval. Send unsolicited Response message every Update Interval seconds containing the complete routing table to all neighboring RIP routers.
Timeout Interval	Indicate the number of seconds for the Timeout Interval. Upon expiration of the Timeout Interval, the routes are no longer valid, however, they are retained in the routing table for a short time so that neighbors can be notified that the route has been dropped.
GC Interval	Indicate the number of seconds for the GC Interval. Upon expiration of the GC Interval, the routes are finally removed from the routing table.
State (OSPF)	Select to enable or disable the OSPF state.
Hello Interval	Indicate the number of seconds for the Hello Interval. Hello packet will be sent every Hello Interval seconds.
Dead Interval	Indicate the number of seconds for the Dead Interval. Sets the time period for which hello packets must not have been seen before neighbors declare the router down.

To Configure Gateway Routing Protocol Settings

Using Web Manager

- ◆ To modify gateway protocol settings, click **Gateway** on the menu and select **Configuration > Routing Protocol**.

Using the CLI

- ◆ To enter the gateway command level: `enable -> config -> gateway -> routing protocols`

Using XML

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

Virtual IP

The PremierWave EN embedded system on module allows the configuration of Virtual IP addresses. Virtual IP is a means to map an externally visible IP address to LAN-side IP addresses. PremierWave units will support creating up to three virtual IP address mappings by creating loop back interfaces and publishing this information via the routing protocols.

Table 5-31 Virtual IP Settings

Virtual IP Settings	Description
Enabled (checkbox)	Uncheck the Enabled checkbox adjacent to a virtual IP address to enable it. Keep the checkbox checked to keep the virtual IP address enabled. A virtual IP address is enabled by default.
Delete (checkbox)	Check the Delete checkbox adjacent to a virtual IP address to be deleted, clicking the Submit button.
Name	The name of an existing virtual IP address.
IP Address	An existing virtual IP address to which the LAN IP address is to be mapped.
LAN IP Address	An existing LAN IP address to which the virtual IP address is to be mapped.

Table 5-32 Adding a Virtual IP

Virtual IP Settings	Description
Name	Enter a name of the virtual IP address.
IP Address	Enter the virtual IP address to which the LAN IP address is to be mapped.
LAN IP Address	Enter the LAN IP address to which the virtual IP address is to be mapped.
Add	Click Add after adding new virtual IP information.

To Configure Gateway Virtual IP

Using Web Manager

- ◆ To modify gateway DHCP server information, click **Gateway** on the menu and select **Configuration > Virtual IP**.

Using the CLI

- ◆ To enter the gateway command level: `enable -> config -> gateway`

Using XML

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

DDNS

The PremierWave EN embedded system on module displays and allows configuration of the DDNS.

Table 5-33 DDNS Configuration

DDNS Settings	Description
State	Select to enable or disable the DDNS state.
User Name	Enter a user name for the DDNS account.
Password	Enter a password for the DDNS account.
Host Name	Specify the host name to be used to update the DDNS.
Interval	Indicate the interval of minutes the IP address will be checked. The DDNS will be updated if the IP address has changed.
Update DDNS (button)	Click this button, to save updated configuration information to the Flash.

To Configure Gateway WAN Settings**Using Web Manager**

- ◆ To view or configure DDNS information, click **DDNS** in the menu.

Using the CLI

- ◆ To enter the gateway command level: `enable -> config -> ddns`

Using XML

- ◆ Not any.

VPN

The PremierWave EN embedded system on module provides the option to configure a virtual private network (VPN) to extend a private network across a public network. Data may be sent and received across a shared or public network as if directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.

Table 5-34 VPN Configuration

VPN Settings	Description
Show details (link)	Click the Show details link to view the vpn log in a separate web browser window.
CONFIGURATION	
Name	Enter the user-defined name of the VPN connection.
State	Select to enable or disable the VPN connection.
Connection Type	Select connection type: <ul style="list-style-type: none"> ◆ Host to Subnet - VPN tunnel for local and remote subnets are fixed. ◆ Host to Host - VPN tunnel for remote subnet area is dynamic and local subnet is fixed.
Authentication Mode	Select the authentication mode of the IPSec VPN: <ul style="list-style-type: none"> ◆ PSK - Pre-shared key is used when there is a single key common to both ends of the VPN. ◆ RSA - Uses RSA digital signatures. ◆ XAUTH - Provides an additional level of authentication by allowing the IPSec gateway to request extended authentication from remote users, thus forcing remote users to respond with their credentials before being allowed access to the VPN.
Mode Configuration	Click to enable or disable extended authentication operation and the settings provided to the client during the configuration exchange.
Type	Select the VPN type: <ul style="list-style-type: none"> ◆ Tunnel - Tunnel mode is used for protecting traffic between networks, when traffic must pass through intermediate, untrusted network. ◆ Transport - Transport mode is used for end-to-end communication (for example, for communications between a client and a server).
Interface	Select the interface to use to connect to VPN Gateway.
REMOTE NETWORK	
Endpoint	Enter the remote VPN gateway's IP address.
Subnet	Enter the subnet behind the VPN gateway.
ID	Specify the identifier through which to receive from the remote host during Phase 1 negotiation.
Router/Next Hop	Enter the next-hop gateway IP address for the VPN gateway.
LOCAL NETWORK	
Subnet	Define which local devices have access to or can be accessed from the VPN connection.
ID	Specify the identifier sent to the remote host during Phase 1 negotiation.
Router/Next Hop	Enter the next-hop gateway IP address for our connection to the public network.

VPN Settings	Description
KEY MANAGEMENT	
Perfect Forward Secrecy (PFS)	Select to enable or disable whether Perfect Forward Secrecy of keys is desired on the connection's keying channel. Enabling this feature will require IKE to generate a new set of keys in Phase 2 rather than using the same key generated in Phase 1.
Pre-shared key (PSK)	Enter the pre-shared key to be used in the IPSec setting between the Local and VPN Gateway.
ISAKMP PHASE 1 (IKE)	
Aggressive Mode	Select to enable or disable Aggressive Mode. In Aggressive mode, IKE tries to combine as much information into fewer packets while maintaining security. Aggressive mode is slightly faster but less secure.
NAT Traversal	Select to enable or disable NAT Traversal. If there is an external NAT device between VPN tunnels, the user must enable NAT Traversal.
Encryption	Select the encryption algorithm in key exchange.
Authentication	Select the hash algorithm in key exchange.
DH Group	Select the Diffie-Hellman group (the Key Exchange group between the Remote and VPN Gateways).
IKE Lifetime	Enter the lifetime, in hours, for IKE SA.
ISAKMP PHASE 2 (ESP)	
Encryption	Select the encryption Algorithm in data exchange.
Authentication	Select the hash Algorithm in data exchange.
DH Group	Select the Diffie-Hellman groups (the Key Exchange group between the Remote and VPN Gateways) for Phase 2.
SA Lifetime	Enter the lifetime, in hours, for SA in Phase 2.
Unreachable Host Detection	
Host	Enter the Host to use failover host and ping interval to monitor connectivity with a host on the remote network.
Ping Interval	Indicate the ping interval, in minutes, to use failover host and ping interval to monitor connectivity with a host on the remote network.
Max Tries	Enter the tries for the VPN tunnel is restarted if Max Tries pings to the host fail.

To Configure VPN Settings

Using Web Manager

- ◆ To view or configure VPN information, click **VPN** in the menu.

Using the CLI

- ◆ To enter the VPN command level: `enable -> config -> vpn`

Using XML

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

GRE Settings

GRE tunneling is available on the PremierWave embedded system on module, providing more capabilities than IP-in-IP tunneling. For example, it supports transporting multicast traffic and IPv6 through a GRE tunnel.

Table 5-35 GRE Settings

GRE Settings	Description
Name	Enter the user-defined name of the GRE tunnel.
State	Select to enable and disable GRE tunnel.
IP Address	Assign an IP address/mask for the GRE tunnel.
MTU	Enter the number of bytes indicating the largest physical packet size that the network can transmit.
Local Network	Select the local network to use the GRE tunnel. Select vpn N to use the VPN network. Select any to use any available interface to remote host.
Remote Host	Enter the remote IP address to use for the GRE tunnel.
Remote Network	Enter the remote network to use for the GRE tunnel.

To Configure Tunnel Serial Settings

Using Web Manager

- ◆ To configure the GRE for a specific tunnel, click **GRE**.

Using the CLI

- ◆ To enter GRE command level: `enable -> gre`

Using XML

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

6: Action Settings

Actions can be configured for alarms and reports available in the PremierWave EN embedded system on module.

Alarms and Reports

The PremierWave EN updates the action settings page to display and configure the alarms. The following alarm and report actions are available in PremierWave EN device:

- ◆ Eth0 link state change
- ◆ Wlan0 link state change
- ◆ On scheduled reboot

One or more types of “action” can be configured and triggered when an event occurs.

Note: The “on scheduled reboot” alarm state will be on at the time of a scheduled reboot and will remain on till the device actually reboots (in approximately 30 seconds). These are not applicable for “on scheduled reboot” alarm: Email Alarm Reminder Interval, Normal Email, Normal Message, Normal Reminder Interval, SNMP Reminder Interval, SNMP Normal Message, and Delay.

Actions

Table 6-1 contains the configuration options for all the alarms and reports listed above.

Table 6-1 Action Settings

Action Settings	Description
Delay	Use Delay to defer alarm processing. Alarm actions will not be executed if the cause is corrected within this time.
Email	Use Email to send an email to configured Email recipients. <ul style="list-style-type: none">◆ If an Alarm Email profile number is selected, that email will be sent when the alarm is turned on. The contents of Alarm Message will be placed into the email body when an alarm email is sent. If the alarm stays on longer than the Reminder Interval, another alarm email is sent.◆ If a Normal Email profile number is selected, that email will be sent when the alarm is turned off. The contents of Normal Message will be placed into the email body when a normal email is sent. If the alarm stays off longer than the Reminder Interval, another normal email is sent.

Action Settings	Description
FTP Put	Use FTP Put to put a file on configured FTP server. Filename will be used to upload to remote FTP server. The IP Address or hostname is the FTP server to connect. Port number is port on which FTP server is listening on. Use Protocol to connect to FTP server. FTPS is a SSL encrypted communication channel and SSL Trusted Authorities must be setup with FTP server SSL certificate. Username is used to logon to FTP server. If FTP server does not require authentication, use anonymous. Password is used to logon to FTP server. If FTP server does not require authentication, a common practice is to use user's email address. If the alarm stays on or off longer than the Reminder Interval , another FTP Put is performed. In Sequential mode, connections will be attempted starting with number 1 until a connection is successful. In Simultaneous mode, all possible connections will be made.
HTTP Post	Use HTTP Post post to configured HTTP server. The URL appears behind the HTTP server IP address or hostname. E.g. http://some_http_server/some_url The IP Address or hostname is the HTTP server to connect to. Port number is the port which HTTP server is listening on. Use Protocol to connect to HTTP server. HTTPS is a SSL encrypted communication channel and SSL Trusted Authorities must be setup with HTTP server SSL certificate. Username used to logon to HTTP server if authentication is required. Password used to logon to HTTP server if authentication is required. If the alarm stays on or off longer than the Reminder Interval , another HTTP Post is performed. In Sequential mode, connections will be attempted starting with number 1 until a connection is successful. In Simultaneous mode, all possible connections will be made.
SNMP Trap	Use SNMP Trap to send SNMP trap to configured trap destinations. Check to enable or disable the State . The contents of Alarm Message are included when an alarm SNMP trap is sent. If the alarm stays on longer than the Reminder Interval , another alarm SNMP Trap is sent. The contents of Normal Message are included when a normal SNMP trap is sent. If the alarm stays off longer than the Reminder Interval, another normal SNMP Trap is sent.

To Configure Action Settings

Using Web Manager

- ◆ To view Action status information, click **Action** on the menu and select **Status**.
- ◆ To modify Action information, click **Action** on the menu and select a specific action from the drop-down menu. [Alarms and Reports \(on page 63\)](#) lists the options.

Using the CLI

- ◆ To enter the eth0 link state change command level: `enable -> config -> action -> eth0 link state change`
- ◆ To enter the wlan0 link state change command level: `enable -> config -> action -> wlan0 link state change`
- ◆ To enter on scheduled reboot command level: `enable -> config -> action -> on scheduled reboot`

Using XML

- ◆ Include in your file: `<configgroup name = "action" instance = "eth0 link state change">`

- ◆ **Include in your file:** `<configgroup name = "action" instance = "wlan0 link state change">`
- ◆ **Include in your file:**
`<configgroup name = "action" instance = "on scheduled reboot">`

Python

Python™ is a dynamic, object-oriented programming language that can be used for developing a wide range of software applications. The Lantronix PremierWave EN embedded system on module includes the installation of Python interpreter, making it easy to load and run custom Python scripts on your embedded system on module.

The version of Python programming language installed on the Lantronix PremierWaveEN embedded system on module comes with "batteries included" by having the Python language's standard library. In addition, the developer can take advantage of thousands of available third party packages to speed up development.

IDE

Python scripts can be written with any text editor. If using Windows for development, Notepad++ is a powerful choice as this text editor includes traditional IDE features such as syntax highlighting and automatic indentation (<http://notepad-plus-plus.org/>). Notepad++ also includes the ability to customize through plugins. Some interesting plugins for the development of Python scripts for the Lantronix PremierWave EN platform include the following:

- ◆ **PyNPP:** <https://github.com/mpcabd/PyNPP>
This plugin allows the user to use keystrokes to launch the open Python script in the local Python interpreter for debugging and testing.
- ◆ **NppFTP:** <http://sourceforge.net/projects/nppftp/>
This plugin provides a one-click upload of a file to an FTP server. Debugging and testing on the PremierWave platform easier because PremierWave products have an FTP server through which to upload files into the file system.

Applications

The PremierWave EN embedded system on module supports the ability to install and uninstall user-defined Python scripts and packages and will include the following:

bin	python	
lib	libpython{version}.so	
	<ltrx python sdk>	
	libpython{version}	"python precompiled scripts python shared libraries

Table 6-2 contains the setting options for configuring, installing, uninstalling and running external applications via Python scripts.

Caution: *Use extreme caution when installing and running scripts.*

Table 6-2 Script Settings

Script Settings	Description
Enabled (checkbox)	Check the Enabled checkbox within a particular script to enable it. Uncheck the checkbox to disable the script.
Run on startup (checkbox)	Check the Run on startup checkbox within a particular script to have it run upon the start up of the PremierWave unit. Uncheck the checkbox to disable automatically running the unit upon startup.
Run on shutdown (checkbox)	Check the Run on shutdown checkbox within a particular script to have it run on shutdown of the Premierwave unit. Uncheck the checkbox to disable automatically running the script upon shutdown.
Script	Enter the path of script to run in Filesystem.
Parameter	Enter the script parameters (if any).
Output	Enter output log file (if desired) for the script to redirect output of script to file. If the name of output log contains "%t", it will translate it into timestamp (e.g., script1_%t.log => script1_2007-01-02_19-06-57.log)
Run (button)	Click the Run button to manually execute the script. <i>Note: The script is run with configuration saved to the Flash.</i>
Uninstall (button)	Click the Uninstall button in a Python package to uninstall it.
Remove All (button)	Click the Remove All button to uninstall all Python packages.
Filename	Enter the package file name pathway in the file system and click the Install button to install it.

To Configure Application Settings

Using Web Manager

- ◆ To configure application scripts, click **Applications** on the menu.

Using the CLI

- ◆ To enter the application script change command level: `enable -> config -> applications`

Using XML

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

7: Line and Tunnel Settings

The PremierWave EN embedded device server contains three serial lines. All lines use standard RS232/RS485 serial ports, except Line 3 which is an emulated serial port over the USB Device (USB-CDC-ACM). All lines (except Line 3) can be configured to operate in the following modes:

- ◆ RS232
- ◆ RS485 Full Duplex (also compatible with RS-422)
- ◆ RS485 Half Duplex, with and without termination impedance
- ◆ All serial settings such as Baud Rate, Parity, Data Bits, etc, apply to these lines.

Line Statistics

This page displays the current status and various statistics for the serial line.

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

Using Web Manager

- ◆ To view statistics for Line 1, click **Line** in the menu and select **Line 1 -> Statistics**.

Using the CLI

- ◆ To view Line statistics: `enable -> line 1, show statistics`

Using XML

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

USB-CDC-ACM

Line 3 can only operate as an emulated serial port over the USB device port. It uses the standard CDC/ACM protocol, which is supported natively by most host operating systems (Windows, Linux, etc.). Since it is an emulated serial port, most standard serial port settings are irrelevant. Flow control is inherent to the USB protocol, and the line speed (Baud Rate) will be "as fast as conditions permit".

When the PremierWave EN USB device port is cabled to a host, it will identify itself with the industry standard USB vendor ID of 0x0525 and product ID of 0xa4a7.

When attached to a Windows host, a device driver .inf file (see Appendix E - USB-CDC-ACM Device Driver File for Windows Hosts) must be installed the first time the port is cabled. Once installed, Windows will configure an available COM port, each time the USB cable is attached.

Caution: *Under Windows, if the PremierWave device is rebooted when an active COM port is configured and in use, the COM port will come back up in an unstable state. When this happens, any terminal program accessing the COM port must be disconnected before reboot, and the USB cable physically replugged.*

When attached to a Linux host, the USB-CDC-ACM connection will automatically be configured, assuming the Linux host is configured for USB host operation and the "cdc_acm" driver is available. Once recognized, the cdc_acm driver will configure a standard serial port in the /dev/ttyACMx series, where x is a number 0, 1, 2, 3, etc.

Caution: *Under Linux, if the /dev/ttyACMx device is in use when the PremierWave EN unit is rebooted, some terminal programs under Linux will automatically disconnect while others will not. If a terminal program does not disconnect automatically, when the PremierWave EN device comes back up, the CDC-ACM connection will be enumerated to a different /dev/ttyACMx device.*

Line Settings

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

To Configure Line Settings

Using Web Manager

- ◆ To configure Line 1, click **Line** in the menu and select **Line 1 -> Configuration**.

Using the CLI

- ◆ To view Line statistics: `enable -> line 1, show statistics`

Using XML

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

The Line Settings allow configuration of the serial lines (ports).

Table 7-1 Line Configuration Settings

Line Settings	Description
Name	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.
Interface	Set the interface type for the Line. The default is RS232 , and USB-CDC-ACM for Line 3. Choices are: <ul style="list-style-type: none"> ◆ RS232but may ◆ RS485 Full-Duplex ◆ RS485 Half-Duplex
Termination	Select to Enable or Disable Line Termination. The default is Disable . Note: <i>This setting is only relevant for Interface type RS485 Half-Duplex.</i>
State	Select to enable or disable the operational state of the Line. The default is Enabled .

Line Settings	Description
Protocol	Set the operational protocol for the Line. The default is Tunnel. Choices are: <ul style="list-style-type: none"> ◆ None ◆ Modbus RTU ◆ Modbus ASCII ◆ Tunnel = Serial-Network tunneling protocol.
Baud Rate	Set the Baud Rate (speed) of the Line. The default is 9600 . Any set speed between 300 and 921600 may be selected: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600. When selecting a Custom baud rate, you may manually enter any value between 300 and 5000000. <i>Note: Custom baud rates are not supported when a line is configured for Command Mode. For Interface type USB-CDC-ACM (Line 3 only), this setting is irrelevant.</i>
Parity	Set the Parity of the Line. The default is None . <i>Note: For Interface type USB-CDC-ACM (Line 3 only), this setting is irrelevant.</i>
Data Bits	Set the number of data bits for the Line. The default is 8 . <i>Note: For Interface type USB-CDC-ACM (Line 3 only), this setting is irrelevant.</i>
Stop Bits	Set the number of stop bits for the Line. The default is 1 . <i>Note: For Interface type USB-CDC-ACM (Line 3 only), this setting is irrelevant.</i>
Flow Control	Set the flow control for the Line. The default is None . <i>Note: For Interface type USB-CDC-ACM (Line 3 only), this setting is irrelevant.</i> <i>Note: This field becomes available if RS232 or RS485 Full-Duplex is selected under Interface above.</i>
Xon Char	Set Xon Char to be used when Flow Control is set to Software. Prefix decimal with \ or prefix hexadecimal with 0x or prefix a single control character <control>. <i>Note: This field becomes available for configuration when Software is selected under Flow Control.</i>
Xoff Char	Set Xoff Char to be used when Flow Control is set to Software. Prefix decimal with \ or prefix hexadecimal with 0x or prefix a single control character <control>. <i>Note: This field becomes available for configuration when Software is selected under Flow Control.</i>
Gap Timer	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).
Threshold	Set the number of threshold bytes which need to be received in order for the driver to forward received characters.

Table 7-2 Line Command Mode Settings

Line Command Mode Settings	Description
Mode	<p>Set the Command Mode state of the Line. When in Command Mode, a CLI session operates exclusively on the Line. Choices are:</p> <ul style="list-style-type: none"> ◆ Always ◆ User Serial String ◆ Disabled <p>Note: In order to enable Command Mode on the Line, Tunneling on the Line must be Disabled (both Connect and Accept modes). Also, custom baud rates are not supported in Command Mode.</p>
Wait Time	<p>Enter the amount of time to wait during boot time for the Serial String. This timer starts right after the Signon Message has been sent on the Serial Line and applies only if mode is "Use Serial String".</p> <p>Note: This field becomes available when Use Serial String is selected for Mode.</p>
Serial String	<p>Enter the Text or Binary string of bytes that must be read on the Serial Line during boot time in order to enable Command Mode. It may contain a time element to specify a required delay in milliseconds x, formed as {x}. Applies only if mode is "User Serial String". It may contain a binary character(s) of the form [x]. For example, use decimal [12] or hex [0xc].</p> <p>Note: This field becomes available when Use Serial String is selected for Mode.</p>
Echo Serial String	<p>Select Enable or Disable for Echo Serial String. Applies only if mode is "User Serial String". Select enable to echo received characters backed out on the line while looking for the serial string.</p> <p>Note: This field becomes available when Use Serial String is selected for Mode.</p>
Signon Message	<p>Enter the string of bytes to be sent to the Serial Line during boot time. It may contain a binary character(s) of the form [x]. For example, use decimal [12] or hex [0xc].</p>

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

To Configure Line Command Mode

Using Web Manager

- ◆ To configure a specific line, click **Line** in the menu and select **Line 1 -> Configuration** ([Table 7-1](#)).
- ◆ To configure a specific line in Command Mode, click **Line** in the menu and select **Line 1 -> Command Mode** ([Table 7-2](#)).

Using the CLI

- ◆ To enter Line 1 command level: `enable -> line 1`

Using XML

- ◆ Include in your file: `<configgroup name="line" instance="1">`
- ◆ Include in your file: `<configgroup name="serial command mode" instance="1">`

Tunnel 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.

Note: The following section describes the steps to view Tunnel 1 statistics; these steps apply to other tunnel instances of the device.

To View Tunnel Statistics

Using Web Manager

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

Using the CLI

- ◆ To view Tunnel 1 statistics: enable -> tunnel 1, show statistics

Using XML

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

Tunnel Settings

Tunneling allows serial devices to communicate over a network, without “being aware” of the devices that establish the network connection between them. Tunneling parameters are configured using the Tunnel menu and submenus. The Tunnel settings allow you to configure how the Serial-Network tunneling operates. Tunneling is available on all serial lines. The connections on one serial line are separate from those on another serial port.

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

Serial 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 7-3 Tunnel Serial Settings

Tunnel Serial Settings	Description
Line Settings	Line Settings information here is display only. Go to the section, To Configure Line Command Mode to modify these settings.
Protocol	Protocol information here is display only. Go to the section, To Configure Line Command Mode to modify these settings.

Tunnel Serial Settings (continued)	Description
DTR	<p>Select the conditions under which the Data Terminal Ready (DTR) control signal on the serial line is asserted. Choices are:</p> <ul style="list-style-type: none"> ◆ Unasserted ◆ TruPort = the DTR is asserted whenever either a connect or an accept mode tunnel connection is active with the Telnet Protocol RFC2217 saying that the remote DSR is asserted. ◆ Asserted while connected = the DTR is asserted whenever either a connect or an accept mode tunnel connection is active. ◆ Continuously asserted

To Configure Tunnel Serial Settings

Using Web Manager

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

Using the CLI

- ◆ To enter Tunnel 1 command level: `enable -> tunnel 1 -> serial`

Using XML

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

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 7-4 Tunnel Packing Mode Settings

Tunnel Packing Mode Settings	Description
Mode	<p>Configure the Tunnel Packing Mode. Choices are:</p> <ul style="list-style-type: none"> ◆ Disable = Data not packed. ◆ Timeout = data sent after timeout occurs. ◆ Send Character = data sent when the Send Character is read on the Serial Line.
Threshold	<p>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.</p>
Timeout	<p>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. This setting becomes available when the Timeout mode is selected.</p>

Tunnel Packing Mode Settings	Description
Send Character	Enter Control Characters in any of the following forms: <ul style="list-style-type: none"> ◆ <control>J ◆ 0xA (hexadecimal) ◆ \10 (decimal) 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.
Trailing Character	Enter Control Characters in any of the following forms: <ul style="list-style-type: none"> ◆ <control>J ◆ 0xA (hexadecimal) ◆ \10 (decimal). 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 <None>).

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 Mode**.

Using the CLI

- ◆ To enter the Tunnel 1 Packing command level: `enable -> tunnel 1 -> packing`

Using XML

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

Accept Mode

In Accept Mode, the PremierWaveEN device 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. Supported serial lines and associated local port numbers progress sequentially in matching value. For instance, the default local port is 10001 for serial line 1 and the default local port for serial line 2 is 10002, and so on for the number of serial lines supported.

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

Table 7-5 Tunnel Accept Mode Settings

Tunnel Accept Mode Settings	Description
Mode	Set the method used to start a tunnel in Accept mode. Choices are: <ul style="list-style-type: none"> ◆ Disable = do not accept an incoming connection. ◆ Always = accept an incoming connection (<i>default</i>). ◆ Any Character = start waiting for an incoming connection when any character is read on the serial line. ◆ Start Character = start waiting for an incoming connection when the start character for the selected tunnel is read on the serial line. ◆ Modem Control Asserted = start waiting for an incoming connection as long as the Modem Control pin (DSR) is asserted on the serial line until a connection is made. ◆ Modem Emulation = start waiting for an incoming connection when triggered by modem emulation AT commands. Connect mode must also be set to Modem Emulation.
Local Port	Set the port number for use as the network local port. The default local port number for each supported serial line number progresses sequentially in equal value so that Tunnel X: 1000X. For example: <ul style="list-style-type: none"> ◆ Tunnel 1: 10001 ◆ Tunnel 2: 10002 ◆ Tunnel 3: 10003
Protocol	Select the protocol type for use with Accept Mode: <ul style="list-style-type: none"> ◆ SSH ◆ SSL ◆ TCP (default protocol) ◆ TCP AES <p><i>Note:</i> Telnet</p>
Credentials	Specifies the name of the set of RSA and/or DSA certificates and keys to be used for an SSL connection.
AES Encrypt Key	Specify the text or hexadecimal advanced encryption standard (AES) key for encrypting outgoing data for a TCP AES connection.
AES Decrypt Key	Specify the text or hexadecimal AES key for decrypting incoming data for a TCP AES connection.
TCP Keep Alive Idle Time	Enter the time, in milliseconds, the PremierWave EN module waits during a silent TCP connection before checking if the currently connected network device is still on the network.
TCP Keep Alive Interval	Enter, in milliseconds, the amount of time between two successive keep alive probes if no acknowledgment to the previous keep alive probe is not received.
TCP Keep Alive Probes	Specify the number of TCP Keep Alive probes (after the TCP Initial Kleep Alive probe) to send before closing the connection if no response is received. Valid values are between 1 and 16. Blank the display field to restore the default.

Tunnel Accept Mode Settings (continued)	Description
Initial Send	<p>Enter the Initial Send string indicating whether it is in Text or Binary form. This Initial Send data will be sent out to the network upon connection establishment, before any data, from the Line. It may contain one or more directives in the form %<char>.</p> <p>The binary form allows square braces [] to enclose one or more character designations separated by commas. Use straight decimals up to 255 or hexadecimal numbers prefixed with 0x up to 0xFF within the square braces. To specify an open brace in binary mode, use two in a row. Example (in binary mode): AB [255, 0xFF [C [[D] results in a string containing binary values where the dots appear: AB . . C [D].</p> <p>Directives:</p> <ul style="list-style-type: none"> %i local IP address %m MAC address %n network interface name %p local port %s serial number %% %
Flush Serial	<p>Set whether the serial line data buffer is flushed upon a new network connection. Choices are:</p> <ul style="list-style-type: none"> ◆ Enabled = serial data buffer is flushed on network connection ◆ Disabled = serial data buffer is not flushed on network connection (<i>default</i>)
Block Serial	<p>Set whether Block Serial is enabled for debugging purposes. Choices are:</p> <ul style="list-style-type: none"> ◆ Enabled = 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. ◆ Disabled = this is the default setting; incoming characters from the Serial Line are sent on into the network. Any buffered characters are sent first.
Block Network	<p>Set whether Block Network is enabled for debugging purposes. Choices are:</p> <ul style="list-style-type: none"> ◆ Enabled = 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. ◆ Disabled = this is the default setting; incoming characters from the network are sent on into the Serial Line. Any buffered characters are sent first.
Password	<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"> ◆ 0A (Line Feed) ◆ 00 (Null) ◆ 0D 0A (Carriage Return/Line Feed) ◆ 0D 00 (Carriage Return/Null) <p>If, Prompt for Password is set to Enabled and a password is provided, the user will be prompted for the password upon connection.</p>
Prompt for Password	<p>Select Enabled or Disabled (to enable or disable). This option will only appear if a password is specified above.</p>
Email on Connect	<p>Select an email profile number to which an email notification will be sent upon the establishment of an accept mode tunnel.</p>
Email on Disconnect	<p>Select an email profile number to which an email notification will be sent upon the disconnection of an accept mode tunnel.</p>

Tunnel Accept Mode Settings (continued)	Description
CP Output	Enter the CP Output Group whose value should change when a connection is established and dropped. Connection Value specifies the value to set the CP Group to when a connection is established. Disconnection Value specifies the value to set the CP Group to when the connection is closed. To display the "Connection Value" and "Disconnection Value", first enter a "CP Output Group", then click outside that field.

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 Mode**.

Using the CLI

- ◆ To enter Tunnel 1 Accept Mode command level: `enable -> tunnel 1 -> accept`

Using XML

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

Connect Mode

In Connect Mode, the PremierWave EN unit continues to attempt an outgoing connection on the network, until established (based on which connection method is selected in the configuration described in [Table 7-6](#)). If the connection attempt fails or the connection drops, then it retries after a timeout. The remote node on the network must listen for the Connect Mode's connection.

For Connect Mode to function, it must be enabled, have a remote station (node) configured, and a remote port configured (TCP or UDP). When established, Connect Mode is always on. Enter the remote station as an IPv4 or IPv6 address or DNS name. The PremierWave EN device will not make a connection unless it can resolve the address.

For Connect Mode using UDP, the PremierWave EN module accepts packets from any device on the network. It will send packets to the last device that sent it packets.

Note: *The port in Connect Mode is not the same port configured in Accept Mode. Telnet protocol is supported in only Tunnels 1 and 2 when in connect mode. RFC2217 is not supported by USB serial.*

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

Table 7-6 Tunnel Connect Mode Settings

Tunnel Connect Mode Settings	Description
Mode	<p>Set the method to be used to attempt a connection to a remote host or device. Choices are:</p> <ul style="list-style-type: none"> ◆ Disable = an outgoing connection is never attempted. (<i>default</i>) ◆ Always = a connection is attempted until one is made. If the connection gets disconnected, the device retries until it makes a connection. ◆ Any Character = a connection is attempted when any character is read on the serial line. ◆ Start Character = a connection is attempted when the start character for the selected tunnel is read on the serial line. ◆ Modem Control Asserted = a connection is attempted as long as the Modem Control pin (DSR) is asserted, until a connection is made. ◆ Modem Emulation = a connection is attempted when triggered by modem emulation AT commands.
Local Port	<p>Enter an alternative Local Port. The Local Port is set to <Random> by default but can be overridden. Blank the field to restore the default.</p>
Host (Number)	<p>Click on the displayed information to expand it for editing. If <None> is displayed, clicking it will allow you to configure a new host. At least one Host is required to enable Connect Mode as this information is necessary to connect to that host. Once you start to edit Host 1, a box for Host 2 will show up. Editing Host 2 will cause a Host 3 box to appear. Up to 32 hosts are available. Complete the following fields to configure a host:</p> <ul style="list-style-type: none"> ◆ Address: enter the address for the remote host connection. Either a DNS address or an IP address maybe provided. ◆ Port: designate the TCP or UDP port on the remote host for connection. ◆ Protocol: select the desired security protocol. SSH is recommended for circumstances with high security concerns. When using SH, both the SSH server host keys and the SSH server authorized users must be configured. ◆ Credentials: specify the name of the set of RSA and/or DSA certificates and keys to be used for the SSL connection. ◆ Validate Certificate: Select to enable or disable. Enabling requires the tunnel to verify the remote SSL server certificate when making a connection. ◆ SSH Username: specify the SSH client user to use for an outgoing SSH connections. ◆ TCP Keep Alive Idle Time: specify the amount of time to wait before the first Keep Alive probe is sent to the remote host in order to keep the TCP connection up during idle transfer periods. Set to 0 to disable and blank the display field to restore the default. ◆ TCP Initial Keep Alive: specify the amount of time to wait before the first Keep Alive probe is sent to the remote host in order to keep the TCP connection up during idle transfer periods. Set to 0 to disable and blank the display field to restore the default. ◆ TCP Keep Alive Interval: specify the amount of time to wait before probing the remote host, after the initial probe, in order to keep the TCP connection up during idle transfer periods. Blank the display field to restore the default. ◆ TCP Keep Alive Probes: specify the number of TCP Keep Alive probes (after the TCP Initial Keep Alive Probe) to send before closing the connection if no response is received. Valid values are between 1 and 16. Blank the display field to restore the default.

Tunnel Connect Mode Settings (continued)	Description
Host (Number) (continued)	<ul style="list-style-type: none"> ◆ TCP User Timeout: specify the amount of time the TCP segments will be retransmitted before the connection is closed. ◆ AES Encrypt Key: enter the AES encrypt key to encrypt outgoing data. Enter the key in the fixed 16, 24, or 32 byte length and either in Text or Hexadecimal form. Keys are stored and exchanged in Hexadecimal form only. To remove a key, delete <Configured> in the display. All keys are shared secret keys which are known by both sides of the connection and kept secret. ◆ AES Decrypt Key: enter the AES decrypt key to decrypt outgoing data. Enter the key in the fixed 16, 24, or 32 byte length and either in Text or Hexadecimal form. Keys are stored and exchanged in Hexadecimal form only. To remove a key, delete <Configured> in the display. All keys are shared secret keys which are known by both sides of the connection and kept secret. ◆ Initial Send: enter the Initial Send string for data sent out of the network upon connection establishment (before any data from the Line). The string may contain one or more Directives of the form %<char> and can be entered in Text or Binary form. <p>Notes:</p> <ul style="list-style-type: none"> ◆ <i>If the keep alive idle time (the initial keep alive probe) expires, the user timeout is expired, and there are probes in flight, the connection will be reset. For this reason, it is recommended that if keep alive is used in conjunction with the user timeout, the keep alive timeouts be larger than the user timeout. If they are smaller, what will typically be seen is that the initial probe will be sent, then at the interval where the next probe would normally be sent, the connection will be reset, with no additional probes sent. Also note that the probe count can be disregarded in these cases: if the keep alive timers are significantly smaller than the user timeout, probes will continue to be sent for an unreachable host until the user timeout expires.</i> ◆ <i>If there is data in flight when the TCP retransmission timeout kicks in, the user timeout is checked as a limiting condition only when the timer expirations would normally be checked during RTO handling. In other words, the user timeout will not be an exact limit; in practice, it will always take somewhat longer for the connection to be closed. The longer the user timeout is, the more likely it will expire between exponentially slower retransmissions, and the connection will not experience an error until the next retransmission timeout is checked. Also note that the user timeout expiration during retransmission returns an error to the application; it does not automatically reset the connection as happens with keep alive timeout. It is up to the application (e.g., tunneling) to close the connection (this happens almost immediately with tunneling).</i> ◆ <i>Tunnel 3 does not support Telnet protocol.</i>
Reconnect Timer	Set the value of the reconnect timeout (in milliseconds) for outgoing connections established by the device. Valid range is 1 to 65535 milliseconds. Default is 15000.
Flush Serial Data	Set whether the serial Line data buffer is flushed upon a new network connection. Choices are: <ul style="list-style-type: none"> ◆ Enabled = serial data buffer is flushed on network connection ◆ Disabled = serial data buffer is not flushed on network connection (<i>default</i>)

Tunnel Connect Mode Settings (continued)	Description
Block Serial	Set whether Block Serial is enabled for debugging purposes. Choices are: <ul style="list-style-type: none"> ◆ Enabled = 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. ◆ Disabled = this is the default setting; incoming characters from the Serial Line are sent on into the network. Any buffered characters are sent first.
Block Network	Set whether Block Network is enabled for debugging purposes. Choices are: <ul style="list-style-type: none"> ◆ Enabled = 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. ◆ Disabled = this is the default setting; incoming characters from the network are sent on into the Serial Line. Any buffered characters are sent first.
Email on Connect	Select an email profile number to which an email notification will be sent upon the establishment of an accept mode tunnel.
Email on Disconnect	Select an email profile number to which an email notification will be sent upon the disconnection of an accept mode tunnel.
CP Output	Enter the CP Output Group whose value should change when a connection is established and dropped. Connection Value specifies the value to set the CP Group to when a connection is established. Disconnection Value specifies the value to set the CP Group to when the connection is closed. To display the "Connection Value" and "Disconnection Value", first enter a "CP Output Group", then click outside that field.

To Configure Tunnel Connect Mode Settings

Using Web Manager

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

Using the CLI

- ◆ To enter the Tunnel 1 Connect Mode command level: `enable -> tunnel 1 -> connect`

Using XML

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

Connecting Multiple Hosts

If more than one host is configured, a **Host Mode** option appears. Host Mode controls how multiple hosts will be accessed. For the PremierWave device, the Connect Mode supports up to 32 hosts. Hosts may be accessed sequentially or simultaneously:


- ◆ **Sequential** – Sequential host lists establish a prioritized list of tunnels. The host specified as Host 1 will be attempted first. If that fails, it will proceed to Host 2, 3, etc, in the order they are specified. When a connection drops, the cycle starts again with Host 1 and proceeds in order. Establishing the host order is accomplished with host list promotion (see [Host List Promotion on page 80](#)). Sequential is the default Host Mode.

- ◆ **Simultaneous** – A tunnel will connect to all hosts accepting a connection. Simultaneous connections occur at the same time to all listed hosts. The device can support a maximum of 64 total aggregate connections.

Host List Promotion

This feature allows Host IP promotion of individual hosts in the overall sequence.

To promote a specific Host:

1. Click the  icon in the desired Host field, for example Host 2 and Host 3.
2. The selected Host(s) exchanges its place with the Host above it.
3. Click **Submit**. The hosts change sequence.

Disconnect Mode

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

Table 7-7 Tunnel Disconnect Mode Settings

Tunnel Disconnect Mode Settings	Description
Stop Character	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: <control>J or 0xA(hexadecimal) or \10 (decimal). Disable the Stop Character by blanking the field to set it to <None>.
Modem Control	Set whether Modem Control enables disconnect when the Modem Control pin is not asserted on the Serial Line. Choices are: <ul style="list-style-type: none"> ◆ Enabled ◆ Disabled (default)
Timeout	Enter the number of milliseconds a tunnel may be idle before disconnection. The value of zero disables the idle timeout.
Flush Serial Data	Set whether to flush the Serial Line when the Tunnel is disconnected. Choices are: <ul style="list-style-type: none"> ◆ Enabled ◆ Disabled (default)

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 Mode**.

Using the CLI

- ◆ To enter the Tunnel 1 Disconnect command level: `enable -> tunnel 1 -> disconnect`

Using XML

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

Modem Emulation

Some older equipment is designed to attach to a serial port and dial into a network with a modem. This equipment uses AT commands to control the connection. For compatibility with these older devices on modern networks, the PremierWave device mimics the behavior of the modem.

Table 7-8 Tunnel Modem Emulation Settings

Tunnel Modem Emulation Settings	Description
Echo Pluses	Set whether the pluses will be echoed back during a "pause +++ pause" escape sequence on the Serial Line. Choices are: <ul style="list-style-type: none"> ◆ Enabled ◆ Disabled (default)
Echo Commands	Set whether characters read on the Serial Line will be echoed, while the Line is in Modem Command Mode. Choices are: <ul style="list-style-type: none"> ◆ Enabled ◆ Disabled (default)
Verbose Response	Set whether Modem Response Codes are sent out on the Serial Line. Choices are: <ul style="list-style-type: none"> ◆ Enabled ◆ Disabled (default)
Response Type	Select a representation for the Modem Response Codes sent out on the Serial Line. Choices are: <ul style="list-style-type: none"> ◆ Text (ATV1) (default) ◆ Numeric (ATV0)
Error Unknown Commands	Set whether the Error Unknown Commands is enabled (ATU0) and ERROR is returned on the Serial Line for unrecognized AT commands. Otherwise (ATU1) OK is returned for unrecognized AT commands. Choices are: <ul style="list-style-type: none"> ◆ Enabled ◆ Disabled (default)
Incoming Connection	Set how and if requests are answered after an incoming RING (ATS0=2). Choices are: <ul style="list-style-type: none"> ◆ Disabled (default) ◆ Automatic ◆ Manual
Connect String	Enter the customized Connect String sent to the Serial Line with the Connect Modem Response Code.
Display Remote IP	Set whether the Display Remote IP is enabled so that the incoming RING sent on the Serial Line is followed by the IP address of the caller. Choices are: <ul style="list-style-type: none"> ◆ Enabled ◆ Disabled (default)

To Configure Tunnel Modem Emulation Settings

Using Web Manager

To configure the Modem Emulation for a specific tunnel, click **Tunnel** in the menu and select **Tunnel 1 -> Modem Emulation**. *Using the CLI*

- ◆ To enter the Tunnel 1 Modem command level: enable -> tunnel 1 -> modem

Using XML

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

8: Terminal and Host Settings

Predefined connections are available via Telnet, SSH, or a serial port. A user can choose one of the presented options and the device automatically makes the predefined connection.

Either the Telnet, SSH, or serial port connection can present the CLI or the Login Connect Menu. By default, the CLI is presented when the device is accessed. When configured to present the Login Connect Menu, the hosts configured via the Host selections, and named serial lines are presented.

Terminal Settings

You can configure whether each serial line or the Telnet/SSH server presents a CLI or a Login Connect menu when a connection is made.

Table 8-1 Terminal on Network and Line Settings

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

To Configure the Terminal Network Connection

Using Web Manager

- ◆ To configure the Terminal on Network, click **Terminal** on the menu and select **Network -> Configuration**.

Using the CLI

- ◆ To enter the Terminal Network command level: `enable -> config -> terminal network`

Using XML

- ◆ Include in your file: `<configgroup name="terminal" instance="network">`

To Configure the Terminal Line Connection

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

Using Web Manager

- ◆ To configure a particular Terminal Line, click **Terminal** on the menu and select **Line 1 -> Configuration**.

Using the CLI

- ◆ To enter the Terminal Line command level: `enable -> config -> terminal 1`

Using XML

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

Host Configuration

Table 8-2 Host Configuration

Host Settings	Description
Name	Enter a name for the host. This name appears on the Login Connect Menu. To leave a host out of the menu, leave this field blank.
Protocol	Select the protocol to use to connect to the host. Choices are: <ul style="list-style-type: none"> ◆ Telnet ◆ SSH <p>Note: SSH keys must be loaded or created on the SSH page for the SSH protocol to work.</p>

Host Settings	Description
SSH Username	Appears if you selected SSH as the protocol. Enter a username to select a pre-configured Username/Password/Key (configured on the SSH: Client Users page), or leave it blank to be prompted for a username and password at connect time. <i>Note: This configuration option is only available when SSH is selected for Protocol.</i>
Remote Address	Enter an IP address for the host to which the device will connect.
Remote Port	Enter the port on the host to which the device will connect.

To Configure Host Settings

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

Using Web Manager

- ◆ To configure a particular Host, click **Host** on the menu and select **Host 1 -> Configuration**.

Using the CLI

- ◆ To enter the Host command level: `enable -> config -> host 1`

Using XML

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

9: Configurable Pin Manager

The Configurable Pin Manager (CPM) is responsible for assignment and control of the configurable pins (CPs) available on the PremierWave EN embedded device server. There are nine configurable pins on the PremierWave EN device.

You must configure the CPs by making them part of a group. A CP Group may consist of one or more CPs. This increases flexibility when incorporating the PremierWave EN embedded device server into another system.

Note: The blue text in the XML command strings of this chapter are to be replaced with a user-specified name.

CPM: Configurable Pins

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

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

Table 9-1 Current Configurable Pins

CP	Ref	Configured as	Value	Groups	Active in Group
CP1	Pin 14	Input	0	1	<available>
CP2	Pin 16	Input	1	0	<available>
CP3	Pin 18	Input	0	0	<available>
CP4	Pin 20	Input	1	0	<available>
CP5	Pin 32	Input	0	0	<available>
CP6	Pin 27	Input	0	0	<available>
CP7	Pin 44	Input	0	0	<available>
CP8	Pin 38	Input	0	0	<available>
CP9	Pin 42	Input	0	0	<available>

Table 9-2 CP Status

CPM – CPs Status	Description
Name	Shows the CP number.
State	Shows the current enable state of the CP.
Type	Shows the CP hardware pin type. <ul style="list-style-type: none">◆ Pin type can be updated by selecting from the drop down menu:<ul style="list-style-type: none">➢ Input➢ Output When a CP is configured as output, it can be toggled by setting the value. Whatever value is given, the first bit 0 is used as the setting. 1 means asserted and 0 means de-asserted.◆ Check to Assert Low. The CP logic can be inverted so that assertion is low.◆ Check Assert Low as desired and click Change to make these changes.

CPM – CPs Status	Description
Value	Shows the last bit in the CP current value.
Bit	Visual display of the bitwise 32 bit placeholders for a CP.
Level	A “+” symbol indicates the CP is asserted (the voltage is high). A “-“ indicates the CP voltage is low.
I/O	Indicates the current status of the pin: <ul style="list-style-type: none"> ◆ I = input ◆ O = output ◆ <blank> = unassigned
Logic	An “I” indicates the CP is inverted (active low).
Binary	Shows the binary assertion value of the corresponding bit.
CP#	Shows the CP number.
Groups	Lists the groups in which the CP is a member.

Notes:

- ◆ To modify a CP, all groups 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 Group. When the CP Group is saved, its CP settings are saved with it. Thus, a particular CP may be defined as "Input" in one group but as "Output" in another. Only one group containing any particular CP may be enabled at once.

CPM: Groups

The CP Groups settings allow for the management of CP groups. Groups can be created or deleted. CPs can be added to or removed from groups. A group, based on its state, can trigger outside events (such as sending email messages). Only an enabled group can be a trigger.

Table 9-3 CPM Group Current Configuration

CPM – Groups Current Configuration	Description
Group Name	Shows the CP group's name. Click on any particular Group Name to reveal the current, modifiable Group Status information in a table below.
State	Indicates whether the group is enabled or disabled.
CP Info	Shows the number of CPs assigned to the group.
Create Group	Enter the name of a new group and click Submit to create it. Once created, the group will appear below to allow modification.

Table 9-4 CPM Group Status

CPM – Groups Group Status	Description
Name	Shows the CP Group name representing the group status information displayed in this table. The status of a specific CP group appears in this table once either a particular preexisting group name is clicked in the above table under Current Configuration or immediately after a new group is created. Click the X to delete the current group as desired.

CPM – Groups Group Status (continued)	Description
State	Current enable state of the CP group is displayed. Click Enable or Disable to change the state.
Value	Displays the CP group's current value or shows "Disabled" if the group is disabled.
Bit	Visual display of the bit placeholders for a CP.
Level	A "+" symbol indicates the CP's bit position is asserted (the voltage is high). A "-" indicates the CP voltage is low.
I/O	Indicates the current status of the pin: <ul style="list-style-type: none"> ◆ I = input ◆ O = output ◆ <blank> = unassigned
Logic	An "I" indicates the CP output is inverted.
Binary	Shows the assertion value of the corresponding bit. X = group is disabled or bit is unassigned in group
CP#	Shows the configurable pin number and its bit position in the CP group.
Add (button)	Select to add a specific configurable pin (CP) at a particular bit size, assign the CP as Input or Output , click Assert Low (if desired), then click the Add button to add the particular configurable pin information for the current group displayed in the table. Once added, the information for the configurable pin will display for this group name.
Remove (button)	Select to delete a specific configurable pin (CP) and click Remove to remove this pin configuration for the group name displayed in the table.

To Configure CPM Settings

Using Web Manager

- ◆ To configure a configurable pin, click **CPM** in the menu, select **CPs** and then the **desired CP** to configure.
- ◆ To configure a CPM Group, click **CPM** in the menu, select **Groups** and then the **desired Group Name** to configure.

Using the CLI

- ◆ To enter the CPM command level: `enable -> cpm`

Using XML

- ◆ Include in your file: `<configgroup name="cp group" instance="group name" >`
- ◆ Include in your file: `<configitem name="cp" instance="cp number" >`

10: Network Services

DNS Settings

This section describes the active run-time settings for the domain name system (DNS) protocol. The primary and secondary DNS addresses come from the active interface. The static addresses from the Network Interface configuration settings may be overridden by DHCP.

Note: The blue text in the XML command strings of this chapter are to be replaced with a user-specified name.

Table 10-1 DNS Settings

Setting / Field	Description
Lookup	Perform one of the following: <ul style="list-style-type: none">◆ Enter an IP address, and perform a reverse Lookup to locate the hostname for that IP address◆ Enter a hostname, and perform a forward Lookup to locate the corresponding IP address

To View or Configure DNS Settings:

Using Web Manager

- ◆ To view DNS current status, click **DNS** in the menu.
- ◆ To lookup DNS name or IP address, click **DNS** in the menu to access the **Lookup** field.

Note: To configure DNS for cases where it is not supplied by a protocol, click **Network** in the menu and select **Interface -> Configuration**.

Using the CLI

- ◆ To enter the DNS command level: `enable -> dns`

Using XML

- ◆ Include in your file: `<configgroup name="interface" instance="eth0">`

FTP Settings

The FTP protocol can be used to upload and download user files, and upgrade the PremierWave EN embedded system on module firmware. A configurable option is provided to enable or disable access via this protocol.

Table 10-2 FTP Settings

FTP Settings	Description
State	Select to enable or disable the FTP server: <ul style="list-style-type: none"> ◆ Enabled (default) ◆ Disabled

To Configure FTP Settings

Using Web Manager

- ◆ To configure FTP and view FTP statistics, click **FTP** in the menu.

Using the CLI

- ◆ To enter the FTP command level: `enable -> config -> ftp`

Using XML

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

Syslog Settings

The Syslog information shows the current configuration and statistics of the syslog. Here you can configure the syslog host and the severity of the events to log.

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

Table 10-3 Syslog Settings

Syslog Settings	Description
State	Select to enable or disable the syslog: <ul style="list-style-type: none"> ◆ Enabled ◆ Disabled (default)
Host	Enter the IP address of the remote server to which system logs are sent for storage.
Remote Port	Enter the number of the port on the remote server that supports logging services. The default is 514.

Syslog Settings (continued)	Description
Severity Log Level	Specify the minimum level of system message the PremierWave device should log by selecting from the drop-down menu. This setting applies to all syslog facilities. The drop-down list in the Web Manager is in descending order of severity (e.g., Emergency is more severe than Alert.)

To View or Configure Syslog Settings

Using Web Manager

- ◆ To configure the Syslog and view current Syslog status, click **Syslog** in the menu.

Using the CLI

- ◆ To enter the Syslog command level: `enable -> config -> syslog`

Using XML

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

HTTP Settings

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

Table 10-4 HTTP Settings

HTTP Settings	Description
State	Select to enable or disable the HTTP server: <ul style="list-style-type: none"> ◆ Enabled (default) ◆ Disabled
Port	Enter the port for the HTTP server to use. The default is 80 .
Secure Port	Enter the port for the HTTPS server to use. The default is 443 . The HTTP server only listens on the HTTPS Port when an SSL certificate is configured.
Secure Protocols	Select to enable or disable the following protocols: <ul style="list-style-type: none"> ◆ SSL3 = Secure Sockets Layer version 3 ◆ TLS1.0 = Transport Layer Security version 1.0. TLS 1.0 is the successor of SSL3 as defined by the IETF. ◆ TLS1.1 = Transport Layer Security version 1.1 The protocols are enabled by default. <p><i>Note: A server certificate and associated private key need to be installed in the SSL configuration section to use HTTPS.</i></p>
Secure Credentials	Specify the name of the set of RSA and/or DSA certificates and keys to be used for the secure connection.

HTTP Settings (continued)	Description
Max Timeout	Enter the maximum time for the HTTP server to wait when receiving a request. This prevents Denial-of-Service (DoS) attacks. The default is 10 seconds.
Max Bytes	Enter the maximum number of bytes the HTTP server accepts when receiving a request. The default is 40 KB (this prevents DoS attacks). Note: You may need to increase this number in some cases where the browser is sending data aggressively within TCP Windows size limit, when file (including firmware upgrade) is uploaded from webpage.
Logging State	Select to enable or disable HTTP server logging: <ul style="list-style-type: none"> ◆ Enabled (default) ◆ Disabled
Max Log Entries	Set the maximum number of HTTP server log entries. Only the last Max Log Entries are cached and viewable.
Log Format	Set the log format string for the HTTP server. Follow these Log Format rules: <ul style="list-style-type: none"> ◆ %a - remote IP address (could be a proxy) ◆ %b - bytes sent excluding headers ◆ %B - bytes sent excluding headers (0 = '-') ◆ %h - remote host (same as '%a') ◆ %{h}i - header contents from request (h = header string) ◆ %m - request method ◆ %p - ephemeral local port value used for request ◆ %q - query string (prepend with '?' or empty '-') ◆ %t - timestamp HH:MM:SS (same as Apache '%(%H:%M:%S)t' or '%(%T)t') ◆ %u - remote user (could be bogus for 401 status) ◆ %U - URL path info ◆ %r - first line of request (same as '%m %U%q <version>') ◆ %s - return status
Authentication Timeout	The timeout period applies if the selected authentication type is either Digest or SSL/Digest . After this period of inactivity, the client must authenticate again.
Submit (button)	Click the Submit button which appears when any changes are entered in the HTTP Configuration table. Clicking the Submit button submits the changes.

To Configure HTTP Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

Table 10-5 HTTP Authentication Settings

HTTP Authentication Settings	Description
URI	Enter the Uniform Resource Identifier (URI). <i>Note: The URI must begin with '/' to refer to the filesystem.</i>
Auth Type	Select the authentication type: <ul style="list-style-type: none"> ◆ None = no authentication is necessary. ◆ Basic = encodes passwords using Base64. ◆ Digest = encodes passwords using MD5. ◆ SSL = can only be accessed over SSL (no password is required). ◆ SSL/Basic = is accessible only over SSL and encodes passwords using Base64. ◆ SSL/Digest = is accessible only over SSL and encodes passwords using MD5. <i>Note: When changing the parameters of Digest or SSL Digest authentication, it is often best to close and reopen the browser to ensure it does not attempt to use cached authentication information.</i>
Submit (button)	Click the Submit button after entering the HTTP authentication information.
Delete (button)	Click the Delete button to delete the HTTP authentication information.

To Configure HTTP Authentication

Using Web Manager

- ◆ To configure HTTP Authentication, click **HTTP** in the menu and select **Authentication**.

Using the CLI

- ◆ To enter the HTTP command level: enable -> config -> http

Using XML

- ◆ Include in your file:

```
<configgroup name="http authentication uri" instance="uri name">
```

RSS Settings

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

Table 10-6 RSS Settings

RSS Settings	Description
RSS Feed	Select On or Off for RSS feeds to an RSS publisher. The default setting is off.
Persistent	Select On or Off for RSS feed to be written to a file (<code>cfg_log.txt</code>) and to be available across reboots. The default setting is off.
Max Entries	Set the maximum number of log entries. Only the last Max Entries are cached and viewable.

RSS Settings	Description
View	Click the button to view RSS feeds.
Clear	Click the button to clear RSS feed data.

To Configure RSS Settings

Using Web Manager

- ◆ To configure RSS and view current RSS statistics, click **RSS** in the menu.

Using the CLI

- ◆ To enter the RSS command level: `enable -> config -> rss`

Using XML

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

SNMP Settings

Simple Network Management Protocol (SNMP) settings may be viewed and configured in this section.

Table 10-7 SNMP Settings

SNMP Settings	Description
State	Select to enable or disable the SNMP agent state.
Version	Select the SNMP version used by the SNMP agent.
Read Community	Specify the read community used by the agent (defaults to public community).
Write Community	Specify the write community used by the agent (defaults to private community).
System Contact	Specify the system contact.
System Name	Update the system name, as necessary. The default system name is "".
System Description	Update the system description, as necessary. The default system information includes the manufacturer name, model name, version and the serial number of the device.
System Location	Specify a system location for the SNMP setting.
Lantronix MIB File	Click the Lantronix MIB file name to save and load it into the MIB browser and trap receiver. This is the base MIB file for Lantronix products. Load or compile this file first.
MIB File	Click the MIB file name to save and load it into the MIB browser and trap receiver. This is the product specific MIB file. Load or compile this after the Lantronix MIB File.

To Configure SNMP Settings

Using Web Manager

- ◆ To configure SNMP, click **SNMP** in the menu.

Using the CLI

- ◆ To enter the SNMP command level: `enable -> config -> snmp`

Using XML

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

Discovery

The current statistics and configuration options for device discovery, including UPnP query port are available for the PremierWave EN embedded system on module.

Table 10-8 Discovery Settings

Discovery	Description
Query Port Server State	Select to enable or disable the query port server from responding to autodiscovery messages on port 0x77FE.
UPnP Server State	Select to enable or disable the UPnP server from discovering devices in Windows network places.
UPnP Server Port	Update the UPnP server port. Leaving this field blank will restore the default settings.

To Configure Discovery

Note: If you are utilizing Windows XP, make sure to select **UPnP User Interface** under **Windows Components > Networking Services > Details** before setting up the PremierWave device to utilize Discovery.

Using Web Manager

- ◆ To access the area with options to configure discovery and view current discovery statistics, click **Discovery** in the menu.

Using the CLI

- ◆ To enter the command level: `enable -> config -> discovery`

Using XML

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

SMTP Settings

Table 10-9 SMTP Settings

SMTP Settings	Description
From Address	Enter the From Address here. This is an email address and is required. If you wish to direct outbound email messages through a mail server, put your client email address here.
Server Address	Enter the Server Address to direct outbound email messages through a mail server.
Server Port	Enter the SMTP server port number. The default is 25
Username	Enter a Username to direct outbound email messages through a mail server.
Password	Enter a Password to direct outbound email messages through a mail server.
Overriding Domain	Enter the domain name to override the current domain name in EHLO (Extended Hello).

To Configure SMTP Settings

Using Web Manager

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

Using the CLI

- ◆ To enter the command level: `enable -> config -> smtp`

Using XML

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

Email Settings

View and configure email alerts relating to events occurring within the system.

Table 10-10 Email Configuration

Email – Configuration Settings	Description
From	Click the Configure SMTP link to configure SMTP. See SMTP Settings (on page 96) .
To	Enter the email address to which the email alerts will be sent. Multiple addresses are separated by semicolon (;). Required field if email is to be sent.
CC	Enter the email address to which the email alerts will be copied. Multiple addresses are separated by semicolon (;).
Reply To	Enter the email address to list in the Reply-To field of the email alert.

Email – Configuration Settings (continued)	Description
Subject	Enter the subject for the email alert. <i>Note: Emails sent as a result of an alarm will display the name of the alarm in the subject of the email, overriding the email subject configured in this field.</i>
Message File	Enter the path of the file to send with the email alert. This file appears within the message body of the email, not as an attachment.
Priority	Select the priority level for the email alert: <ul style="list-style-type: none"> ◆ Urgent ◆ High ◆ Normal ◆ Low ◆ Very Low
Trigger Email Send	Configure these fields to send an email based on a CP Group trigger. The device sends an email when the specified Value matches the current Group 's value. The Value field appears once the CP Group is identified.

To View, Configure, and Send Email

Note: The following section describes the steps to view and configure Email 1 settings; these steps apply to other emails available for the device.

Using Web Manager

- ◆ To view Email statistics, click **Email** in the menu and select **Email 1 -> Statistics**.
- ◆ To configure basic Email settings, click **Email** in the menu and select **Email 1 -> Configuration**.
- ◆ To send an email, click **Email** in the menu and select **Email 1 -> Send Email**.

Using the CLI

- ◆ To enter Email command level: `enable -> email 1`

Using XML

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

11: Security Settings

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

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

Note: *The device supports SSLv3 and its successors, TLS1.0 and TLS1.1. An incoming SSLv2 connection attempt is answered with an SSLv3 response. If the initiator also supports SSLv3, SSLv3 handles the rest of the connection.*

Public Key Infrastructure

Public key infrastructure (PKI) is based on an encryption technique that uses two keys: a public key and private key. Public keys can be used to encrypt messages which can only be decrypted using the private key. This technique is referred to as asymmetric encryption, as opposed to symmetric encryption, in which a single secret key is used by both parties.

TLS (SSL)

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), use asymmetric encryption for authentication. In some scenarios, only a server needs to be authenticated, in others both client and server authenticate each other. Once authentication is established, clients and servers use asymmetric encryption to exchange a secret key. Communication then proceeds with symmetric encryption, using this key.

SSH and some wireless authentication methods on the PremierWave EN embedded system on module make use of SSL. The PremierWave EN unit supports SSLv2, SSLv3, and TLS1.0.

TLS/SSL application hosts use separate digital certificates as a basis for authentication in both directions: to prove their own identity to the other party, and to verify the identity of the other party. In proving its own authenticity, the PremierWave EN embedded system on module will use its own "personal" certificate. In verifying the authenticity of the other party, the PremierWave EN device will use a "trusted authority" certificate.

In short:

- ◆ When using EAP-TLS, the PremierWave EN embedded system on module needs a personal certificate with matching private key to identify itself and sign its messages.
- ◆ When using EAP-TLS, EAP-TTLS or PEAP, the PremierWave EN unit needs the authority certificate(s) that can authenticate those it wishes to communicate with.

Digital Certificates

The goal of a certificate is to authenticate its sender. It is analogous to a paper document that contains personal identification information and is signed by an authority, for example a notary or government agency. With digital certificates, a cryptographic key is used to create a unique digital signature.

Trusted Authorities

A private key is used by a trusted certificate authority (CA) to create a unique digital signature. Along with this private key is a certificate of authority, containing a matching public key that can be used to verify the authority's signature but not re-create it.

A chain of signed certificates, anchored by a root CA, can be used to establish a sender's authenticity. Each link in the chain is certified by a signed certificate from the previous link, with the exception of the root CA. This way, trust is transferred along the chain, from the root CA through any number of intermediate authorities, ultimately to the agent that needs to prove its authenticity.

Obtaining Certificates

Signed certificates are typically obtained from well-known CAs, such as VeriSign, Inc. This is done by submitting a certificate request for a CA, typically for a fee. The CA will sign the certificate request, producing a certificate/key combo: the certificate contains the identity of the owner and the public key, and the private key is available separately for use by the owner.

As an alternative to acquiring a signed certificate from a CA, you can act as your own CA and create self-signed certificates. This is often done for testing scenarios, and sometimes for closed environments where the expense of a CA-signed root certificate is not necessary.

Self-Signed Certificates

A few utilities exist to generate self-signed certificates or sign certificate requests. The PremierWave EN embedded system on module also has the ability to generate its own self-signed certificate/key combo. You can use XML to export the certificate in PEM format, but you cannot export the key. Hence, the internal certificate generator can only be used for certificates that are to identify that particular PremierWave EN module.

Certificate Formats

Certificates and private keys can be stored in several file formats. Best known are PKCS12, DER and PEM. Certificate and key can be in the same file or in separate files. Additionally, the key can be either be encrypted with a password or left in the clear. However, PremierWave EN embedded system on module currently only accepts separate PEM files, with the key unencrypted.

Several utilities exist to convert between the formats.

OpenSSL

OpenSSL is a widely used open source set of SSL related command line utilities. It can act as server or client. It can also generate or sign certificate requests, and can convert from and to several different of formats.

OpenSSL is available in binary form for Linux and Windows.

To generate a self-signed RSA certificate/key combo:

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

See www.openssl.org or www.madboa.com/geek/openssl for more information.

Note: *Signing other certificate requests is also possible with OpenSSL but the details of this process are outside the scope of this document.*

Steel Belted RADIUS

Steel Belted RADIUS is a commercial RADIUS server from Juniper Networks that provides a GUI administration interface. It also provides a certificate request and self-signed certificate generator.

The self-signed certificate has extension .sbrpvk and is in the PKCS12 format. OpenSSL can convert this into a PEM format certificate and key:

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

The sbr_certkey.pem file contains both certificate and key. If loading the SBR certificate into an PremierWave EN embedded system on module as an authority, you will need to edit it:

1. Open the file in any plain text editor.
2. Delete all info before "----- BEGIN CERTIFICATE-----" and after "----- END CERTIFICATE-----", and then save as sbr_cert.pem.

SBR accepts trusted-root certificates in the DER format. Again, OpenSSL can convert any format into DER:

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

Note: *With SBR, when the identity information includes special characters such as dashes and periods, SBR changes the format it uses to store these strings and becomes incompatible with the current PremierWave EN embedded system on module release. Support may be added for this and other formats in future releases.*

Free RADIUS

Note: Free RADIUS is another versatile Linux open-source RADIUS server.

SSH Settings

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

Configuration is required when the PremierWave EN device is either (1) the SSH server or (2) an SSH client. The SSH server is used by the CLI (Command Mode) and for tunneling in Accept Mode. The SSH client is for tunneling in Connect Mode.

To configure the PremierWave EN embedded system on module as an SSH server, there are two requirements:

- ◆ **Defined Host Keys:** both private and public keys are required. These keys are used for the Diffie-Hellman key exchange (used for the underlying encryption protocol).
- ◆ **Defined Users:** these users are permitted to connect to the PremierWave EN device SSH server.

SSH Server Host Keys

The SSH Server Host Keys are used by all applications that play the role of an SSH Server. Specifically Tunneling in Accept Mode. These keys can be created elsewhere and uploaded to the device or automatically generated on the device.

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

Note: Some SSH Clients require RSA Host Keys to be at least 1024 bits in size.

Table 11-1 SSH Server Host Keys

SSH Settings	Description
Private Key	Click Choose File to browse to and select the existing private key you want to upload. In Web Manager, you can also browse to the private key to be uploaded. Be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.
Public Key	Click Choose File to browse to and select the existing public key you want to upload. In Web Manager, you can also browse to the public key to be uploaded.
Key Type	Select a key type to use for the new key: <ul style="list-style-type: none"> ◆ RSA ◆ DSA
Bit Size	Select a bit length for the new key: <ul style="list-style-type: none"> ◆ 512 ◆ 768 ◆ 1024
Submit (button)	Click the Submit button after setting the information for Upload Keys or Create New Keys .

Note: SSH Keys from other programs may be converted to the required PremierWave EN unit format. Use Open SSH to perform the conversion.

SSH Client Known Hosts

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

Table 11-2 SSH Client Known Hosts

SSH Settings	Description
Server	Specify either a DNS Hostname or IP Address when adding public host keys for a Server. This Server name should match the name used as the Remote Address in Connect Mode Tunneling.
Public RSA Key	Click Choose File to browse to and select the existing public RSA key you want to use with this user. In Web Manager, you can also browse to the public RSA key to be uploaded. If authentication is successful with the key, no password is required.
Public DSA Key	Click Choose File to browse to and select the existing public DSA key you want to use with this user. In Web Manager, you can also browse to the public DSA key to be uploaded. If authentication is successful with the key, no password is required.
Submit (button)	Click the Submit button after setting the information for SSH Client: Known Hosts .

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

SSH Server Authorized Users

The SSH Server Authorized Users are used by all applications that play the role of an SSH Server and specifically Tunneling in Accept Mode. Every user account must have a Password.

The user's Public Keys are optional and only necessary if public key authentication is wanted. Using public key authentication will allow a connection to be made without the password being asked at that time.

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

Table 11-3 SSH Server Authorized Users

SSH Settings	Description
Username	Enter a new username or edit an existing one.
Password	Enter a new password or edit an existing one.
Public RSA Key	Click Choose File to browse to and select the existing public RSA key you want to use with this user. In Web Manager, you can also browse to the public RSA key to be uploaded. If authentication is successful with the key, no password is required.
Public DSA Key	Click Choose File to browse to and select the existing public DSA key you want to use with this user. In Web Manager, you can also browse to the public DSA key to be uploaded. If authentication is successful with the key, no password is required.
Add/Edit (key)	Click the Add/Edit button after setting the information for SSH Client: Authorized Users .

SSH Client Users

The SSH Client Users are used by all applications that play the role of an SSH Client. Specifically Tunneling in Connect Mode. To configure the PremierWave EN embedded system on module as an SSH client, an SSH client user must be both configured and also exist on the remote SSH server.

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

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

The default Remote Command is '<Default login shell>' which tells the SSH Server to execute a remote shell upon connection. This can be changed to anything the SSH Server on the remote host can execute.

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

Table 11-4 SSH Client Users

SSH Settings	Description
Username	Enter the name that the device uses to connect to an SSH server.
Password	Enter the password associated with the username.
Remote Command	Enter the command that can be executed remotely. Default is shell, which tells the SSH server to execute a remote shell upon connection. This command can be changed to anything the remote host can perform.
Private Key	Click Choose File to browse to and select the existing private key you want to upload. In Web Manager, you can also browse to the private key to be uploaded. Be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.
Public Key	Click Choose File to browse to and select the existing public key you want to upload. In Web Manager, you can also browse to the public key to be uploaded.
Key Type	Select a bit length for the key: <ul style="list-style-type: none"> ◆ RSA ◆ DSA
Add/Edit (button)	Click the Add/Edit button after completing the Username, Password, and Remote Command fields above, and selecting the key and key type.

Table 11-5 Create New Keys

SSH Settings	Description
Username	Enter the name that the device uses to connect to an SSH server.
Key Type	Select a bit length for the key: <ul style="list-style-type: none"> ◆ RSA ◆ DSA

SSH Settings	Description
Bit Size	<p>Select the bit length of the new key:</p> <ul style="list-style-type: none"> ◆ 512 ◆ 768 ◆ 1024 <p>Using a larger Bit Size takes more time to generate the key. Approximate times are:</p> <ul style="list-style-type: none"> ◆ 1 second for a 512 bit RSA key ◆ 1 second for a 768 bit RSA key ◆ 1 second for a 1024 bit RSA key ◆ 2 seconds for a 512 bit DSA key ◆ 2 seconds for a 768 bit DSA key ◆ 20 seconds for a 1024 bit DSA key <p>Note: Some SSH clients require RSA host keys to be at least 1024 bits long. This device generates keys up to 2048 bits long.</p>
Submit (button)	Click the Submit button after entering the information for the new key.

To Configure SSH Settings

Using Web Manager

- ◆ To configure SSH, click **SSH** in the menu.

Using the CLI

- ◆ To enter the SSH command level: `enable -> ssh`

Using XML

- ◆ Include in your file:

```
<configgroup name="ssh server">
                                and
                                <configgroup name="ssh client">
```

SSL Settings

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

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

Note: The blue text in the XML command strings of this chapter are to be replaced with a user-specified name.

Create a New Credential

After creating a new credential, you can either establish your credential through [Certificate and Key Generation](#) or [Upload Certificate](#).

Table 11-6 Create a New Credentials

Upload Field	Description
Create new credential	Enter the name of the new credential to be created.
Submit (button)	Click the Submit button after entering the new credential name.

To Create a New Credential

Using Web Manager

- ◆ To create a new credential, click **SSL** in the menu and select **Credentials**.

Using the CLI

- ◆ To enter the SSL command level: `enable -> ssl`
- ◆ To enter the Credentials command level: `enable -> ssl -> credentials`

Using XML

- ◆ Not applicable.

Upload Certificate

SSL certificates identify the PremierWave EN embedded system on module to peers, and can be used with some methods of wireless authentication. Certificate and key pairs can be uploaded to the PremierWave EN unit through either the CLI or XML import mechanisms. Certificates can be identified on the PremierWave EN embedded system on module by a name provided at upload time.

Table 11-7 Upload Certificate Settings

Upload Certificate Settings	Description
New Certificate	Click Choose File to browse to and select the new certificate file to be uploaded. The SSL certificate to be uploaded. RSA or DSA certificates are allowed. The format of the certificate must be PEM. It must start with “-----BEGIN CERTIFICATE-----” and end with “-----END CERTIFICATE-----”. Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.
New Certificate Type	Choose the new certificate type to be uploaded: <ul style="list-style-type: none"> ◆ PEM ◆ PKCS7 ◆ PKCS12

Upload Certificate Settings (continued)	Description
New Private Key	Click Choose File to browse to and select the certificate type being uploaded. The key needs to belong to the certificate entered above. The format of the file must be PEM. It must start with “-----BEGIN RSA PRIVATE KEY-----” and end with “-----END RSA PRIVATE KEY-----”. Read DSA instead of RSA in case of a DSA key. Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.
New Key Type	Click Choose File to browse to and select the key type being uploaded: <ul style="list-style-type: none"> ◆ PEM ◆ Encrypted PEM ◆ PKCS12
Submit (button)	Click the Submit button after selecting the certificate and private key information for the uploaded certificate.

Certificate and Key Generation

The PremierWave EN embedded system on module can generate self signed certificates and their corresponding keys. This can be done for both the rsa and dsa certificate formats. Certificates can be identified on the PremierWave EN unit by a name provided at generation time.

Table 11-8 Certificate and Key Generation Settings

Certificate Generation Settings	Description
Country (2 Letter Code)	Enter the 2-letter country code to be assigned to the new self-signed certificate. Examples: US for United States and CA for Canada
State/Province	Enter the state or province to be assigned to the new self-signed certificate.
Locality (City)	Enter the city or locality to be assigned to the new self-signed certificate.
Organization	Enter the organization to be associated with the new self-signed certificate.
Organization Unit	Enter the organizational unit to be associated with the new self-signed certificate.
Common Name	Enter the common name to be associated with the new self signed certificate, preferably matching the host name or the ip address of the device, whichever will be the intended access approach. This is a required field.
Expires	Enter the expiration date, in mm/dd/yyyy format, for the new self-signed certificate. Example: An expiration date of May 9, 2018 is entered as 05/09/2018.
Type	Select the type of key: <ul style="list-style-type: none"> ◆ RSA = Public-Key Cryptography algorithm based on large prime numbers, invented by Rivest Shamir and Adleman. Used for encryption and signing. ◆ DSA = Digital Signature Algorithm also based on large prime numbers, but can only be used for signing. Developed by the US government to avoid the patents on RSA.

Certificate Generation Settings (continued)	Description
Key Length	Select the bit size of the new self-signed certificate. Choices are: <ul style="list-style-type: none"> ◆ 512 bit ◆ 768 bit ◆ 1024 bit ◆ 2048 bit ◆ 4096 bit The larger the bit size, the longer it takes to generate the key.
Submit (button)	Click the Submit button after setting the information for new self-signed certificate.

To Configure an Existing SSL Credential

Follow these steps after a new credential has been established via [Create a New Credential on page 104](#).

Using Web Manager

- ◆ To configure an existing SSL Credential, click **SSL** in the menu, select **Credentials**, and click on the name of an existing SSL credential.

Using the CLI

- ◆ To enter the SSL command level: `enable -> ssl`
- ◆ To enter the Credential command level: `enable -> ssl -> credentials`

Using XML

- ◆ Include in your file:

```
<configgroup name="ssl">
and <configitem name="credentials" instance="name">
and <value name="RSA certificate"/> OR <value name="DSA certificate"/>
```

Trusted Authorities

One or more authority certificates are needed to verify a peer's identity. Authority certificates are used with some wireless authentication methods. These certificates do not require a private key.

Trusted Authorities Settings	Description
Authority	Click Choose File to browse to and select the SSL authority certificate. RSA or DSA certificates are allowed. The format of the authority certificate can be PEM or PKCS7. PEM files must start with "-----BEGIN CERTIFICATE-----" and end with "-----END CERTIFICATE-----". Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.

Trusted Authorities Settings (continued)	Description
Authority Certificate Type	This field will be automatically updated depending upon extension of the certificate entered. If the field is NONE i.e., certificate is not supported then it will not load. If the field is PKCS12, then PKCS12 password should be entered in the Password field.
Delete	Click the Delete button beside a specific certificate authority to delete it.
Delete All	Click the Delete All button to delete all existing certificate authorities.

Using Web Manager

- ◆ To upload an Authority Certificate, click **SSL** in the menu and select **Trusted Authorities**.

Using the CLI

- ◆ To enter the SSL command level: `enable -> ssl`
- ◆ To enter the Trusted Authorities command level: `enable -> ssl -> trusted authorities`

Using XML

- ◆ Include in your file:


```
<configgroup name="ssl">
and <configitem name="trusted authority" instance="1">
and <configitem name="intermediate authority" instance="1">
```

12: Maintenance and Diagnostics Settings

Filesystem Settings

Use the file system to list, view, create, upload, copy, move, remove, and transfer files. The PremierWave EN embedded system on module uses a flash file system to store files.

Statistics

The filesystem statistics page displays statistics and current usage information of the flash filesystem. The filesystem can be formatted here.

Warning: *Formatting the filesystem will delete all files on it.*

When the USB drive is connected to one of the two USB ports on the device, it will be automatically mounted and accessed using the filesystem. USB drives can be simultaneously connected to both the USB ports.

Table 12-1 File Statistics

Filesystem Commands	Description
Format	Displays a list of files on the PremierWave EN device, and their respective sizes.

To View Statistics

Using Web Manager

- ◆ To view statistics, format the filesystem or configure USB auto mount features, click **Filesystem** in the menu and select **Statistics**.

File Display

View the list of existing files and their contents in the ASCII or hexadecimal formats.

Table 12-2 File Display Settings

File Display Commands	Description
ls	Displays a list of files on the PremierWave EN device, and their respective sizes.
cat	Displays the specified file in ASCII format.
dump	Displays the specified file in a combination of hexadecimal and ASCII formats.
pwd	Print working directory.
cd	Change directories.
show tree	Display file/directory tree.

To Display Files

Using Web Manager

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

Using the CLI

- ◆ To enter the Filesystem command level: `enable -> filesystem`

Using XML

- ◆ Not applicable.

File Modification

The PremierWave EN embedded system on module allows for the creation and removal of files on the Filesystem.

Table 12-3 File Modification Settings

File Modification Commands	Description
rm	Removes the specified file from the file system.
touch	Creates the specified file as an empty file.
cp	Creates a copy of a file.
mkdir	Creates a directory on the file system.
rmdir	Removes a directory from the file system.
format	Format the file system and remove all data.

File Transfer

Files can be transferred to and from the PremierWave EN device via the TFTP protocol. This can be useful for saving and restoring XML configuration files. Files can also be uploaded via HTTP.

Table 12-4 File Transfer Settings

File Transfer Settings	Description
Create	Type in a File or Directory name and click the Create button. The newly created File or Directory will appear above.
Upload File	Click Choose File to browse to location of the file to be uploaded via HTTP. Click Upload to upload the chosen file.
Copy File	Enter the Source and Destination name for file to be copied and click the Copy button.
Move	Enter the Source and Destination name for file to be moved and click the Move button.

File Transfer Settings	Description
TFTP	
Action	Select the action that is to be performed via TFTP: <ul style="list-style-type: none"> ◆ Get = a “get” command will be executed to store a file locally. ◆ Put = a “put” command will be executed to send a file to a remote location.
Local File	Enter the name of the local file on which the specified “get” or “put” action is to be performed.
Remote File	Enter the name of the file at the remote location that is to be stored locally (“get”) or externally (“put”).
Host	Enter the IP address or name of the host involved in this operation.
Port	Enter the number of the port involved in TFTP operations.
Transfer (button)	Click the Transfer button after TFTP settings are entered.

To Transfer or Modify Filesystem Files

Using Web Manager

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

Using the CLI

- ◆ To enter the Filesystem command level: `enable -> filesystem`

Using XML

- ◆ Not applicable.

Protocol Stack Settings

There are various low level network stack specific items that are available for configuration. This includes settings related to IP, ICMP, ARP and SMTP, which are described in the sections below.

IP Settings

Table 12-5 IP Protocol Stack Settings

Protocol Stack IP Settings	Description
IP Time to Live	This value typically fills the Time To Live in the IP header. SNMP refers to this value as "ipDefaultTTL". Enter the number of hops to be transmitted before the packet is discarded.

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

To Configure IP Protocol Stack Settings

Using Web Manager

- ◆ To configure IP protocol settings, click **Protocol Stack** in the menu and select **IP**.

Using the CLI

- ◆ To enter the command level: `enable -> config -> ip`

Using XML

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

ICMP Settings

Table 12-6 ICMP Protocol Stack Settings

Protocol Stack ICMP Settings	Description
State	Click to enable or disable the processing of ICMP messages. This includes both incoming and outgoing messages.

To Configure ICMP Protocol Stack Settings

Using Web Manager

- ◆ To configure ICMP protocol settings, click **Protocol Stack** in the menu and select **ICMP**.

Using the CLI

- ◆ To enter the command level: `enable -> config -> icmp`

Using XML

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

To View ICMP Protocol Stack Settings

Using Web Manager

- ◆ To view ICMPv6 protocol settings, click **Protocol Stack** in the menu and select **ICMPv6**.

Using the CLI

- ◆ Not applicable.

Using XML

- ◆ Not applicable.

ARP Settings**Table 12-7 ARP Protocol Stack Settings**

Protocol Stack ARP Settings	Description
IP Address	Enter the IP address to add to the ARP cache. After entering the MAC address, click the Add button.
MAC Address	Enter the MAC address to add to the ARP cache. After also entering the IP address, click the Add button.
Add (button)	Click the Add button after entering the ARP Cache information.
Remove	Click the Remove link beside a specific address to remove it.
Remove All	Click the Remove All link underneath all listed addresses to remove all the addresses.

To Configure ARP Network Stack Settings**Using Web Manager**

- ◆ To configure ARP protocol settings, click **Protocol Stack** in the menu and select **ARP**.

Using the CLI

- ◆ To enter the command level: `enable -> config -> arp`

Using XML

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

Diagnostics

The PremierWave EN embedded system on module has several tools for diagnostics and statistics. Various options allow for the configuration or viewing of IP socket information, ping, traceroute, memory, and processes.

Hardware

To View Hardware Information

Using Web Manager

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

Using the CLI

- ◆ To enter the command level: `enable -> device, show hardware information`

Using XML

- ◆ Include in your file: `<statusgroup name="hardware">`

IP Sockets

You can view the list of listening and connected IP sockets.

To View the List of IP Sockets

Using Web Manager

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

Using the CLI

- ◆ To enter the command level: `enable, show ip sockets`

Using XML

- ◆ Include in your file: `<statusgroup name="ip sockets">`

Ping

The ping command can be used to test connectivity to a remote host.

Table 12-8 Ping Settings

Diagnostics: Ping Settings	Description
Host	Enter the IP address or host name for the PremierWave unit to ping.
Count	Enter the number of ping packets PremierWave device should attempt to send to the Host . The default is 5 .

Diagnostics: Ping Settings (continued)	Description
Timeout	Enter the time, in seconds, for the PremierWave to wait for a response from the host before timing out. The default is 5 seconds.
Submit (Button)	Click the Submit button after entering ping information.

To Ping a Remote Host

Using Web Manager

- ◆ To ping a Remote Host, click **Diagnostics** in the menu and select **Ping**.

Using the CLI

- ◆ To enter the command level: `enable, ping <host> <count> <timeout>`

Using XML

- ◆ Not applicable.

Traceroute

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

Table 12-9 Traceroute Settings

Diagnostics: Traceroute Settings	Description
Host	Enter the IP address or DNS hostname. This address is used to show the path between it and the PremierWave device when issuing the traceroute command.
Protocol	Select the traceroute protocol from the drop-down menu.
Submit (button)	Click the Submit button after entering traceroute information.

To Perform a Traceroute

Using Web Manager

- ◆ To perform a Traceroute, click **Diagnostics** in the menu and select **Traceroute**.

Using the CLI

- ◆ To enter the command level: `enable, trace route <host>`

Using XML

- ◆ Not applicable.

Log

Table 12-10 Log Settings

Diagnostics: Log	Description
Log Output	Select a diagnostic log output type: <ul style="list-style-type: none"> ◆ Disable - Turn off the logging feature. ◆ Filesystem - Directs logging to /log.txt. ◆ Line (1, 2 or 3) - Directs logging to the selected serial line.
Log Max Length	Set the maximum length of the log.txt file in Kbytes. <i>Note: This setting becomes available when Filesystem is selected.</i>
Log Verbosity Level	Select the Verbosity Level from the drop-down menu to specify the verbosity of system messages logged to the Syslog Host.

To Configure the Diagnostic Log Output

Using Web Manager

- ◆ To configure the Diagnostic Log output, click **Diagnostics** in the menu and select **Log**.

Using the CLI

- ◆ To enter the command level: `enable -> config -> diagnostics -> log`

Using XML

- ◆ Include in your file:


```
<configgroup name="diagnostics">
and
<configitem name="log">
```

Memory

The memory information shows the total, used, and available memory (in kilobytes).

To View Memory Usage

Using Web Manager

- ◆ To view memory information, click **Diagnostics** in the menu and select **Memory**.

Using the CLI

- ◆ To enter the command level: `enable -> device, show memory`

Using XML

- ◆ Include in your file: `<statusgroup name="memory">`

Processes

The PremierWave EN device shows all the processes currently running on the system. It shows the Process ID (PID), Parent Process ID (PPID), user, CPU percentage, percentage of total CPU cycles, and process command line information.

To View Process Information

Using Web Manager

- ◆ To view process information, click **Diagnostics** in the menu and select **Processes**.

Using the CLI

- ◆ To enter the command level: `enable, show processes`

Using XML

- ◆ Include in your file: `<statusgroup name="processes" >`

Threads

The PremierWave unit threads information shows details of threads in the `ltrx_evo` task which can be useful for technical experts in debugging.

To View Thread Information

Using Web Manager

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

Using the CLI

- ◆ To enter the command level: `enable -> device, show task state`

Clock

The Clock settings page can be updated by one of three methods: manually entering the date and time, synchronizing with the SNTP, or synchronizing with the wireless network server. If the network synchronization method is selected, the user can also choose the time zone to be detected automatically.

Table 12-11 Clock Settings

Clock	Description
Method	Select a clock change method from the drop-down menu: <ul style="list-style-type: none"> ◆ Manual: this option allows you to directly set the date and time. ◆ SNTP: this option keeps the time synchronized with the NTP Server. ◆
Date	Use the drop-down menu to select the Year , Month and Day . This option becomes available when the Manual method is selected.

Time (24 hour)	Use the drop-down menu to select the Hour , Min and Sec . This option becomes available when the Manual method is selected.
NTP Server	Set NTP Server to an NTP server's IP address or hostname. This option becomes available when the SNTP method is selected.
Time Zone	Select the geographical time zone from the drop-down list.

To Specify Clock Setting Method

Using Web Manager

- ◆ To view thread information, click **Clock** in the menu.

Using the CLI

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

Using the XML

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

System Settings

The PremierWave EN embedded system on module system settings allow for rebooting the device, restoring factory defaults, uploading new firmware and updating a system's short and long name.

Note: *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 12-12 System Settings

System Settings	Description
State	Click to enable or disable the reboot schedule.
Current date and time	Displays the current date and time.
Schedule	Select the Daily or Interval schedule from the drop-down menu.
Time (24 hour)	Enter the Hour and Min (minute) in 24 hour time, for the reboot time if Daily schedule is selected.
Interval	Enter the interval number and select the interval type (Hours , Days , or Weeks) from the drop-down menu.
Reboot Device	Click the Reboot button to reboot the device.
Restore Factory Defaults	Click Factory Defaults to restore the device to the original factory settings. All configuration will be lost. The PremierWave unit automatically reboots upon setting back to the defaults.

System Settings	Description
Upload New Firmware	Upload new firmware to the PremierWave unit by clicking Choose File to browse to the new firmware file, and click Upload button to upload the chosen file to the system. The device automatically reboots upon the installation of new firmware.
Short Name	Enter a short name for the system name. A maximum of 32 characters are allowed.
Long Name	Enter a long name for the system name. A maximum of 64 characters are allowed.
Submit (button)	Click Submit after entering the system name.

To Reboot or Restore Factory Defaults

Using Web Manager

- ◆ To access the area with options to reboot, restore to factory defaults, upload new firmware, update the system name (long or short names) or to view the current configuration, click **System** in the menu.

Using the CLI

- ◆ To enter the command level: `enable`

Using XML

- ◆ Include in your file: `<configgroup name="xml import control">`

13: Management Interface Settings

Command Line Interface Settings

The Command Line Interface settings allow you to control how users connect to and interact with the command line of the PremierWave EN embedded system on module. It is possible to configure access via the Telnet and SSH protocols, in addition to general CLI options.

Basic CLI Settings

The basic CLI settings control general CLI access and usability options.

Table 13-1 CLI Configuration Settings

Command Line Interface Configuration Settings	Description
Login Password	Enter the password for the admin account. "PASS" is the default password.
Enable Level Password	Enter the password for access to the Command Mode Enable level. There is no password by default.
Quit Connect Line	Enter the Quit Connect Line string to be used to terminate a Telnet and SSH session and resume the CLI. Type <control> before the key to be pressed while holding down the [Ctrl] key (example: <control>L)
Inactivity Timeout	Set a time period in which the CLI session should disconnect if no data is received. Enter 0 to disable. Blank the display field to restore the default.
Line Authentication	Select to enable or disable authentication for CLI access on the serial lines.

To View and Configure Basic CLI Settings

Using Web Manager

- ◆ To view CLI statistics, click **CLI** in the menu and select **Statistics**.
- ◆ To configure basic CLI settings, click **CLI** in the menu and select **Configuration**.

Using the CLI

- ◆ To enter CLI command level: `enable -> config -> cli`

Using XML

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

Telnet Settings

The Telnet settings control CLI access to the PremierWave EN embedded system on module telnet over the Telnet protocol.

Table 13-2 Telnet Settings

Telnet Settings	Description
Telnet State	Select to enable or disable CLI access via Telnet
Telnet Port	Enter an alternative Telnet Port to override the default used by the CLI server. Blank the field to restore the default.
Telnet Max Sessions	Specify the maximum number of concurrent Telnet sessions that will be allowed.
Telnet Authentication	Select to enable or disable authentication for Telnet logins.

To Configure Telnet CLI Settings

Using Web Manager

- ◆ To configure Telnet settings, click **CLI** in the menu and select **Configuration**.

Using the CLI

- ◆ To enter the Telnet command level: `enable -> config -> cli -> Telnet`

Using XML

- ◆ Include in your file:


```
<configgroup name="Telnet">
and
<configitem name="state">
and
<configitem name="authentication">
```

SSH CLI Settings

The SSH settings control CLI access to the PremierWave EN device over the SSH protocol.

Table 13-3 SSH Settings

SSH Settings	Description
SSH State	Select to enable or disable CLI access via SSH.
SSH Port	Specify the SSH Port and override the default, as needed. Blank the field to restore the default.
SSH Max Sessions	Specify the maximum number of concurrent SSH sessions that will be allowed.

To Configure SSH Settings

Using Web Manager

- ◆ To configure SSH settings, click **CLI** in the menu and select **Configuration**.

Using the CLI

- ◆ To enter the SSH command level: `enable -> config -> cli -> ssh`

Using XML

- ◆ Include in your file:

```
<configgroup name="ssh"> and <configitem name="state">
```

XML Settings

The PremierWave EN embedded system on module allows for the configuration of units using an XML configuration record (XCR). Export a current configuration for use on other PremierWave EN unit or import a saved configuration file.

XML: Export Configuration

You can export the current system configuration in XML format. The generated XML file can be imported later to restore a configuration. It can also be modified and imported to update the configuration on this PremierWave EN unit or another. The XML data can be dumped to the screen or exported to a file on the file system.

By default, all groups are exported. You may also select a subset of groups to export.

Table 13-4 XML Exporting Configuration

XML Export Configuration Settings	Description
Export to browser	Select this option to export the XCR data in the selected fields to the browser. Use the "xcr dump" command to export the data to the browser.
Export to local file	Select this option to export the XCR data to a file on the device. If you select this option, enter a file name for the XML configuration record. Use the "xcr export" command to export the data to a local file.
Export secrets	Select to export secret password and key information. Use only with a secure link, and save only in secure locations. Note: Only use with extreme caution.
Comments	Select this option to include descriptive comments in the XML.
Lines to Export	Select instances to be exported in the line, serial, tunnel and terminal groups. Click Clear All to clear all checkmarks, or Select All to check all checkmarks.

XML Export Configuration Settings (continued)	Description
Groups to Export	Check the configuration groups that are to be exported to the XML configuration record. The group list should be comma delimited and encased in double quotes. The list of available groups can be viewed with the “xcr list” command. Click Clear All to clear all checkmarks, or Select All but Networking to check all checkmarks except Networking.
Export (button)	Click Export after selecting the XML: Export Configuration settings.

To Export Configuration in XML Format

Using Web Manager

- ◆ To export configuration format, click **XML** in the menu and select **Export Configuration**.

Using the CLI

- ◆ To enter the XML command level: `enable -> xml`

Using XML

- ◆ Not applicable.

XML: Export Status

You can export the current status in XML format. By default, all groups are exported. You may also select a subset of groups to export.

Table 13-5 Exporting Status

XML Export Status Settings	Description
Export to browser	Select this option to export the XCR data in the selected fields to the browser. Use the “xcr dump” command to export the data to the browser.
Export to local file	Select this option to export the XCR data to a file on the device. If you select this option, enter a file name for the XML configuration record. Use the “xcr export” command to export the data to a local file.
Lines to Export	Select instances to be exported in the line, serial, tunnel and terminal groups. Click Clear All to clear all checkmarks, or Select All to check all checkmarks.
Groups to Export	Check the configuration groups that are to be exported to the XML configuration record. The group list should be comma delimited and encased in double quotes. The list of available groups can be viewed with the “xcr list” command. Click Clear Click Clear All to clear all checkmarks, or Select All to check all checkmarks.
Export (button)	Click Export after selecting the XML: Export Status settings.

To Export in XML Format

Using Web Manager

- ◆ To export configuration format, click **XML** in the menu and select **Export Status**.

Using the CLI

- ◆ To enter the XML command level: `enable -> xml`

Using XML

- ◆ Not applicable.

XML: Import Configuration

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

The XML data can be imported from a file on the file system or pasted into a CLI session. The groups to import can be specified at the command line, the default is all groups.

Configuration from External File

This import option requires entering the path and file name of the external XCR file you want to import.

Configuration from Filesystem

This import option picks up settings from a file and your import selections of groups, lines, and instances. The list of files can be viewed from the filesystem level of the CLI.

Line(s) from single line Settings on the Filesystem

This import option copies line settings from an the input file containing only one Line instance to all of the selected Lines.

Table 13-6 Import Configuration from Filesystem Settings

Import Configuration from Filesystem Settings	Description
Filename	Enter the name of the file on the PremierWave unit (local to its filesystem) that contains XCR data.
Lines to Import	Select filter instances to be imported in the line, serial, tunnel and terminal groups. This affects both Whole Groups to Import and Text List selections. Click Clear All to clear all checkmarks, or Select All to check all checkmarks.
Whole Groups to Import	Select the configuration groups to import from the XML configuration record. This option imports all instances of each selected group. Click Clear All to clear all checkmarks, or Select All but Networking to check all checkmarks except Networking.
Import (button)	Click Import after selecting the XML: Import Configuration settings.

To Import Configuration in XML Format

Using Web Manager

- ◆ To import configuration, click **XML** in the menu and select **Import Configuration**.

Using the CLI

- ◆ To enter the XML command level: `enable -> xml`

Using XML

- ◆ Not applicable.

14: Bridging

The PremierWave EN embedded device server supports bridging of traffic between a single external Ethernet device and the wireless network. When bridging is enabled and active, the MAC address of the external device is used as the MAC address for the WLAN interface. The PremierWave EN unit then bridges traffic between the two interfaces. The external Ethernet device appears as a wireless node on the network.

When bridging is enabled, the concept of the Primary Interface is introduced. The Primary Interface is the interface over which all device features and services operate, as if bridging were not enabled. FTP, Telnet/SSH CLI, HTTP, 77FE, etc, all may be accessed as usual over the Primary Interface. The Primary Interface dynamically switches between eth0 and wlan0, depending on the state of the Ethernet physical link. If the Ethernet link is up, eth0 is the Primary Interface; otherwise, wlan0 is the Primary Interface.

When bridging is enabled, operation of Network 1 (eth0) and Network 2 (wlan0) are overridden and controlled by the bridging subsystem. Each Network Interface's own configuration is used when it becomes the Primary Interface. Network 1 (eth0) and Network 2 (wlan0) Link Configuration settings are still used to configure and control the physical links.

Bridging Configuration

To configure and enable bridging:

1. Configure Network 1 (eth0) and Network 2 (wlan0) Interface settings, which will be used for the Primary Interface. For example,
 - ◆ DHCP Disabled
 - ◆ IP Address 192.168.1.100/24
 - ◆ Default Gateway 192.168.1.1
2. Configure Network 1 (eth0) Link settings, if desired. These include the Ethernet link speed and duplex.
3. Configure Network 2 (wlan0) Link settings as desired for connection to a wireless network. Primarily, configure the WLAN Profile(s) for connection to the wireless network.
4. Create the corresponding WLAN Profile(s) under WLAN Profiles.

At this point, it is a good idea to ensure that the PremierWave EN device can connect to your wireless network, before enabling bridging. Check your WLAN settings by continuing with the following steps:

5. Enable Network 2 (wlan0) and Disable Network 1 (eth0).
6. Configure Network 2 (wlan0) Interface settings as desired.
7. Reboot.
8. Verify the wireless connection.
9. Enable Bridge 1 (br0).
10. Optionally configure the Bridge 1 Bridging MAC Address.
11. Reboot for changes to take effect.

Bridging Operation

During initialization, both eth0 and wlan0 are enabled and controlled by the bridging subsystem. Important aspects to keep in mind:

- ◆ If eth0 physical link is down, wlan0 is the Primary Interface.
- ◆ If eth0 physical link is up, eth0 is the Primary Interface.

When eth0 link is up, wlan0 link is established, and the Bridging MAC Address is acquired (via pre-configuration or auto-detection), Bridging enters the Active state. If either link goes down, bridging falls back to the Inactive state.

When in the **Active** state, all packets that arrive on the wlan0 interface are bridged out the eth0 interface. Similarly, all packets that arrive on the eth0 interface are bridged out the wlan0 interface. However, exceptions to this behavior include:

- ◆ Ethernet packets directed specifically to the Ethernet (eth0) MAC Address are terminated internally and are not bridged to WLAN.
- ◆ ARP Requests for the Primary Interface's IP address are terminated internally and are not bridged to WLAN
- ◆ Ethernet packets which are not originated from the Bridging MAC Address are discarded

Bridge Configuration

A bridge may be configured between an Ethernet interface and a WLAN interface. A bridge represents a relationship between the interface minor numbers. For example, br0 is a bridge between eth0 and wlan0.

Table 14-1 Bridge Settings

WLAN Profile WPA & WPA2 Settings	Description
State	Select to enable or disable bridging.
Bridging MAC Address	Specify the MAC address of bridgeable traffic between the Ethernet and WLAN interfaces. When bridging is active, this MAC Address will be used as the MAC address of the WLAN interface. Packets received on the Ethernet interface from this address will be bridged to the WLAN interface (except traffic directed at the Primary Interface). If this field is not configured, then the device waits for the first packet to arrive on the Ethernet interface and uses the source address as the bridging address. <i>Note: if a Bridging MAC Address is not configured, then once it is obtained and configured dynamically, it remains in effect until a reboot.</i>

To View or Configure Bridge Settings

Using Web Manager

- ◆ To view the Bridge status, click **Bridge** on the menu, select a particular bridge and click **Status**.
- ◆ To configure Bridge settings, click **Bridge** on the menu, select a particular bridge and click **Configuration**.

Using the CLI

- ◆ To enter the Bridge command level: enable -> config -> bridge 1 or enable -> config -> bridge br0

Using XML

- ◆ Include in your file: <configgroup name="bridge" instance="br0">

15: Security in Detail

Public Key Infrastructure

Public key infrastructure (PKI) is based on an encryption technique that uses two keys: a public key and private key. Public keys can be used to encrypt messages which can only be decrypted using the private key. This technique is referred to as asymmetric encryption, as opposed to symmetric encryption, in which a single secret key is used by both parties.

TLS (SSL)

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), use asymmetric encryption for authentication. In some scenarios, only a server needs to be authenticated, in others both client and server authenticate each other. Once authentication is established, clients and servers use asymmetric encryption to exchange a secret key. Communication then proceeds with symmetric encryption, using this key.

SSH and some wireless authentication methods on the PremierWave EN device make use of SSL. The PremierWave EN embedded device server supports SSLv2, SSLv3, and TLS1.0.

TLS/SSL application hosts use separate digital certificates as a basis for authentication in both directions: to prove their own identity to the other party, and to verify the identity of the other party. In proving its own authenticity, the PremierWave EN device server will use its own "personal" certificate. In verifying the authenticity of the other party, the PremierWave EN unit will use a "trusted authority" certificate.

In short:

- ◆ When using EAP-TLS, the PremierWave EN device server needs a personal certificate with matching private key to identify itself and sign its messages.
- ◆ When using EAP-TLS, EAP-TTLS or PEAP, the PremierWave EN unit needs the authority certificate(s) that can authenticate those it wishes to communicate with.

Digital Certificates

The goal of a certificate is to authenticate its sender. It is analogous to a paper document that contains personal identification information and is signed by an authority, for example a notary or government agency. With digital certificates, a cryptographic key is used to create a unique digital signature.

Trusted Authorities

A private key is used by a trusted certificate authority (CA) to create a unique digital signature. Along with this private key is a certificate of authority, containing a matching public key that can be used to verify the authority's signature but not re-create it.

A chain of signed certificates, anchored by a root CA, can be used to establish a sender's authenticity. Each link in the chain is certified by a signed certificate from the previous link, with

the exception of the root CA. This way, trust is transferred along the chain, from the root CA through any number of intermediate authorities, ultimately to the agent that needs to prove its authenticity.

Obtaining Certificates

Signed certificates are typically obtained from well-known CAs, such as VeriSign, Inc. This is done by submitting a certificate request for a CA, typically for a fee. The CA will sign the certificate request, producing a certificate/key combo: the certificate contains the identity of the owner and the public key, and the private key is available separately for use by the owner.

As an alternative to acquiring a signed certificate from a CA, you can act as your own CA and create self-signed certificates. This is often done for testing scenarios, and sometimes for closed environments where the expense of a CA-signed root certificate is not necessary.

Self-Signed Certificates

A few utilities exist to generate self-signed certificates or sign certificate requests. The PremierWave EN system on module also has the ability to generate its own self-signed certificate/key combo. You can use XML to export the certificate in PEM format, but you cannot export the key. Hence the internal certificate generator can only be used for certificates that are to identify that particular PremierWave EN system on modules.

Certificate Formats

Certificates and private keys can be stored in several file formats. Best known are PKCS12, DER and PEM. Certificate and key can be in the same file or in separate files. Additionally, the key can be either be encrypted with a password or left in the clear. However, the PremierWave EN device currently only accepts separate PEM files, with the key unencrypted.

Several utilities exist to convert between the formats.

OpenSSL

OpenSSL is a widely used open source set of SSL related command line utilities. It can act as server or client. It can also generate or sign certificate requests, and can convert from and to several different of formats.

OpenSSL is available in binary form for Linux and Windows.

To generate a self-signed RSA certificate/key combo:

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

See www.openssl.org or www.madboa.com/geek/openssl for more information.

Note: *Signing other certificate requests is also possible with OpenSSL but the details of this process are outside the scope of this document.*

Steel Belted RADIUS

Steel Belted RADIUS is a commercial RADIUS server from Juniper Networks that provides a GUI administration interface. It also provides a certificate request and self-signed certificate generator.

The self-signed certificate has extension `.sbrpvk` and is in the PKCS12 format. OpenSSL can convert this into a PEM format certificate and key:

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

The `sbr_certkey.pem` file contains both certificate and key. If loading the SBR certificate into PremierWave EN system on module as an authority, you will need to edit it:

1. Open the file in any plain text editor.
2. Delete all info before "----- BEGIN CERTIFICATE-----" and after "----- END CERTIFICATE-----", and then save as `sbr_cert.pem`.

SBR accepts trusted-root certificates in the DER format. Again, OpenSSL can convert any format into DER:

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

Note: With SBR, when the identity information includes special characters such as dashes and periods, SBR changes the format it uses to store these strings and becomes incompatible with the current PremierWave EN release. Support may be added for this and other formats in future releases.

Free RADIUS

Free RADIUS is another versatile Linux open-source RADIUS server.

16: Updating Firmware

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/) or by using anonymous FTP (<ftp://ftp.lantronix.com/>).

Devices upgrading from existing firmware version 7.8 needing Python support will need to include a two-step upgrade process.

1. Install a new version of firmware (kernel + rootfs).
2. Install (python).rom image (new) or reinstall the complete firmware image (kernel + rootfs + python).rom (new).

Note: *The devices that upgrade from existing firmware versions (7.7 and earlier) and need Python support should use the DeviceInstaller serial recovery to upgrade to 7.9. Users must select the erase all flash option while upgrading firmware to 7.9 with (kernel + rootfs).rom. After that, install (python).rom or reinstall the complete firmware image (kernel + rootfs + python).rom. It takes approximately 13 minutes to complete advanced recovery.*

Loading New Firmware through Web Manager

Upload the firmware using the device web manager System page.

To upload new firmware:

1. Select **System** in the menu bar. The System page appears.

Figure 16-1 Uploading New Firmware

The screenshot shows the Lantronix PremierWave EN web interface. The left sidebar contains a menu with items like Status, Action, Applications, Bridge, CLI, Clock, CPM, Diagnostics, Discovery, DNS, DDNS, Email, Filesystem, FTP, Gateway, GRE, Host, HTTP, Line, Modbus, Network, Protocol Stack, RSS, SMTP, SNMP, SSH, SSL, Syslog, System (highlighted), Terminal, Tunnel, VPN, WLAN Profiles, WLAN QuickConnect, and XML. The main content area is titled 'System' and includes sections for 'Reboot Schedule', 'Reboot Device', 'Restore Factory Defaults', 'Upload New Firmware', 'Name', and 'Current Configuration'. The 'Upload New Firmware' section has a 'Choose File' button (showing 'No file chosen') and an 'Upload' button. The 'Name' section has input fields for 'Short Name' and 'Long Name', and a 'Submit' button. The 'Current Configuration' section shows a table with fields: Firmware Version (8.0.0.0R12), Short Name (premierwave_en), and Long Name (Lantronix PremierWave EN). The right sidebar contains a '[Logout]' button and several warning messages regarding scheduled reboots and firmware uploads.

2. Click **Browse** (under the **Upload New Firmware** heading) to browse to the firmware file.
3. Select the file and click **Open**.
4. Click **Upload** to install the firmware on the PremierWave EN unit.
5. Click **OK** in the confirmation popup which appears. The firmware will be installed and the device will automatically reboot afterwards.
6. Close and reopen the web manager internet browser to view the device's updated web pages.

Note: You may need to increase HTTP Max Bytes in some cases where the browser is sending data aggressively within TCP Windows size limit when file (including firmware upgrade) is uploaded from webpage.

Loading New Firmware through FTP

Firmware may be updated by sending the file to the PremierWave EN embedded system on module over an FTP connection. The destination file name on the PremierWave EN unit must have a "firmware.rom" type of format. The device will reboot upon successful completion of the firmware upgrade.

Example FTP session:

```
$ ftp 192.168.10.127
Connected to 192.168.10.127.
220 (vsFTPD 2.0.7)
Name (192.168.10.127:user): admin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put premierwave_en_8_0_0_OR12
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 File receive OK.
9308164 bytes sent in 3.05 seconds (3047859 bytes/s)
ftp> quit
221 Goodbye.
```

17: Branding the PremierWave EN Device

This chapter describes how to brand your PremierWave EN embedded system on module by using Web Manager and Command Line Interface (CLI). It contains the following sections on customization:

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

Web Manager Customization

Customize the Web Manager's appearance by modifying `index.html`, `style.css`, and the product logo. The style (fonts, colors, and spacing) of the Web Manager is controlled with `style.css`. The text and graphics are controlled with `index.html`. The product logo is the image in top-left corner of the page and defaults to a product name image.

Note: *The recommended dimensions of the new graphic are 300px width and 50px height.*

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

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

1. FTP to the PremierWave EN device.
2. Make a directory (`mkdir`) and name it `http/config`.
3. Change to the directory (`cd`) that you created in step 2 (`http/config`).
4. Save the contents of `index.html` and `style.css` by using a web browser and navigating to `http://<PremierWaveEN hostname>/config/index.html` and `http://<PremierWaveEN hostname>/config/style.css`.
5. Modify the file as required or create a new one with the same name.
6. To customize the product logo, save the image of your choice as `logo.gif`.
7. Put the file(s) by using `put <filename>`.
8. Type `quit`. The overriding files appear in the file system's `http/config` directory.
9. Restart any open browser to view the changes.
10. If you wish to go back to the default files in the firmware image, simply delete the overriding files from the file system.

Short and Long Name Customization

You can customize the short and long names in your PremierWave EN embedded system on module. The names display in the CLI show command and in the System web page in the Current Configuration table. The short name is used for the show command. Both names display in the CLI Product Type field.

Note: See [System Settings \(on page 118\)](#) for additional configuration options available on the Systems page.

Table 17-1 Short and Long Name Settings

Name Settings	Description
Short Name	Enter a short name for the system name. A maximum of 32 characters are allowed.
Long Name	Enter a long name for the system name. A maximum of 64 characters are allowed.

To Customize Short or Long Names

Using Web Manager

- ◆ To access the area with options to customize the short name and the long name of the product, or to view the current configuration, click **System** in the menu.

Using the CLI

- ◆ To enter the command level: `enable`

Using XML

- ◆ Include in your file:


```
<configitem name="short name">
and
<configitem name="long name">
```


Appendix A: Lantronix Technical Support

Lantronix offers many resources to support our customers and products at <http://www.lantronix.com/support>. For instance, you can ask a question, find firmware downloads, access the FTP site and search through tutorials. At this site you can also find 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 B: Binary to Hexadecimal Conversions

Many of the unit's configuration procedures require you to assemble a series of options (represented as bits) into a complete command (represented as a byte).

The resulting binary value must be converted to a hexadecimal representation.

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

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

Converting Binary to Hexadecimal

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

Conversion Table

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

Scientific Calculator

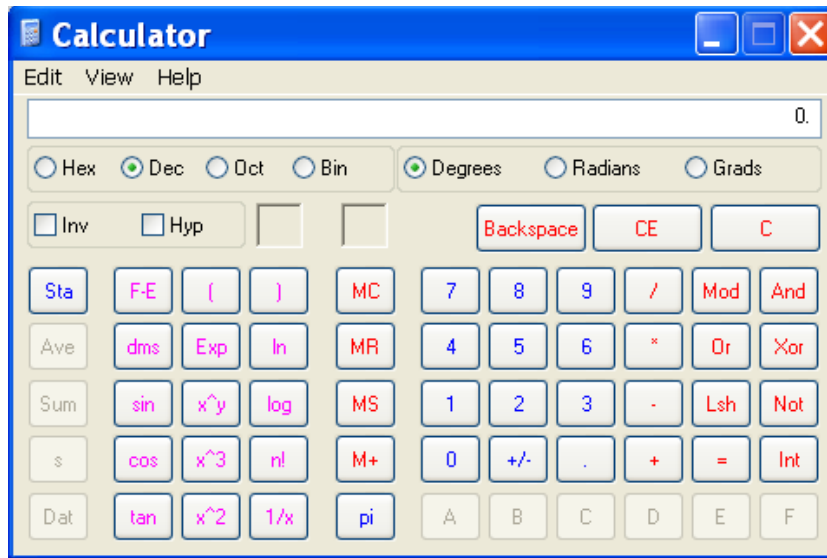
Another simple way to convert binary to hexadecimal is to use a scientific calculator, such as the one available on the Windows operating systems. For example:

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

Table B-1 Binary to Hexadecimal Conversion

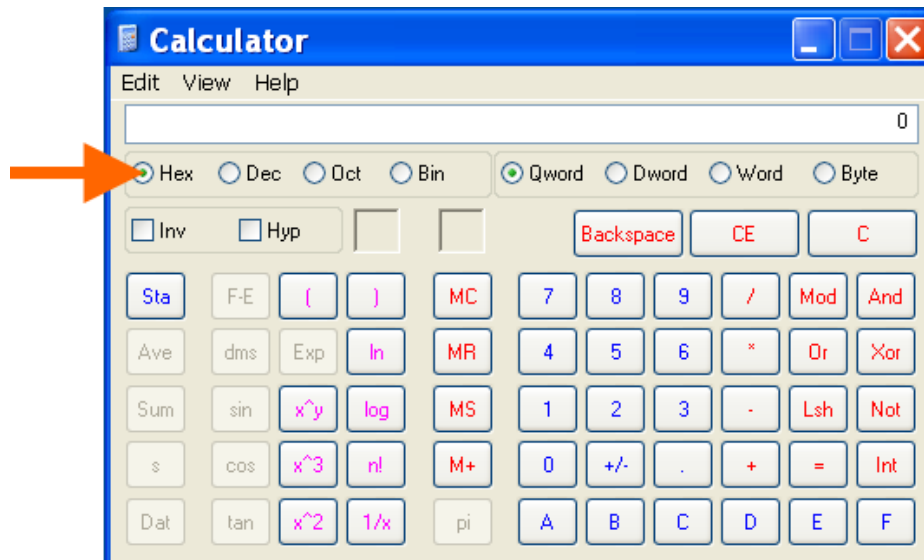
Decimal	Binary	Hex
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Figure B-2 Windows Scientific Calculator



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

Figure B-3 Hexadecimal Values in the Scientific Calculator



Appendix C: Compliance

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

Manufacturer's Name & Address:

Lantronix, Inc.
7535 Irvine Center Drive, Suite 100, Irvine, CA 92618 USA

Product Name Model:

PremierWave® EN Embedded Device Server

Conforms to the following standards or other normative documents:

Safety

- ◆ IEC 60950-1, Second Edition
- ◆ EN 60950-1, Second Edition
- ◆ UL 60950-1, Second Edition
- ◆ CSA 22.2, No. 60950-1-07, Second Edition

Wireless Regulatory Standards

- ◆ 47 CFR Part 15, Subpart C Section 15.247
- ◆ 47 CFR Part 15, Subpart E Section 15.407
- ◆ RSS-210 Issue 8 December 2010
- ◆ RSS-GEN Issue 2 June 2007
- ◆ ICES-003 Issue 4 February 2004
- ◆ ETSI EN 301 893 v1.7.1
- ◆ ETSI EN 301 489-1 V1.8.1
- ◆ ETSI EN 301 489-17 V2.1.1
- ◆ ETSI EN 300 328 V1.9.1
- ◆ Japan Article 2, Section 1, No. 19
- ◆ Japan Article 2, Section 1, No. 19-3
- ◆ Japan Article 2, Section 1, No. 19-3-2

Transmitter IDs

- ◆ FCC ID: R68PEN
- ◆ IC ID: 3867A-PEN
- ◆ Japan IDs: 006WWC0244, 006XWA0019, 006YWA0009

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.

Table C-1 PremierWave Regulatory Domains

REGION:		US/CANADA		JAPAN		EUROPEAN UNION		WORLDWIDE		
Frequency	Channel	Scan Type	Adhoc Permitted	Scan Type	Adhoc Permitted	Scan Type	Adhoc Permitted	Scan Type	Adhoc Permitted	
2.4 GHz Band	2412	1	Active	Yes	Active	Yes	Active	Yes	Passive	Yes
	2417	2	Active	Yes	Active	Yes	Active	Yes	Passive	Yes
	2422	3	Active	Yes	Active	Yes	Active	Yes	Passive	Yes
	2427	4	Active	Yes	Active	Yes	Active	Yes	Passive	Yes
	2432	5	Active	Yes	Active	Yes	Active	Yes	Passive	Yes
	2437	6	Active	Yes	Active	Yes	Active	Yes	Passive	Yes
	2442	7	Active	Yes	Active	Yes	Active	Yes	Passive	Yes
	2447	8	Active	Yes	Active	Yes	Active	Yes	Passive	Yes
	2452	9	Active	Yes	Active	Yes	Active	Yes	Passive	Yes
	2457	10	Active	Yes	Active	Yes	Active	Yes	Passive	Yes
	2462	11	Active	Yes	Active	Yes	Active	Yes	Passive	Yes
	2467	12	N/A	N/A	Active	Yes	Active	Yes	Passive	Yes
	2472	13	N/A	N/A	Active	Yes	Active	Yes	Passive	Yes
	2484	14	N/A	N/A	Active	Yes	N/A	N/A	Passive	Yes
5 GHz Band	5180	36	Active	Yes	Active	Yes	Active	Yes	Passive	Yes
	5200	40	Active	Yes	Active	Yes	Active	Yes	Passive	Yes
	5220	44	Active	Yes	Active	Yes	Active	Yes	Passive	Yes
	5240	48	Active	Yes	Active	Yes	Active	Yes	Passive	Yes
	5260	52	Passive	No	Passive	No	Passive	No	Passive	No
	5280	56	Passive	No	Passive	No	Passive	No	Passive	No
	5300	60	Passive	No	Passive	No	Passive	No	Passive	No
	5320	64	Passive	No	Passive	No	Passive	No	Passive	No
	5500	100	Passive	No	Passive	No	Passive	No	Passive	No
	5520	104	Passive	No	Passive	No	Passive	No	Passive	No
	5540	108	Passive	No	Passive	No	Passive	No	Passive	No
	5560	112	Passive	No	Passive	No	Passive	No	Passive	No
	5580	116	Passive	No	Passive	No	Passive	No	Passive	No
	5600	120	N/A	N/A	Passive	No	Passive	No	Passive	No
	5620	124	N/A	N/A	Passive	No	Passive	No	Passive	No
	5640	128	N/A	N/A	Passive	No	Passive	No	Passive	No
	5660	132	Passive	No	Passive	No	Passive	No	Passive	No
	5680	136	Passive	No	Passive	No	Passive	No	Passive	No
	5700	140	Passive	No	Passive	No	Passive	No	Passive	No
	5745	149	Active	Yes	N/A	N/A	N/A	N/A	Passive	Yes
5765	153	Active	Yes	N/A	N/A	N/A	N/A	Passive	Yes	
5785	157	Active	Yes	N/A	N/A	N/A	N/A	Passive	Yes	
5805	161	Active	Yes	N/A	N/A	N/A	N/A	Passive	Yes	
5825	165	Active	Yes	N/A	N/A	N/A	N/A	Passive	Yes	

Note: The PremierWave does not support 40 Mhz bandwidth channels. Country codes are not available to the end user. Last updated for Ganges driver version 3.2.12.

Appendix D: USB-CDC-ACM Device Driver File for Windows Hosts

A `linux-cdc-acm.inf` file may be used to enable Windows to recognize the USB-CDC-ACM connection to the USB device port of the PremierWave EN embedded system on module.

Creating a USB-CDC-ACM Device Driver File

1. Create the `linux-cdc-acm.inf` file on the Windows host somewhere using the contents provided below.

```
; Windows USB CDC ACM Setup File
; Based on INF template which was:
;   Copyright (c) 2000 Microsoft Corporation
;   Copyright (c) 2007 Microchip Technology Inc.
; likely to be covered by the MLPL as found at:
;   <http://msdn.microsoft.com/en-us/cc300389.aspx#MLPL>.
; For use only on Windows operating systems.

[Version]
Signature="$Windows NT$"
Class=Ports
ClassGuid={4D36E978-E325-11CE-BFC1-08002BE10318}
Provider=%Linux%
DriverVer=11/15/2007,5.1.2600.0

[Manufacturer]
%Linux%=DeviceList, NTamd64

[DestinationDirs]
DefaultDestDir=12

;-----
; Windows 2000/XP/Vista-32bit Sections
;-----

[DriverInstall.nt]
include=mdmcpq.inf
CopyFiles=DriverCopyFiles.nt
AddReg=DriverInstall.nt.AddReg

[DriverCopyFiles.nt]
usbser.sys,,,0x20
```

```
[DriverInstall.nt.AddReg]
HKR,,DevLoader,,*ntkern
HKR,,NTMPDriver,,USBSER.sys
HKR,,EnumPropPages32,, "MsPorts.dll,SerialPortPropPageProvider"
[DriverInstall.nt.Services]
AddService=usbser, 0x00000002, DriverService.nt
[DriverService.nt]
DisplayName=%SERVICE%
ServiceType=1
StartType=3
ErrorControl=1
ServiceBinary=%12%\USBSER.sys
;-----
; Vista-64bit Sections
;-----
[DriverInstall.NTamd64]
include=mdmcpq.inf
CopyFiles=DriverCopyFiles.NTamd64
AddReg=DriverInstall.NTamd64.AddReg
[DriverCopyFiles.NTamd64]
USBSER.sys,, 0x20
[DriverInstall.NTamd64.AddReg]
HKR,,DevLoader,,*ntkern
HKR,,NTMPDriver,,USBSER.sys
HKR,,EnumPropPages32,, "MsPorts.dll,SerialPortPropPageProvider"
[DriverInstall.NTamd64.Services]
AddService=usbser, 0x00000002, DriverService.NTamd64
[DriverService.NTamd64]
DisplayName=%SERVICE%
ServiceType=1
StartType=3
ErrorControl=1
ServiceBinary=%12%\USBSER.sys
;-----
; Vendor and Product ID Definitions
;-----
```

```

; When developing your USB device, the VID and PID used in the PC side
; application program and the firmware on the microcontroller must
match.

; Modify the below line to use your VID and PID. Use the format as
shown

; below.

; Note: One INF file can be used for multiple devices with different
; VID and PIDs. For each supported device, append
; ",USB\VID_xxxx&PID_yyyy" to the end of the line.
;-----
[SourceDisksFiles]
[SourceDisksNames]
[DeviceList]
%DESCRIPTION%=DriverInstall, USB\VID_0525&PID_A4A7,
USB\VID_0525&PID_A4AB&MI_02
[DeviceList.NTamd64]
%DESCRIPTION%=DriverInstall, USB\VID_0525&PID_A4A7,
USB\VID_0525&PID_A4AB&MI_02
;-----
; String Definitions
;-----
;Modify these strings to customize your device
;-----
[Strings]
Linux           = "Linux Developer Community"
DESCRIPTION    = "Gadget Serial"
SERVICE       = "USB RS-232 Emulation Driver"

```

2. When Windows prompts for a device driver for the USB connection, point it to this file.

Note: For Windows 7 installation, it is recommended to manually install the driver before plugging in the USB cable to the PremierWave EN device port. This can be done by installing a legacy driver for a COM port, with the Have Disk... option.

Installing the USB-CDC-ACM Device Driver File

Note: These instructions were created for Windows 7 PC users. Users with other versions of Windows may have slightly different instructions.

Use these instructions to install the USB serial (line 3) drivers.

1. Copy the attached `linux-cdc-acm.ini` file to any location on your Windows PC.
2. Connect the gadget USB serial (2.4) to the PC. Windows downloads the drivers automatically and fails.
3. Open **Windows Device Manager** and select **Actions** (on the top).
4. Select to **Add legacy hardware** and click **Next**.
5. Select **Install the hardware manually** and click **Next**.
6. Double click **Ports (COM & LPT)** and click **Next**.
7. Select the **PC manufacturer** and **PC model**.
8. Click **Have Disk** and browse to and select the `linux-cdc-acm.ini` file and click **Next**.
9. Reboot your device after Windows finishes installing the drivers. Once rebooted, the USB serial drivers are successfully installed and available to use.