PremierWave™ EN User Guide

Part Number 900-579
Revision C July 2011

Copyright & Trademark

Warranty

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

Contacts

Lantronix Corporate Headquarters

167 Technology Drive
Irvine, CA 92618, USA

Phone: 949-453-3990
Fax: 949-450-7249

Technical Support

Online: www.lantronix.com/support

Sales Offices

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

Disclaimer

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

Revision History

Date	Rev.	Comments
January 2011	A	Initial Document.
July 2011	B	Updated for release 7.2.0.0. Includes the new Bridging feature.
July 2011	C	Added chapter on OEM branding capabilities.

Table of Contents

6: Line and Tunnel Settings 40

List of Figures

List of Tables

1: Using This Guide

Purpose and Audience

This guide provides the information needed to configure, use, and update the PremierWave EN. It is intended for software developers and system integrators who are embedding PremierWave in 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 current configuration using DeviceInstaller.
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: Line and Tunnel Settings	Instructions for configuring line and tunnel settings.
7: Terminal and Host Settings	Instructions for configuring terminal and host settings.
8: Configurable Pin Manager	Information about the Configurable Pin Manager (CPM) and how to set the configurable pins to work with a device.
9: Services Settings	Instructions for configuring DNS, FTP, HTTP and Syslog settings.
10: Security Settings	Instructions for configuring SSL security settings.
11: Maintenance and Diagnostics Settings	Instructions to maintain the PremierWave EN, view statistics, files, and diagnose problems.
12: Advanced Settings	Instructions for configuring email, CLI and XML settings.
13: Bridging	Instructions for establishing a bridge.
14: Security in Detail	Detailed description and configuration of SSL security settings.
15: Updating Firmware	Instructions for obtaining the latest firmware and updating the PremierWave EN.
16: VIP Settings	Information about Virtual IP (VIP) features available on the device and instructions on configuring settings.
17: Branding the PremierWave EN	Instructions on how to brand your device.
Appendix A: Technical Support	Instructions for contacting Lantronix Technical Support.
Appendix B: Binary to Hexadecimal Conversions	Instructions for converting binary values to hexadecimals.
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 Integration Guide	Information about the PremierWave EN hardware, testing the PremierWave EN using the demonstration board, and integrating the PremierWave EN into your product.
PremierWave EN 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 Eval Board Quick Start	Instructions for getting the PremierWave EN evaluation board up and running.
PremierWave Eval Board User Guide	Information needed to use the PremierWave EN on the evaluation board.
DeviceInstaller Online Help	Instructions for using the Lantronix Windows-based utility to locate the PremierWave EN and to view its current settings.
Com Port Redirector Quick Start and Online Help	Instructions for using the Lantronix Windows-based utility to create virtual com ports.
Secure Com Port Redirector User Guide	Instructions for using the Lantronix Windows-based utility to create secure virtual com ports.

2: Introduction

The PremierWave EN embedded Ethernet Device Server is a complete network-enabling solution in a 30 (1.181) X 55 (2.165) X 6.45 (0.248) package. This miniature device server 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 is a step-down converter to 1.5 volts for the processor core and 1.8 volts for the memory subsystem. All voltages have LC filtering to minimize noises and emissions.
- Controller: 32-bit ARM9 microprocessor running at 400 MHz with 32kB Data Cache and 32 kB Instruction Cache Memory: Up to 64 MB SDRAM and 256 MB NAND Flash (Default 64 MB each). Up to 16 MB serial SPI Flash (Default 8 MB).
- Ethernet: 10/100 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.
- Two USB 2.0 Full Speed (12 Mbps) Host ports
- USB 2.0 Full Speed (12 Mbps) 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.
- Temperature Range: Operates over an extended temperature range of -40°C to +85°C.

Applications

The PremierWave EN device server connects serial devices such as those listed below to Ethernet networks using the IP protocol family.

- ATM machines
- CNC controllers
- Data collection devices
- Universal Power Supply (UPS) management unit
- Telecommunications equipment
- 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 device server contains a full-featured IP stack. Supported protocols include:

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

Troubleshooting Capabilities

The PremierWave EN 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 memory and IP socket information.
- Perform ping and traceroute operations.
- Conduct forward or reverse DNS lookup operations.
- View all processes currently running on the PremierWave EN, including CPU utilization.
- View system log messages.

Configuration Methods

After installation, the PremierWave EN 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 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 23.*)

DeviceInstaller: Configure the IP address and related settings and view current settings on the PremierWave EN using a Graphical User Interface (GUI) on a PC attached to a network. (*See "Using DeviceInstaller" on page 21.*)

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

XML: The PremierWave EN 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 Command Reference Guide for instructions and commands.)

Addresses and Port Numbers

Hardware Address

The hardware address is also referred to as the Ethernet address or MAC address. Sample Hardware Address:

- `00-20-4A-14-01-18`
- `00:20:4A:14:01:18`

IP Address

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

Port Numbers

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

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

- 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
- TCP/UDP Port 10002: Tunnel 2
- TCP/UDP Port 10003: Tunnel 3

Product Information Label

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

- Bar code
- Product Revision
- Part number
- Hardware Address (MAC Address)
- 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 00-20-4A-14-01-18, then the Ethernet address is 00-20-4A-14-01-18 and the WLAN address is 00-20-4A-14-01-19.*

Figure 2-1 Product Label

3: Using DeviceInstaller

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

Notes:

- *For instructions on using DeviceInstaller 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.*

Accessing PremierWave EN using DeviceInstaller

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

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 -> 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 PremierWave 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 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	Name identifying the PremierWave EN.
DHCP Device Name	The name associated with the PremierWave EN module's current IP address, if the IP address was obtained dynamically.

Current Settings *(continued)*	Description
Group	Configurable field. Enter a group to categorize the PremierWave EN. 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. 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”.
Type	Shows the device type as “PremierWave EN”.
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 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.
IP Address was Obtained	Appears “Dynamically” if the PremierWave EN automatically received an IP address (e.g., from DHCP). Appears “Statically” if the IP address was configured manually. If the IP address was assigned dynamically, the following fields appear: ◆ **Obtain via DHCP** with values of True or False. ◆ **Obtain via BOOTP** with values of True or False.
Subnet Mask	Shows the subnet mask specifying the network segment on which the PremierWave EN resides.
Gateway	Shows the IP address of the router of this network. There is no default.
Number of Ports	Shows the number of serial ports on this PremierWave EN.
Supports Configurable Pins	Shows True, indicating configurable pins are available on the PremierWave EN.
Supports Email Triggers	Shows True, indicating email triggers are available on the PremierWave EN.
Telnet Enabled	Indicates whether Telnet is enabled on this PremierWave EN.
Telnet Port	Shows the PremierWave EN port for Telnet sessions.
Web Enabled	Indicates whether Web Manager access is enabled on this PremierWave EN.
Web Port	Shows the PremierWave EN port for Web Manager configuration (if Web Enabled field is True).
Firmware Upgradable	Shows True, indicating the PremierWave EN firmware is upgradable as newer versions become available.

4: Configuration Using Web Manager

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

Accessing Web Manager

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

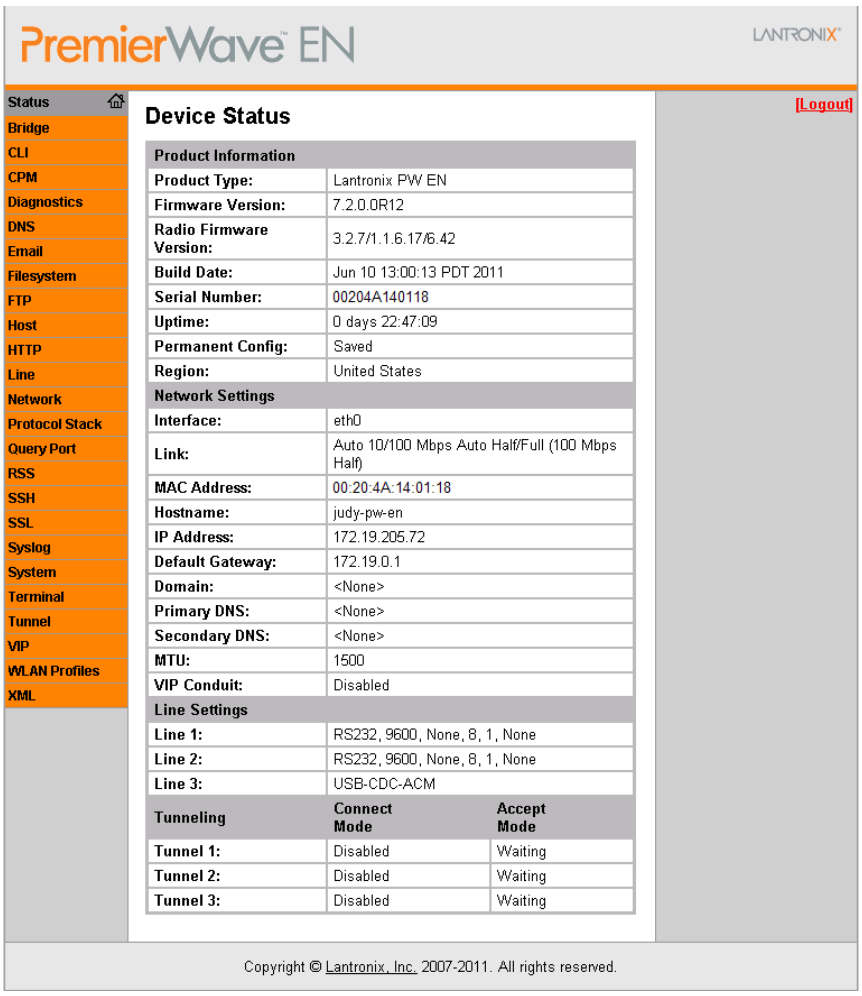
To access Web Manager, perform the following steps:

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

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

Device Status Page

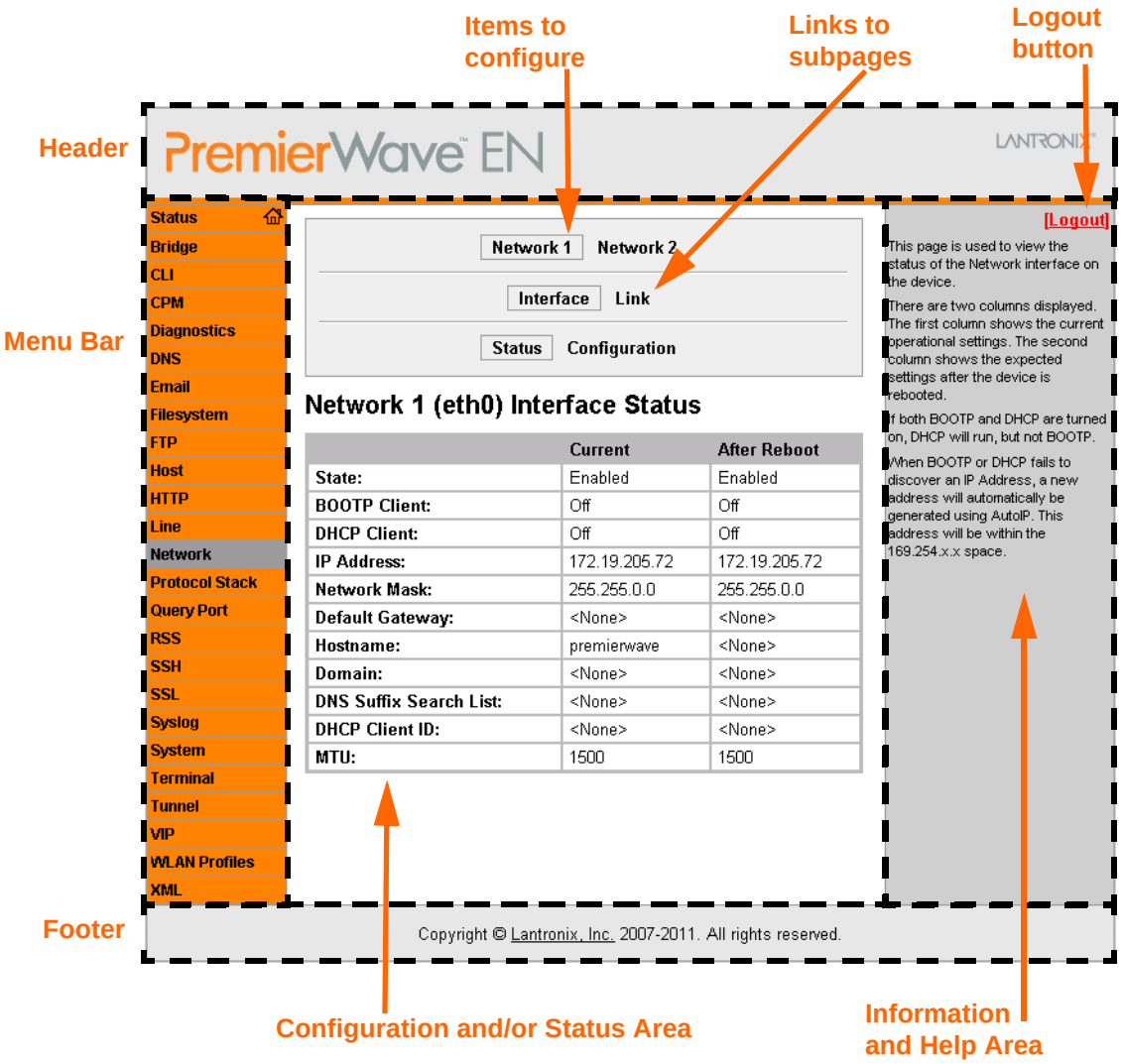
The Device Status page is the first page that appears after you log into the Web Manager. It also appears when you click **Status** in the Main Menu.



Web Manager Page Components

The layout of a typical Web Manager page is below.

Figure 4-1 Components of the Web Manager Page



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

The main area of the page has these additional sections:

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

- At the bottom of most pages, the current configuration is displayed. In some cases, you can reset or clear a setting.
- The information or help area shows information or instructions associated with the page.
- A **Logout** link is available at the upper right corner of every web page. In Chrome or Safari, it is necessary to close out of the browser to 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 the Web Manager

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

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

Web Manager Page	Description	See Page
Status	Shows product information and network, line, and tunneling settings.	*24*
Bridge	Allows you to configure a bridge and shows the current operational state of the bridge.	*83*
CLI	Shows Command Line Interface (CLI) statistics and lets you change the current CLI configuration settings.	*78*
CPM	Shows information about the Configurable Pins Manager (CPM) and how to set the configurable pins and pin groups to work with a device.	*55*
Diagnostics	Lets you perform various diagnostic procedures.	*73*
DNS	Shows the current configuration of the DNS subsystem and the DNS cache.	*58*
Email	Shows email statistics and lets you clear the email log, configure email settings, and send an email.	*77*
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.	*68*
FTP	Shows statistics and lets you change the current configuration for the File Transfer Protocol (FTP) server.	*59*
Host	Lets you view and change settings for a host on the network.	*53*
HTTP	Shows HyperText Transfer Protocol (HTTP) statistics and lets you change the current configuration and authentication settings.	*60*
Line	Shows statistics and lets you change the current configuration and Command mode settings of a serial line.	*41*
Network	Shows status and lets you configure the network interface.	*28*
Protocol Stack	Lets you perform lower level network stack-specific activities.	*70*
Query Port	Lets you change configuration settings for the query port.	*72*

Web Manager Page (continued)	Description	See Page
RSS	Lets you change current Really Simple Syndication (RSS) settings.	62
SSH	Lets you change the configuration settings for SSH server host keys, SSH server authorized users, SSH client known hosts, and SSH client users.	79
SSL	Lets you upload an existing certificate or create a new self-signed certificate.	64
Syslog	Lets you specify the severity of events to log and the server and ports to which the syslog should be sent.	59
System	Lets you reboot device, restore factory defaults, upload new firmware, and change the device long and short names.	76
Terminal	Lets you change current settings for a terminal.	52
Tunnel	Lets you change the current configuration settings for a tunnel.	43
VIP	Lets you configure Virtual IP addresses to be used in Tunnel Accept Mode and Tunnel Connect Mode.	90
WLAN Profiles	Lets you view, edit, delete and create a WLAN profile on a device.	33
XML	Lets you export XML configuration and status records, and import XML configuration records.	80

5: Network Settings

The Network Settings show the status of the Ethernet or WLAN interface/link and let you configure the settings on the device. Interface settings are related to the configuration of the IP and related protocols. Link settings are related to the physical link connection, which carries the IP traffic.

The PremierWave EN contains two network interfaces. Only one interface may be active at a time; however, if bridging is enabled, both interfaces will be activated and controlled by the bridging subsystem. The Ethernet interface is also called **interface 1** or **eth0**, and the WLAN interface is called **interface 2** or **wlan0**.

Notes:

- *Some settings require a reboot to take effect. These settings are noted below.*
- *The* blue text *in the XML command strings of this chapter are to be replaced with a user-specified name.*

Network Interface Settings

Table 5-1 shows the network interface settings that can be configured. These settings apply to both the Ethernet (eth0) and WLAN (wlan0) interfaces, but are configured independently for each interface.

Table 5-1 Network Interface Settings

Network Interface Settings	Description
State	Enables or disables the interface.
BOOTP Client	Select Enable or Disable. At boot up, after the physical link is up, the PremierWave EN will attempt to obtain IP settings from a BOOTP server. ***Note:*** *Overrides the configured IP address/mask, gateway, hostname, and domain. When DHCP is* ***Enable****, the system automatically uses DHCP, regardless of whether BOOTP is* ***Enable****. Changing this value requires you to reboot the device.*
DHCP Client	Select Enable or Disable. At boot up, after the physical link is up, the PremierWave EN will attempt to obtain IP settings from a DHCP server and will periodically renew these settings with the server. ***Note:*** *Overrides BOOTP, the configured IP address/mask, gateway, hostname, and domain. Changing this value requires you to reboot the device.* ***Note:*** *Within WebManager, click* ***Renew*** *to renew the DHCP lease.*
IP Address	Enter the static IP address to use for the interface. You may enter it alone or in CIDR format. ***Note:*** *This setting will be used if Static IP is active (both DHCP and BOOTP are* ***Disable****). Changing this value requires you to reboot the device. When DHCP or BOOTP is enabled, the PremierWave EN tries to obtain an IP address from a DHCP or BOOTP server. If it cannot, the PremierWave EN generates and uses an Auto IP address in the range of 169.254.xxx.xxx, with a network mask of 255.255.0.0.*

Network Interface Settings (continued)	Description
Default Gateway	Enter the IP address of the router for this network. *Note: This setting will be used if Static IP is active (both DHCP and BOOTP are **Disable**).*
Hostname	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. *Note: This setting will take effect immediately, but will not register the hostname with a DNS server until the next reboot.*
Domain	Enter the domain name suffix for the interface. *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.*
DHCP Client ID	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 MAC address.
Primary DNS	Enter the IP address of the primary Domain Name Server. *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.*
Secondary DNS	Enter the IP address of the secondary Domain Name Server. *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.*
MTU	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.

To Configure Network Interface Settings

Using Web Manager

- To modify Ethernet (eth0) settings, click **Network** on the menu and select **Network 1 -> Interface -> Configuration**.
- To modify Wireless (wlan0) settings, click **Network** on the menu and select **Network 2 -> Interface -> Configuration**.

Using the CLI

- To enter the eth0 command level: `enable -> config -> if 1`
- To enter the wlan0 command level: `enable -> config -> if 2`

Using XML

- Include in your file: `<configgroup name="interface" instance="eth0">`
- Include in your file: `<configgroup name="interface" instance="wlan0">`

To View Network Interface Status

Using Web Manager

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

- To view the Ethernet (eth0) Status page, click **Network** on the menu and select **Network 1 -> Interface -> Status**.
- To view the Wireless (wlan0) Status page, click **Network** on the menu and select **Network 2 -> Interface -> Status**.

Network Link Settings

Physical link parameters can be configured for an Ethernet (eth0) Network Interface (see Table 5-2) and a WLAN (wlan0) Network Interface (see Table 5-3).

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** = Force 10 Mbps ◆ **100** = Force 100 Mbps
Duplex	Select t he 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.*

Table 5-3 Network 2 (wlan0) Link Settings

Network 2 WLAN (wlan0) Link Settings	Description
Choice 1 Profile **Choice 2 Profile** **Choice 3 Profile** **Choice 4 Profile**	Up to four (4) WLAN Profiles may be selected for automatic connection to wireless networks. More information on wireless settings is available in the section, *To Configure Network Link Settings on page 31*. Enter the name of the WLAN Profile desired for each choice.

Network 2 WLAN (wlan0) Link Settings (continued)	Description
Debugging Level	The Debugging Level sets the verbosity level for printing WLAN Link messages to the TLOG. (Default is Info) Available levels, from most to least verbose: ◆ Dump ◆ Debug ◆ Info ◆ Warning ◆ Error
Active Channel Scan Time	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 prove requests and gathers prove responses from other devices. The range of values is 50 to 100 ms.
Passive Channel Scan Time	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 ms.
Radio Band Selection	Selects the band(s) on which the radio will operate. Options are 2.4 GHz only, 5 GHz only or Dual band.

To Configure Network Link Settings

Using Web Manager

- To modify Ethernet (eth0) Link information, click **Network** on the menu and select **Network 1 -> Link**.
- To modify Wireless (wlan0) Link information, click **Network** on the menu and select **Network 2 -> Link -> Configuration.**

Using the CLI

- To enter the eth0 Link command level: `enable -> config -> if 1 -> link`
- To enter the wlan0 Link command level: `enable -> config -> if 2 -> link` or `enable -> config -> if 2 -> link -> choice 1|2|3|4`

Using XML

- Include in your file: `<configgroup name="ethernet" instance="eth0">`
- Include in your file: `<configgroup name="wlan" instance="wlan0">`

WLAN Link Status and Scan Commands

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

WLAN Link Information Commands	Description
Scan "<network SSID>"	Performs a scan for devices within range of the PremierWave EN. 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. ***Note:*** *When omitting the network SSID it is still necessary to include the opening and closing quotation marks (scan "").*
Status	Displays status information about the WLAN link.

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

WLAN Link Scan Results Field	Description
SSID	The Service Set Identifier (network name) of the device.
BSSID	Basic Service Set Identifier.
Channel	The channel on which the device is operating.
Signal Level	The Received Signal Strength Indication (RSSI) of the device measured in dBm.
Flags	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:

WLAN Link Status Results Field	Description
Type	Indicates this is a WLAN link
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.
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 EN
RSSI	A measure of the power level of the received radio signal in dBm.

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="wlan status">`

  and

  `<statusgroup name="wlan scan">`

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.) A maximum of six profiles can exist on the PremierWave EN at a time. Of these, up to four can be configured as active.

To Configure WLAN Profiles

You can view, edit, create or delete a default adhoc or infrastructure 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 5-4 WLAN Profile Basic Settings

WLAN Profile Basic Settings	Description
Network Name (SSID)	The name of the wireless network (SSID.) *Note: The PremierWave EN performs only passive scans on the DFS channels (52–140.) In order for the PremierWave EN to connect with an access point on one of these channels, the access point must be configured to broadcast the SSID in its beacons.*
Topology	Specifies Infrastructure (ESS) or Adhoc (IBSS) mode. ◆ **Infrastructure**: mode that communicates with access points. ◆ **Adhoc**: mode that communicates with other clients.
Channel	Specifies the channel for an Adhoc network. *Note: This setting only applies to the creation of an Adhoc network.*
Scan 2.4 GHz Band	Enables or disables scanning for a WLAN profile on the 2.4 GHz band. *Note: Setting this value to "Disabled" prevents this profile from connecting to any device operating in the 2.4 GHz band.*
Scan 5 GHz Band	Enables or disables scanning for a WLAN profile on the 5 GHz band. *Note: Setting this value to "Disabled" prevents this profile from connecting to any device operating in the 5 GHz band.*
Scan DFS Channels	Enables or disables scanning on the DFS (Dynamic Frequency Selection) channels in the 5 GHz band. *Note: This setting only applies if scanning in the 5 GHz band is enabled.*

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 5-5 WLAN Profile Advanced Settings

WLAN Profile Advanced Settings	Description
TX Data Rate Maximum	Specifies the rate for data transmission. *Note: This setting only applies if '**TX Data Rate**' is set to '**Fixed**'.*

WLAN Profile Advanced Settings	Description
TX Data Rate	PremierWave lets you control the transmission data rate or controls it automatically. ◆ **Fixed** = keeps the transmission rate at the configured value. ◆ **Auto-reduction** = allows the PremierWave EN to reduce the data rate automatically, depending on link quality.
TX Power Maximum	Maximum transmission output power in dBm.
Antenna Diversity	Selects the antenna the radio will use or allows the PremierWave EN to automatically make the selection. ◆ **Enabled** = allow the PremierWave EN to select the antenna. ◆ **Antenna 1** = use the internal antenna. ◆ **Antenna 2** = use the external antenna.
Power Management	Power management reduces the overall power consumption of the PremierWave EN unit, but can increase latency. ◆ **Enabled** = allows the PremierWave EN to turn off the receiver when it is idling. ◆ **Disabled** = keeps the receiver on at all times.
Power Management Interval	Number of beacons (100 ms interval) between 1 and 10. The above-mentioned latency can be up to this number X 100ms.

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 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 5-6 WLAN Profile Security Settings

WLAN Profile Security Settings	Description
Suite	Specifies the security suite to be used for this profile. ◆ **None** = no authentication or encryption method will be used. ◆ **WEP** = Wired Equivalent Privacy ◆ **WPA** = WiFi Protected Access ◆ **WPA2** = Robust Secure Network.
Key Type	Selects the format of the security key.
Passphrase	The passphrase consists of up to 63 characters. ***Note:*** *Lantronix recommends using a passphrase of 20 characters or more for maximum security. Spaces and punctuation characters are permitted.* ***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.*

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 5-7 Additional WEP Settings for WLAN Profile.

WLAN Profile WEP Settings	Description
Authentication	Select one of the following options: ◆ **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 Size	Key size in bits. Select 40 for WEP40 and WEP64; select 104 for WEP104 and WEP128.
TX Key Index	Selects one of four indexes listing keys for transmitting data. Reception is allowed with all four keys. ***Note:*** *For operability with some products that generate four identical keys from a passphrase, this index must be one.*
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.

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 the WiFi 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 WiFi's subset of the broad IEEE802.11i standard to enforce better interoperability. The PremierWave EN is compliant with both WPA2 and IEEE802.11i.

Table 5-8 WLAN Profile WPA and WPA2/IEEE802.11i Settings

WLAN Profile WPA & WPA2 Settings	Description
Authentication	Selects the authentication method to be used. ◆ **PSK** = Pre-Shared Key. The same key needs to be configured on both sides of the connection. (On the PremierWave EN 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 EN with an internal database.
Key	64 hexadecimal digits (32 bytes.)
IEEE 802.1X	Selects the protocol to use to authenticate the WLAN client. ◆ **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 EN uses a more generic version to be compatible with other major brand WiFi 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 EN 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 EN), 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 EN. 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. ***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 to the RADIUS server. For more information about SSL certificates see* *TLS (SSL) on page 86.*
EAP-TTLS Option	Selects the inner authentication method to be used with EAP-TTLS (if configured.) ◆ EAP-MSCHAPv2 ◆ MSCHAPv2 ◆ MSCHAP ◆ CHAP ◆ PAP ◆ EAP-MD5
PEAP Option	Selects the inner authentication method to be used with EAP-PEAP (if configured.) ◆ EAP-MSCHAPv2 ◆ EAP-MD5

WLAN Profile WPA & WPA2 Settings (continued)	Description
Username	Userid for identifying the PremierWave EN to the RADIUS server in the network
Password	Password for identifying the PremierWave EN to the RADIUS server in the network.
Validate Certificate	If enabled, the PremierWave will attempt to validate the certificate received from the RADIUS server.
Encryption	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. ◆ **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. *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.*
Credentials	Name of client certificate (required for EAP-TLS.) For more information about SSL certificates see sections, *TLS (SSL) on page 86*.

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">`

6: Line and Tunnel Settings

The PremierWave EN contains three Lines. Lines 1 and 2 are standard RS232/RS485 serial ports, while Line 3 is an emulated serial port over the USB Device (USB-CDC-ACM).

RS232/RS485

Lines 1 and 2 can be configured to operate in the following modes:

- RS232
- RS485 Full Duplex
- RS485 Half Duplex, with and without termination impedance
- All serial settings such as Baud Rate, Parity, Data Bits, etc, apply to these Lines.

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 EN 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, and the USB cable physically replugged (or the COM port under Device Manager disabled/ enabled).***

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 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 comes back up, the CDC-ACM connection will be enumerated to a different /dev/ttyACMx device.***

Line Settings

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

Some settings may be specific to only certain Lines. Such settings are noted below.

Table 6-1 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	Sets the interface type for the Line. The default is **RS232** for Lines 1 and 2, and **USB-CDC-ACM** for Line 3. Choices are: ◆ **RS232** (Lines 1 and 2 only) ◆ **RS485 Full-Duplex** (Lines 1 and 2 only) ◆ **RS485 Half-Duplex** (Lines 1 and 2 only) ◆ **USB-CDC-ACM** (Line 3 only) = CDC-ACM over USB
Termination	Sets the Line Termination to **Enable** or **Disable**. The default is **Disable**. ***Note:*** *This setting is only relevant for Lines 1 and 2 with Interface type RS485 Half-Duplex.*
State	Sets the operational state of the Line to either **Enable** or **Disable**. The default is **Enable**.
Protocol	Sets the operational protocol for the Line. The default is **Tunnel**. Choices are: ◆ None ◆ Tunnel = Serial-Network tunneling protocol.
Baud Rate	Sets 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 Custom baud rate (available for line 1 and line 2 only), you may manually enter any value between 300 and 5000000. ***Note:*** *For Interface type USB-CDC-ACM (Line 3 only), this setting is irrelevant.*
Parity	Sets the Parity of the Line. The default is **None**. ***Note:*** *For Interface type USB-CDC-ACM (Line 3 only), this setting is irrelevant.*
Data Bits	Sets the number of data bits for the Line. The default is 8. ***Note:*** *For Interface type USB-CDC-ACM (Line 3 only), this setting is irrelevant.*
Stop Bits	Sets the number of stop bits for the Line. The default is 1. ***Note:*** *For Interface type USB-CDC-ACM (Line 3 only), this setting is irrelevant.*
Flow Control	Sets the flow control for the Line. The default is None. ***Note:*** *For Interface type USB-CDC-ACM (Line 3 only), this setting is irrelevant.*
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>.
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>.
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 ms).

Line Settings	Description
Threshold	Set the number of threshold bytes which need to be received in order for the driver to forward received characters.

Table 6-2 Line Command Mode Settings

Line Command Mode Settings	Description
Mode	Sets the Command Mode state of the Line. When in Command Mode, a CLI session operates exclusively on the Line. Choices are: ◆ Always ◆ User Serial String ◆ Disabled *Note: In order to enable command mode on the Line, Tunneling on the Line must be Disabled (both connect and accept modes).*
Wait Time	Enter the amount of time to wait during boot time for the Serial String. This timer starts right after the Signon Message has been set on the Serial Line and applies only if mode is "Use Serial String".
Serial String	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].
Echo Serial String	Select Yes or No 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.
Signon Message	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].

To Configure Line Settings

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

Using Web Manager

- To configure a specific line, click **Line** in the menu and select **Line 1 -> Configuration** (Table 6-1).
- To configure a specific line in Command Mode, click **Line** in the menu and select **Line 1 -> Command Mode** (Table 6-2).

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">`

To View Line Statistics

Using Web Manager

- To view statistics for a specific line, 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">`

Tunnel Settings

Tunneling allows serial devices to communicate over a network, without "being aware" of the devices which establish the network connection between them. Tunneling parameters are configured using the TUnnel menu and submenus.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

This page shows the settings for the tunnel selected at the top of the page and lets you change the settings. The Line Settings and Protocol are displayed for informational purposes and must be configured from the Line pages.

Table 6-3 Tunnel Serial Settings

Tunnel Serial Settings	Description
Line Settings	Line Settings information here is display only. Go to the section, *To Configure Line Settings* to modify these settings.
Protocol	Protocol information here is display only. Go to the section, *To Configure Line Settings* to modify these settings.
DTR	Select the conditions in which the Data Terminal Ready (DTR) control signal on the Serial Line are asserted. Choices are: ◆ 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 6-4 Tunnel Packing Mode Settings

Tunnel Packing Mode Settings	Description
Mode	Configure the Tunnel Packing Mode. Choices are: ◆ 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	Sets 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.
Timeout	Sets 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.
Send Character	Enter Control Characters in any of the following forms: ◆ <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: ◆ <control>J ◆ 0xA (hexadecimal) ◆ \10 (decimal). If used, the Send 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 PremierWave EN listens (waits) for incoming connections from the network. A remove node on the network initiates the connection.

The configurable local port is the port the remote device connects to for this connection. There is no remote port or address. The default local port is 10001 for serial line 1, 10002 for serial line 2 and 10003 for serial line 3.

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

Table 6-5 Tunnel Accept Mode Settings

Tunnel Accept Mode Settings	Description
Mode	Sets the method used to start a tunnel in Accept mode. Choices are: ◆ **Disable** = do not accept an incoming connection. ◆ **Always** = accept an incoming connection. (*default*) ◆ **Any Character** = start waiting for an incoming connection when any character is read on the serial line. ◆ **Start Character** = start waiting for an incoming connection when the start character for the selected tunnel is read on the serial line. ◆ **Modem Control Asserted** = start waiting for an incoming connection as long as the Modem Control pin (DSR) is asserted on the serial line until a connection is made. ◆ **Modem Emulation** = start waiting for an incoming connection when triggered by modem emulation AT commands. Connect mode must also be set to Modem Emulation.
Local Port	Sets the port number for use as the network local port. The defaults are as follows: ◆ Tunnel 1 : 10001 ◆ Tunnel 2 : 10002 ◆ Tunnel 3 : 10003

Tunnel Accept Mode Settings (continued)	Description
Protocol	Select the protocol type for use with Accept Mode: ◆ SSH ◆ SSL ◆ TCP (default protocol) ◆ TCP AES ◆ Telnet
TCP Keep Alive	Enter the time, in milliseconds, the PremierWave EN waits during a silent connection before checking if the currently connected network device is still on the network. If the unit then gets no response after 8 attempt, it drops the connection. Enter 0 to disable.
Flush Serial	Sets whether the serial Line data buffer is flushed upon a new network connection. Choices are: ◆ **Enabled** = serial data buffer is flushed on network connection ◆ **Disabled** = serial data buffer is not flushed on network connection (*default*)
Block Serial	Set whether Block Serial is enabled for debugging purposes. Choices are: ◆ **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: ◆ **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	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: ◆ 0A (Line Feed) ◆ 00 (Null) ◆ 0D 0A (Carriage Return/Line Feed) ◆ 0D 00 (Carriage Return/Null) If, **Prompt for Password** is set to Enabled, the user will be prompted for the password upon connection.
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.

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 continues to attempt an outgoing connection on the network, until established. 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 IP address or DNS name. The PremierWave EN will not make a connection unless it can resolve the address.

For Connect Mode using UDP, the PremierWave EN 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.*

The TCP keepalive time is the time in which proves are priodically sent to the other end of the connectio. This ensures the other side is still conected.

Table 6-6 Tunnel Connect Mode Settings

Tunnel Connect Mode Settings	Description
Mode	Sets the method to be used to attempt a connection to a remote host or device. Choices are: ◆ **Always** = a connection is attempted until one is made. If the connection gets disconnected, the PremierWave EN retries until it makes a connection. ◆ **Disable** = an outgoing connection is never attempted. (*default*)

Tunnel Connect Mode Settings (continued)	Description
Local Port	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.
Host 1	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.
Reconnect Timer	Sets 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	Sets whether the serial Line data buffer is flushed upon a new network connection. Choices are: ◆ **Enabled** = serial data buffer is flushed on network connection ◆ **Disabled** = serial data buffer is not flushed on network connection (*default*)
Block Serial	Set whether Block Serial is enabled for debugging purposes. Choices are: ◆ **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. ◆ **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.
Block Network	Set whether Block Network is enabled for debugging purposes. Choices are: ◆ **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">`

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 6-7 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(hexadercimal) 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: ◆ 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: ◆ 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, our product mimics the behavior of the modem.

Table 6-8 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: ◆ 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: ◆ Enabled ◆ Disabled (default)
Verbose Response	Set whether Modem Response Codes are sent out on the Serial Line. Choices are: ◆ Enabled ◆ Disabled (default)
Response Type	Select a representation for the Modem Response Codes sent out on the Serial Line. Choices are: ◆ 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: ◆ Enabled ◆ Disabled (default)
Incoming Connection	Set how and if requests are answered after an incoming RING (ATS0=2). Choices are: ◆ 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: ◆ 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">`

Statistics

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

To View Tunnel Statistics

Using Web Manager

- To view statistics for a specific tunnel, click **Tunnel** in the menu and select the **Tunnel 1 -> 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">`

7: 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 7-1 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**.
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	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 7-2 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: ◆ Telnet ◆ SSH ***Note:*** *SSH keys must be loaded or created on the SSH page for the SSH protocol to work.*
SSH Username	Appears if you selected SSH as the protocol. Enter a username to select a pre-configured Username/Password/Key (configured on the SSH: Client Users page), or leave it blank to be prompted for a username and password at connect time.

Host Settings	Description
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">`

8: Configurable Pin Manager

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

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 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 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 8-1 Current Configurable Pins

CP	Ref	Configured as	Value	Groups	Active in group
CP1	Pin 14	Input	0	1	<available>
CP2	Pin 16	Input	1	1	<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 8-2 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. Can be updated. Choices are: ◆ **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. Additionally, the CP logic can be inverted so that assertion is low.
Value	Shows the last bit in the CP current value.
Bit	Visual display of the bitwise 32 bit placeholders for a CP.

CPM – CPs Status (continued)	Description
Level	A "**+**" symbol indicates the CP is asserted (the voltage is high). A "**-** "indicates the CP voltage is low.
I/O	Indicates the current status of the pin: ◆ **I** = input ◆ **O** = output ◆ **<blank>** = unassigned
Logic	An "**I**" indicates the CP is inverted (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 8-3 CPM Group Current Configuration

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

Table 8-4 CPM Group Status

CPM – Groups Group Status	Description
Name	Shows the CP Group name.
State	Current enable state of the CP group.
Value	Shows 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.

CPM – Groups Group Status (continued)	Description
I/O	Indicates the current status of the pin: ◆ 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.

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”>`

9: Services Settings

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 or BOOTP.

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

Table 9-1 DNS Settings

Setting / Field	Description
Lookup	Perform one of the following: ◆ 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 firmware. A configurable option is provided to enable or disable access via this protocol.

Table 9-2 **FTP Settings**

FTP Settings	Description
State	Select to enable or disable the FTP server.

To Configure FTP Settings

Using Web Manager

- To configure FTP, 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 filesystem 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 9-3 Syslog Settings

Syslog Settings	Description
State	Enable or disable the syslog.
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.
Severity Log Level	Specify the minimum level of system message the PremierWave EN should log. 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, 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 9-4 **HTTP Settings**

HTTP Settings	Description
State	Enable or disable the HTTP server.
Port	Enter the port for the HTTP server to use. The default is **80**.
Secure Port	Enter the port for the HTTPS server to use. The default is **443**. The HTTP server only listens on the **HTTPS Port** when an SSL certificate is configured.
Secure Protocols	Select to enable or disable the following protocols: ◆ **SSL3** = Secure Sockets Layer version 3 ◆ **TLS1.0** = Transport Layer Security version 1.0. TLS 1.0 is the successor of SSL3 as defined by the IETF. ◆ **TLS1.1** = Transport Layer Security version 1.1 The protocols are enabled by default. ***Note:*** *A server certificate and associated private key need to be installed in the* **SSL** *configuration section to use* **HTTPS**.
Secure Credentials	Specify the name of the set of RSA and/or DSA certificates and keys to be used for the secure connection.
Max Timeout	Enter the maximum time for the HTTP server to wait when receiving a request. This prevents Denial-of-Service (DoS) attacks. The default is **10** seconds.
Max Bytes	Enter the maximum number of bytes the HTTP server accepts when receiving a request. The default is **40** kB (this prevents DoS attacks).
Logging State	Select **Enabled** to enable HTTP server logging.
Max Log Entries	Sets the maximum number of HTTP server log entries. Only the last **Max Log Entries** are cached and viewable.

HTTP Settings (continued)	Description
Log Format	Set the log format string for the HTTP server. Follow these **Log Format** rules: ◆ **%a** - remote IP address (could be a proxy) ◆ **%b** - bytes sent excluding headers ◆ **%B** - bytes sent excluding headers (0 = '-') ◆ **%h** - remote host (same as '%a') ◆ **%{h}i** - header contents from request (h = header string) ◆ **%m** - request method ◆ **%p** - ephemeral local port value used for request ◆ **%q** - query string (prepend with '?' or empty '-') ◆ **%t** - timestamp HH:MM:SS (same as Apache '%(%H:%M:%S)t' or '%(%T)t') ◆ **%u** - remote user (could be bogus for 401 status) ◆ **%U** - URL path info ◆ **%r** - first line of request (same as '%m %U%q <version>') ◆ **%s** - return status
Authentication Timeout	The timeout period applies if the selected authentication type is either **Digest** or **SSL/Digest**. After this period of inactivity, the client must authenticate again.

To Configure HTTP Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

Table 9-5 **HTTP Authentication Settings**

HTTP Authentication Settings	Description
URI	Enter the Uniform Resource Identifier (URI). ***Note:*** *The URI must begin with '/' to refer to the filesystem.*

HTTP Authentication Settings (continued)	Description
Auth Type	Select the authentication type: ◆ **None** = no authentication is necessary. ◆ **Basic** = encodes passwords using Base64. ◆ **Digest** = encodes passwords using MD5. ◆ **SSL** = the page can only be accessed over SSL (no password is required). ◆ **SSL/Basic** = the page is accessible only over SSL and encodes passwords using Base64. ◆ **SSL/Digest** = the page is accessible only over SSL and encodes passwords using MD5. *Note: When changing the parameters of Digest or SSL Digest authentication, it is often best to close and reopen the browser to ensure it does not attempt to use cached authentication information.*

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 to the via an RSS publisher. The RSS feeds may also be stored to the file system cfg_log.txt file.

Table 9-6 **RSS Settings**

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

Note:

To Configure RSS Settings

Using Web Manager

- To configure RSS, 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">`

10: Security Settings

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.

For more information regarding certificates and how to obtain them, see the chapter, *Security in Detail on page 86*.

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

Certificate and Key Generation

The PremierWave 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 by a name provided at generation time.

Table 10-1 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. Note that 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, 2012 is entered as 05/09/2012.
Key length	Select the bit size of the new self-signed certificate. Choices are: ◆ 512 bits ◆ 768 bits ◆ 1024 bits ◆ 2048 bits The larger the bit size, the longer it takes to generate the key.

Certificate Generation Settings (continued)	Description
Type	Select the type of key: ◆ **RSA** = Public-Key Cryptography algorithm based on large prime numbers, invented by Rivest Shamir and Adleman. Used for encryption and signing. ◆ **DSA** = Digital Signature Algorithm also based on large prime numbers, but can only be used for signing. Developed by the US government to avoid the patents on RSA.

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.

Certificate Upload Settings

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

Table 10-2 Upload Certificate Settings

Upload Certificate Settings	Description
New Certificate	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 Private Key	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.

To Configure an Existing SSL Credential

Using Web Manager

- To configure an existing SSL Credential, click **SSL** in the menu and select **Credentials**.

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.

Table 10-3 Trusted Authority Settings

Trusted Authorities Settings	Description
Authority	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.

To Upload an Authority Certificate

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">`

11: Maintenance and Diagnostics Settings

Filesystem Settings

The PremierWave EN uses a flash file system to store files. Use the filesystem to list, view, add, remove, and transfer files.

File Display

It is possible to view the list of existing files, and to view their contents in the ASCII or hexadecimal formats.

Table 11-1 File Display Settings

File Display Commands	Description
ls	Displays a list of files on the PremierWave, 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 allows for the creation and removal of files on its filesystem.

Table 11-2 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 via the TFTP protocol. This can be useful for saving and restoring XML configuration files. Files can also be uploaded via HTTP.

Table 11-3 File Transfer Settings

File Transfer Settings	Description
Upload File	Browse to location of the file to be uploaded.
Action	Select the action that is to be performed via TFTP: **Get** = a “get” command will be executed to store a file locally. **Put** = a “put” command will be executed to send a file to a remote location.
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.

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, click **Filesystem** in the menu and select **Browse**.

Using the CLI

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

Using XML

- Not applicable.

IP Network 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.

Table 11-4 **IP Network 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.
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 Network 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">`

Table 11-5 ICMP Network Stack Settings

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

To Configure ICMP Network 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">`

Table 11-6 ARP Network Stack Settings

Protocol Stack ARP Settings	Description
IP Address	Enter the IP address to add to the ARP cache.
MAC Address	Enter the MAC address to add to the ARP cache.

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">`

Table 11-7 SMTP Network Stack Settings

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

To Configure SMTP Network Stack Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

Query Port

The query port (UDP port 0x77FE) is used for the automatic discovery of the device by the DeviceInstaller utility. Only 0x77FE discover messages from DeviceInstaller are supported. For more information on DeviceInstaller, see *Chapter 3: Using DeviceInstaller on page 21*.

Table 11-8 Query Port Settings

Query Port Settings	Description
Query Port Server	Enables or disables listening and responding to query port messages.

To Configure Query Port Settings

Using Web Manager

- To view Query Port settings or to switch the Query Port Server on or off, click **Query Port** in the menu.

Using the CLI

- To enter the Query Port command level: `enable -> config -> query port`

Using XML

- Include in your file:

  `<configgroup name="query port">`

  and

  `<configitem name="state">`

Diagnostics

The PremierWave EN 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 11-9 Ping Settings

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

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`

Using XML

- Not applicable.

Traceroute

Here you can trace a packet from the PremierWave EN 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 11-10 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 EN when issuing the traceroute command.

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`

Using XML

- Not applicable.

Log

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 Processes information 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">`

System Settings

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

Table 11-11 System Settings

System Settings	Description
Reboot Device	This reboots the device.
Restore Factory Defaults	This restores the device to the original factory settings. All configuration will be lost. The PremierWave EN automatically reboots upon setting back to the defaults.
Upload New Firmware	FTP to the PremierWave. Write the new firmware file to firmware.rom on the PremierWave. The device automatically reboots upon the installation of new firmware. See the section, *FTP Settings on page 59*.
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 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">`

12: Advanced Settings

Email Settings

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

Table 12-1 **Email Configuration**

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

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">`

Command Line Interface Settings

The Command Line Interface settings allow you to control how users connect to and interact with the PremierWave's command line. 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 12-2 CLI Configuration Settings

Command Line Interface Configuration Settings	Description
Login Password	Enter the password for logins by the admin account. The default password is "PASS".
Enable Level Password	Enter the password for access to the Command Mode Enable level. There is no password by default.
Quit Connect Line	Set the string used to terminate a connect line session and resume the CLI. Type <control> before any key to be pressed while holding down the Ctrl key, for 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	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 over the Telnet protocol.

Table 12-3 Telnet Settings

Telnet Settings	Description
Telnet State	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	Enable or disable authentication for telnet logins.

To Configure Telnet 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 Settings

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

Table 12-4 SSH Settings

SSH Settings	Description
state	Enable or disable CLI access via telnet.

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 allows for the configuration of units using an XML configuration record (XCR). Export a current configuration for use on other PremierWave ENs 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 12-5 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	Only use this with extreme caution. If selected, secret password and key information will be exported. Use only with a secure link, and save only in secure locations.
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.
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.

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 12-6 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.
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.

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.

Import Configuration from External File

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

Import Configuration from the 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.

Table 12-7 Import Configuration from Filesystem Settings

Import Configuration from Filesystem Settings	Description
Filename	Enter the name of the file on the PremierWave EN (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.
Groups to Import	Select the configuration groups to import from the XML configuration record. This option imports all instances of each selected group.
Text List	Enter the string to import specific instances of a group. The textual format of this string is: <g>:<i>;<g>:<i>;... Each group name <g> is followed by a colon and the instance value <i> and each <g>:<i> value is separated by a semi-colon. If a group has no instance then only the group name <g> should be specified.

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.

13: Bridging

PremierWave EN 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 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 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 13-1 Bridge Settings

WLAN Profile WPA & WPA2 Settings	Description
State	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. ***Note:*** *if a Bridging MAC Address is not configured, then once it is obtained and configured dynamically, it remains in effect until a reboot.*

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">`

14: 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 make use of SSL. The PremierWave EN 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 will use its own "personal" certificate. In verifying the authenticity of the other party, the PremierWave EN will use a "trusted authority" certificate.

In short:

- When using EAP-TLS, the PremierWave EN 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 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. 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 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.

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 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 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.

15: 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/documentation) or by using anonymous FTP (ftp://ftp.lantronix.com/).

Loading New Firmware

Firmware may be updated by sending the file to the PremierWave EN over a FTP connection. The destination file name on the PremierWave EN must be "firmware.rom". 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_7_0_0_0R8.rom firmware.rom
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.
```

16: VIP Settings

Virtual IP (VIP) Configuration

Configuring Connect Mode tunnels to use VIP is a simple matter of configuring a tunnel as is normally done, but also enabling VIP in the Tunnel Host settings, and using a VIP Name for the address.

VIP Accept Mode tunnels do not require special configuration. If VIP access is enabled (in VIP configuration), then VIP Accept Mode requests from a ManageLinx device will be accepted.

Table 16-1 VIP Configuration

VIP Settings	Description
State	Enable (or disable) the VIP State to allow Virtual IP addresses to be used in Tunnel Connect Mode and to accept incoming Virtual IP connection requests to any local listening port.

To Configure VIP Settings

Using Web Manager

- To configure VIP settings, click **VIP** on the menu and select **Configuration**.

Using the CLI

- To enter the VIP command level: `enable -> config -> vip`

Using XML

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

Virtual IP (VIP) Status

The VIP Status shows the current state of the conduit. When configured correctly, a conduit with the AccessMyDevice Gateway will be maintained at all times.

To View VIP Status

Using Web Manager

- Click **VIP** on the menu and select **Status**.

Using the CLI

- To enter the VIP command level: `enable -> config -> vip, show status`

Using XML

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

Virtual IP (VIP) Counters

Table 16-2 VIP Counters

VIP Counters	Description
Data Bytes	Total bytes in the TCP packets (not the UDP packets)
UDP Packet Queue	The number of packets queued for transmission.
UDP Packets	The number of packets transmitted. ***Note:*** *UDP counts are packet based, and do not record the number of data bytes.*

To View VIP Counters

Using Web Manager

- Click **VIP** on the menu and select **Counters**.

Using the CLI

- To enter the VIP command level: `enable -> config -> vip, show counters`

Using XML

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

17: Branding the PremierWave EN

This chapter describes how to brand your PremierWave EN 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 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>/config/index.html and http://<PremierWaveEN>/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 Web Manager. The names display in the CLI show command and in the System web page in the Current Configuration table. The short name is used for the show command. Both names display in the CLI Product Type field.

Table 17-1 Short and Long Name System Settings

System 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: Technical Support

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

Technical Support US

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

Technical Support Europe, Middle East, Africa

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

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

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

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

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 hexadecimals or to look up hexadecimal values in the tables of configuration options. The tables include:

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

Converting Binary to Hexadecimal

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

Conversion Table

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

Table 19-1 Binary to Hexadecimal Conversion

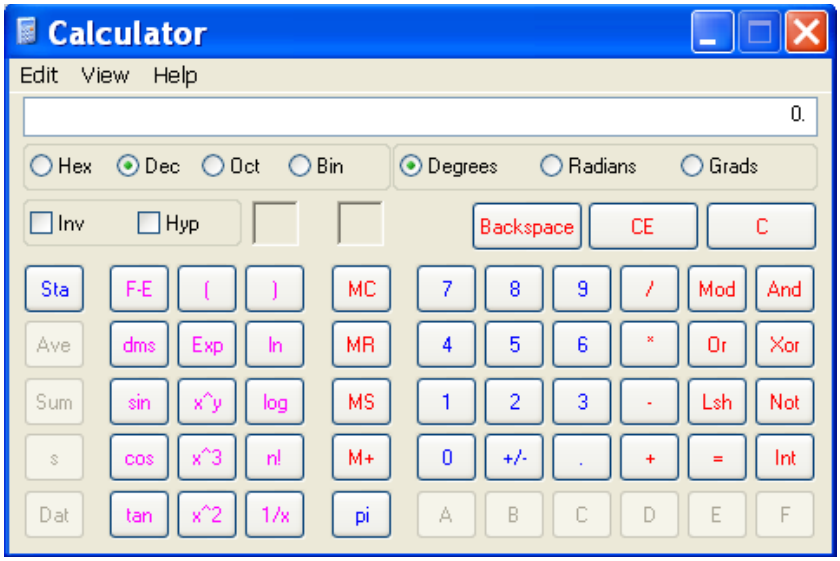
Decimal	Binary	Hex
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

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:

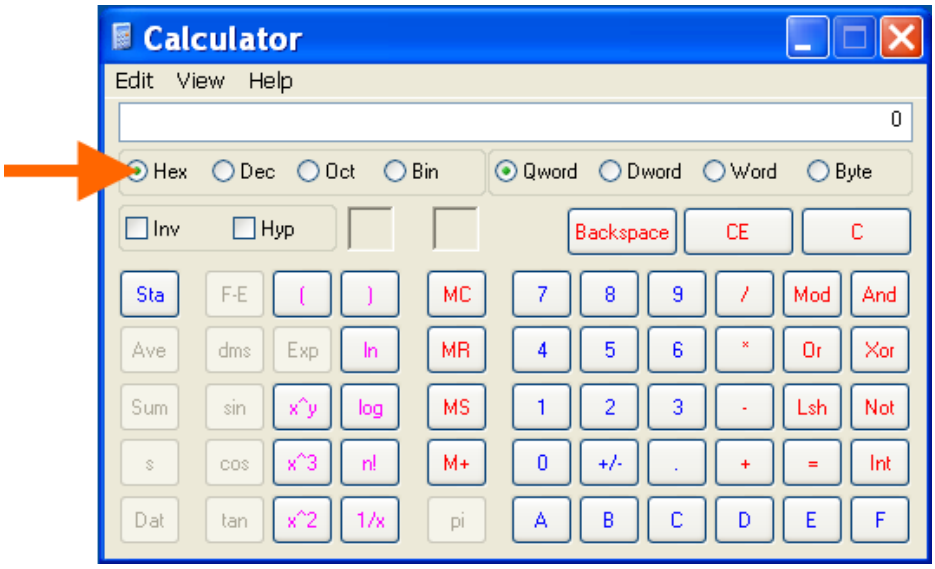
1. On the Windows Start menu, click **Programs -> Accessories -> Calculator**.
2. On the View menu, select **Scientific**. The scientific calculator appears.
3. Click **Bin** (Binary), and type the number you want to convert.

Figure 19-2 Windows Scientific Calculator



4. Click Hex. The hexadecimal value appears.

Figure 19-3 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
167 Technology Drive, Irvine, CA 92618 USA

Product Name Model:

PremierWave EN Embedded Device Server

Conforms to the following standards or other normative documents:

- FCC Part 15.247/15.407 Class B
- RSS-210
- RSS-Gen Issue 2
- ICES-003 Issue 4
- ETSI EN 301 489-1 V1.8.1
- ETSI EN 301 489-17 V1.3.2
- ETSI EN 300 328 V1.7.1
- ETSI EN 301 893 V1.5.1

Manufacturer's Contact:

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

RoHS Notice

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

- Lead (Pb)
- Cadmium (Cd)
- Mercury (Hg)
- Hexavalent Chromium (Cr (VI))
- Polybrominated biphenyls (PBB)
- Polybrominated diphenyl ethers (PBDE)

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

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

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

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

The following file may be used to enable Windows to recognize the USB-CDC-ACM connection to the PremierWave EN's USB Device port.

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

```
; 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"
```