LANTRONIX®

PremierWave® SE1000
Embedded System on Module
User Guide

Part Number 900-716-R
Revision A June 2014

Intellectual Property

© 2014 Lantronix, Inc. All rights reserved. No part of the contents of this book may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

Lantronix and *PremierWave* are registered trademarks of Lantronix, Inc. in the United States and other countries. *DeviceInstaller* is a trademark of Lantronix, Inc. U.S. Patents 7,309,260; 7,698,405; 8,024,446; 8,219,661; 8,504,740. Additional patents pending.

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

Warranty

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

Contacts

Lantronix, Inc.
Corporate Headquarters

167 Technology Drive
Irvine, CA 92618, USA

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

Technical Support

Online: www.lantronix.com/support

Sales Offices

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

Disclaimer

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

Revision History

Date	Rev.	Comments
June 2014	A	Initial document for firmware release 7.8.0.0.

Table of Contents

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 Lantronix® PremierWave® SE1000 system on module (SOM) and application server. It is intended for software developers and system integrators who are embedding this product into their designs.

Summary of Chapters

The remaining chapters in this guide include:

Chapter	Description
2: Introduction	Main features of the product and the protocols it supports. Includes technical specifications.
3: Device Discovery and Quick Setup	Instructions for viewing the device and configuration using UPnP and the DeviceInstaller utility.
4: Configuration Using Web Manager	Instructions for accessing Web Manager and using it to configure settings for the device.
5: Network Settings	Instructions for configuring network settings.
6: 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) including how to set the configurable pins to work with a device and instructions for accessing Web Manager and using it to configure settings for the device.
9: Network Services	Instructions for configuring DNS, FTP, HTTP and Syslog settings.
10: Updating Firmware	Instructions for obtaining and updating the latest firmware for the device.
11: Security Settings	Instructions for configuring SSL security settings.
12: Maintenance and Diagnostics Settings	Instructions to view statistics, files, and diagnose problems.
13: Management Interface Settings	Instructions for configuring CLI and XML settings.
14: Branding the PremierWave SE1000 Device	Instructions on how to brand your device.
Appendix A: Compliance	Lantronix compliance information.
Appendix B: Lantronix Technical Support	Instructions for contacting Lantronix Technical Support.
Appendix C: Binary to Hexadecimal Conversions	Instructions for converting binary values to hexadecimals.
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 SE1000 System on Module Integration Guide	Information about the PremierWave hardware, testing the device server using the demonstration board, and integrating the unit into your product.
PremierWave SE1000 System on Module Command Reference	Instructions for accessing Command Mode (the command line interface) using a Telnet connection or through the port. Detailed information about the commands. Also provides details for XML configuration and status.
PremierWave SE1000 System on Module Quick Start Guide	Instructions for getting the PremierWave device up and running.
PremierWave SE1000 System on Module Evaluation Board	Information needed to use the PremierWave on the evaluation board.
DeviceInstaller™ Utility Online Help	Instructions for using the Windows operating system-based utility to locate the system on module and to view its current settings.
Com Port Redirector Quick Start and Online Help	Instructions for using the Windows operating system-based utility to create virtual com ports.
Secure Com Port Redirector User Guide	Instructions for using the Windows operating system-based utility to create secure virtual com ports.

2: Introduction

The PremierWave SE1000 embedded system on module is a complete network-enabling solution in a 30 (1.181) X 55 (2.165) X 6.45 (0.248) package. This compact system on module empowers original equipment manufacturers (OEMs) to go to market quickly and easily with Ethernet and/or wireless networking and web page serving capabilities built into their products. *[DIMS = mm (in.)]*

Key Features

- **Power Supply:** Regulated 3.3V input required. There are internal step down regulators to convert to processor core and memory required voltages: a step-down converter to 1.5V for the processor core and 1.8V for the memory subsystem. All voltages have LC filtering to minimize noises and emissions.
- **Controller:** 32-bit ARM9 microprocessor running at 400 megahertz (Mhz) with 32 KB Data Cache and 32 Kilobytes (KB). Instruction Cache
- **Memory:** Up to 64 MB SDRAM, 256 MB NAND Flash (64 MB default). Up to 16 MB serial SPI Flash (8 MB default).
- **Ethernet:** 10/100 megabits per second (Mbps) Ethernet transceiver.
- **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.

Note: **External transceiver required for RS232, RS485, RS422 signaling.*

- **USB Ports:** Two USB 2.0 full speedOne USB 2.0 Full Speed (12 Mbps) host device port
- Master/Slave high speed SPI interface
- I2C interface
- Configurable I/O Pins (CPs): Up to nine pins are configurable as general purpose I/Os if no DTR or DCD is used on serial ports. Not 5V tolerant.
- Interface Signals: 3.3V-level interface signals.
- Configuration via CLI, XML and HTTP
- **Temperature Range:**Operates over a temperature range of -40°C to +85°C (-40°F to 158°F). The storage temperature range is -40°C to 85°C (-40°F to 185°F).

Applications

The PremierWave SE1000 embedded system on module is very suitable for these application scenarios:

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

Protocol Support

The PremierWave SE1000 embedded system on module contains a full-featured IP networking stack:

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

Troubleshooting Capabilities

ThePremierWave SE1000 device offers a comprehensive diagnostic toolset that lets you troubleshoot problems quickly and easily. Available from the CLI or Web Manager, the diagnostic tools let you:

- View critical hardware, memory, MIB-II, buffer pool, IP socket information and routing table
- Perform ping and traceroute operations
- Conduct forward or reverse DNS lookup operations

- View all processes currently running on the PremierWave SE1000 embedded system on module device including CPU utilization
- View system log messages

Configuration Methods

After installation, the PremierWave SE1000 unit requires configuration. For the unit to operate correctly on a network, it must have a unique IP address on the network. There are four basic methods for logging into the PremierWave SE1000 embedded system on module and assigning IP addresses and other configurable settings:

- **Web Manager**: View and configure all settings easily through a web browser using the Lantronix Web Manager. (See *Configuration Using Web Manager on page 24*.)
- **DeviceInstaller**: Configure the IP address and related settings and view current settings on the PremierWave SE1000 embedded system on module using a Graphical User Interface (GUI) on a PC attached to a network. You will need the latest version of the Lantronix® DeviceInstaller™ utility. (See *Accessing the PremierWave SE1000 Device Using DeviceInstaller on page 22*.)
- **Command Mode:** There are a few methods for accessing Command Mode (CLI): making a Telnet or SSH connection, or connecting a PC or other host running a terminal emulation program to the unit's serial port. (See the *PremierWave SE1000 Embedded System on Module Command Reference Guide* for instructions and available commands.)
- **XML:** The PremierWave SE1000 embedded system on module supports XML-based configuration and setup records that make device configuration transparent to users and administrators. XML is easily editable with a standard text or XML editor. (See the *PremierWave SE1000 Embedded System on Module Command Reference Guide* for instructions and commands.)

Addresses and Port Numbers

Hardware Address

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

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

IP Address

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

Port Numbers

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

The following is a list of the default server port numbers running on the PremierWave SE1000 embedded system on module:

- TCP Port 22: SSH Server (Command Mode configuration)
- TCP Port 23: Telnet Server (Command Mode configuration)
- TCP Port 80: HTTP (Web Manager configuration)
- TCP Port 443: HTTPS (Web Manager Configuration)
- UDP Port 161: SNMP
- TCP Port 21: FTP
- UDP Port 30718: LDP (Lantronix Discovery Protocol) port
- TCP/UDP Port 10001: Tunnel 1 (see note below)
- UDP Port 1900 and TCP Port 30179: UPnP

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

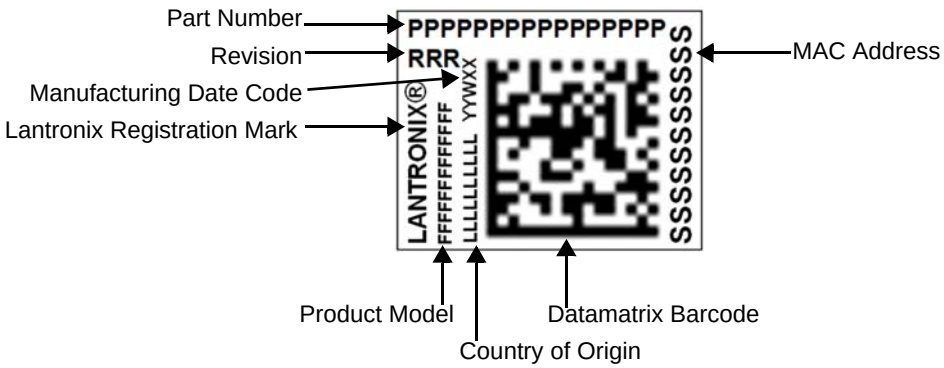
Product Information Label

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

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

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

Figure 2-1 PremierWave Unit Product Label



3: Device Discovery and Quick Setup

Software embedded within the PremierWave SE1000embedded system on module enables the device to be easily discovered via the Ethernet network without any knowledge of the IP address or default network configuration of the device.

The two methods supported are:

1. *Accessing the PremierWave SE1000 Device Using UPnP*
2. *Accessing the PremierWave SE1000 Device Using DeviceInstaller*

Accessing the PremierWave SE1000 Device Using UPnP

This section covers the steps for locating a PremierWave SE1000 unit and viewing its properties and device details using UPnP (Network Discovery). You may also use the DeviceInstaller utility to discover PremierWave SE1000 units. See *Accessing the PremierWave SE1000 Device Using DeviceInstaller on page 22*.

The PremierWave SE1000 units can be discovered automatically from Microsoft Windows® platforms using UPnP (Network Discovery). UPnP enables devices to be discovered and a refreshed list of devices available under "Network Places" within Windows Explorer as devices come online or go offline.

Using the operations described below, it becomes a "plug and play" mechanism to reach the device's Web UI (Web Manager) and complete the rest of the configuration.

Note: *There is no new software to install as UPnP support is built-into Windows operating systems, however it must be enabled on the Windows PC. Please see notes on enabling UPnP (Network Discovery) on Windows XP and Windows 7 operating systems.*

To search devices on Windows XP operating system:

1. Click **Start->My Network Places**. Lantronix PremierWave SE1000 devices will be listed like other network devices.
2. Double-click your device to view the device web page.

To search devices on Windows 7 operating system:

1. Click **Start->Computer->Network**. Lantronix PremierWave SE1000 devices will be listed like other network devices.
2. Double-click or right click your device and select "View device webpage " to view the device web page.

To view device properties on Windows XP operating system:

1. Click **Start->My Network Places**. Lantronix PremierWave SE1000 devices will be listed like other network devices.
2. Right click your device and select **Properties** to view the device properties.

To search device properties on Windows 7 operating system:

1. Click **Start->Computer->Network**. Lantronix PremierWave SE1000 devices will be listed like other network devices.
2. Right click your device and select **Properties** to view the device properties.

Accessing the PremierWave SE1000 Device Using DeviceInstaller

This section covers the steps for locating a PremierWave SE1000 unit and viewing its properties and device details. The DeviceInstaller application is a free utility program provided by Lantronix that discovers, configures, upgrades and manages Lantronix device servers.

Notes:

- *For instructions on using the DeviceInstaller utility to configure the IP address and related settings or for more advanced features, see the DeviceInstaller Online Help.*
- *Auto IP generates a random IP address in the range of 169.254.0.1 to 169.254.255.254, with a netmask of 255.255.0.0, if no BOOTP or DHCP server is found. These addresses are not routable.*
- *Accessing the PremierWave SE1000 Device Using UPnP on page 21*
- *Make note of the MAC address. It may be needed to perform various functions in 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 4.4 -> DeviceInstaller**.
3. When DeviceInstaller starts, it will perform a network device search. To perform another search, click **Search**.
4. Expand the PremierWave folder by clicking the + symbol next to the folder icon. The list of available Lantronix PremierWave devices appears.
5. Select the PremierWave 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 device configuration appears. This is only a subset of the full configuration; the full configuration may be accessed via Web Manager, CLI or XML.

Device Detail Summary

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

Current Settings	Description
Name	Shows PremierWave SE1000 device name.
DHCP Device Name	Displays one of the names the PremierWave SE1000 unit will send to the DHCP server if it is configured to obtain an address in this manner.
Group	Configurable field. Enter a group to categorize the PremierWave unit. Double-click the field, type in the value, and press **Enter** to complete. This group name is local to this PC and is not visible on other PCs or laptops using DeviceInstaller.

Current Settings	Description
Comments	Configurable field. Enter comments for the PremierWave unit. 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 device family type as “PremierWave”.
Short Name	Shows ”PWaveSE1000” by default.
Long Name	Shows “Lantronix PremierWave SE1000” by default.
Type	Shows the device type as “PremierWave SE1000”.
ID	Shows the “PremierWave“ ID embedded within the unit.
Hardware Address	Shows the PremierWave hardware (MAC) address.
Firmware Version	Shows the firmware currently installed on the PremierWave unit.
Extended Firmware Version	Provides additional information on the firmware version.
Online Status	Shows the PremierWave unit status as Online, Offline, Unreachable (the PremierWave is on a different subnet), or Busy (the PremierWave is currently performing a task).
IP Address	Shows the PremierWave 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 device 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 unit resides.
Gateway	Shows the IP address of the router of this network. There is no default.
Number of Serial Ports	Shows the number of serial ports on unit.
Supports Configurable Pins	Shows PremierWave server unit.
Supports Email Triggers	Shows True, indicating email triggers are available on the PremierWave unit
Telnet Supported	Indicates whether Telnet is enabled on this PremierWave unit.
Telnet Port	Shows the PremierWave port for Telnet sessions.
Web Port	Shows the PremierWave port for Web Manager configuration (if Web Enabled field is True).
Firmware Upgradeable	Shows True, indicating the PremierWave firmware is upgradable as newer versions become available.

4: Configuration Using Web Manager

This chapter describes how to configure the PremierWave SE1000 embedded system on module using Web Manager, the Lantronix browser-based configuration tool. The unit's configuration is stored in non-volatile memory and is retained without power. All changes take effect immediately, unless otherwise noted. It contains the following sections:

Accessing Web Manager

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

To access Web Manager, perform the following steps:

1. Open a standard web browser. Lantronix supports the latest versions of Internet Explorer, Mozilla Firefox, Safari or Chrome web browsers.
2. Enter the IP address or hostname of the PremierWave SE1000 unit in the address bar. The IP address may have been assigned manually using DeviceInstaller (see the *PremierWave SE1000 Embedded system on Module Quick Start Guide*) or automatically by DHCP.
3. Enter your username and password. The factory-default username is "**admin**" and "**PASS**" is the default password. The Device Status web page displays configurations including network settings, line settings, tunneling settings, and product information.

Device Status Page

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

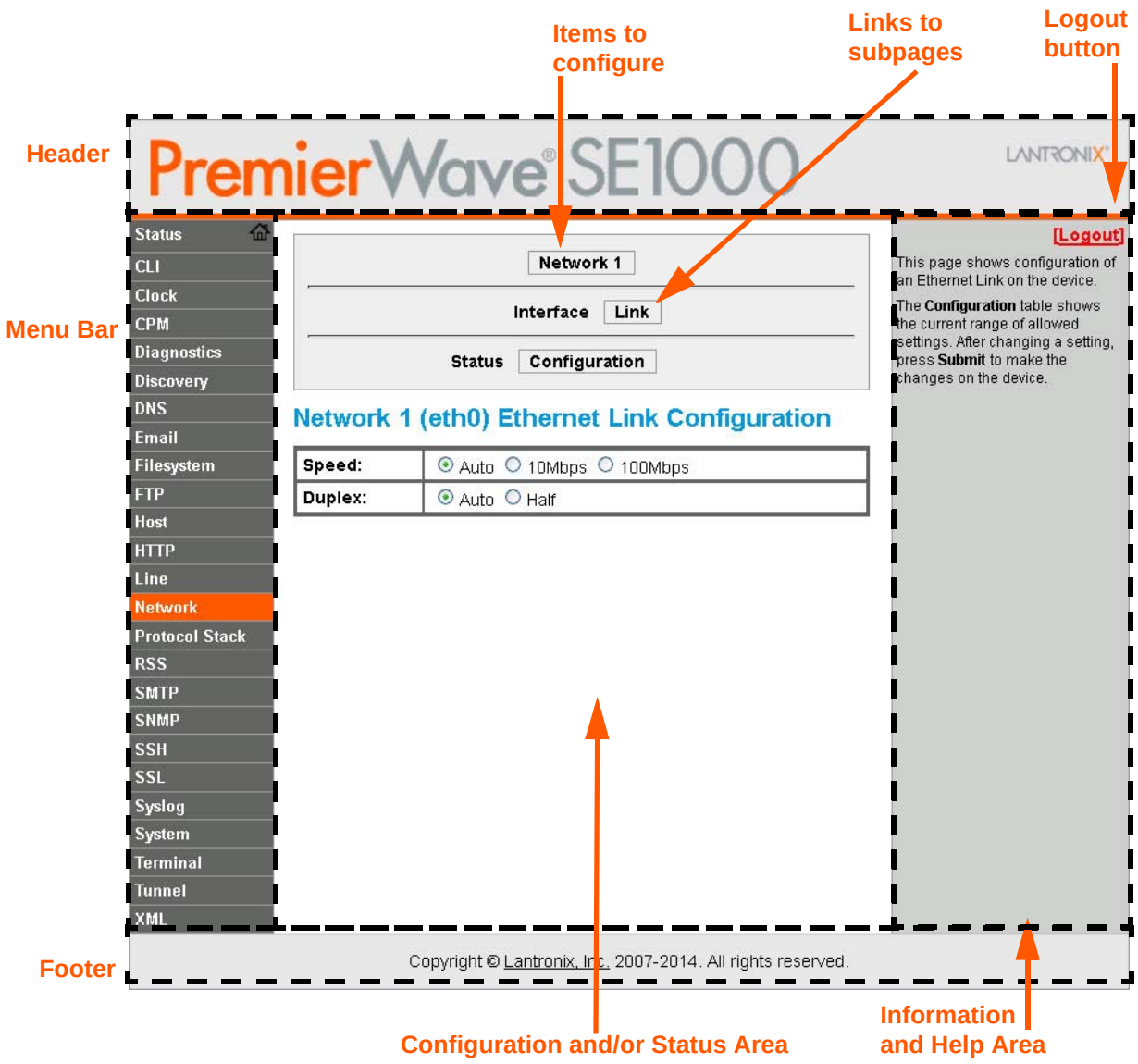
Figure 4-1 PremierWave Device Status Page

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

Web Manager Components

The layout of a typical Web Manager page is below.

Figure 4-2 Components of the Web Manager Page



Web Manager pages have these sections:

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

The main area of the page has these additional sections:

- Links near the top of many pages, such as the one in the example above, enable you to link to additional subpages. On some pages, you must also select the item you are configuring, such as a tunnel.

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

Navigating Web Manager

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

Note: *There may be times when you must reboot the PremierWave SE1000 device for the new configuration settings to take effect. The chapters that follow indicate when a change requires a reboot. Anytime you reboot the unit, this operation will take some time to complete. Please wait a minimum of 25-30 seconds after rebooting the unit before attempting to make any subsequent connections.*

Table 4-3 Web Manager Pages

Web Manager Page	Description	See Page
Status	Shows product information, network, , and tunneling settings.	*25*
CLI	Shows Command Line Interface (CLI) statistics and lets you change the current CLI configuration settings.	*81*
Clock	Allows you to view and configure the current date, time and time zone as it displays in web manager.	*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.	*48*
Diagnostics	Lets you perform various diagnostic procedures.	*75*
Discovery	Allows you to view and modify the configuration and statistics for device discovery.	*57*
DNS	Shows the current configuration of the DNS subsystem and the DNS cache.	*51*
Email	Shows email statistics and lets you clear the email log, configure email settings, and send an email.	*58*
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.	*71*

Web Manager Page (continued)	Description	See Page
FTP	Shows statistics and lets you change the current configuration for the File Transfer Protocol (FTP) server.	*52*
Host	Lets you view and change settings for a host on the network.	*46*
HTTP	Shows HyperText Transfer Protocol (HTTP) statistics and lets you change the current configuration and authentication settings.	*53*
Line	Shows statistics and lets you change the current configuration and Command mode settings of a serial line.	*33*
Network	Shows status and lets you configure the network interface.	*29*
Protocol Stack	Lets you perform lower level network stack-specific activities.	*73*
RSS	Lets you change current Really Simple Syndication (RSS) settings.	*55*
SMTP	Shows and allows modification of the current configuration of SMTP.	*58*
SNMP	Shows and allows modification of the current configuration of SNMP.	*56*
SSH	Lets you change the configuration settings for SSH server host keys, SSH server authorized users, SSH client known hosts, and SSH client users.	*64*
SSL	Lets you upload an existing certificate or create a new self-signed certificate.	*67*
Syslog	Lets you specify the severity of events to log and the server and ports to which the syslog should be sent.	*52*
System	Lets you reboot device, restore factory defaults, upload new firmware, and change the device long and short names.	*79*
Terminal	Lets you change current settings for a terminal.	*45*
Tunnel	Lets you change the current configuration settings for an incoming tunnel connection.	*35*
XML	Lets you export XML configuration and status records, and import XML configuration records.	*82*

5: Network Settings

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

PremierWave SE1000 Ethernet interface is also called Network 1 or eth0.

Notes:.

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

Network 1 (Ethernet "eth0") Interface Settings

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

Table 5-1 .Network Interface Settings

Network Interface Settings	Description
BOOTP Client	Select to turn **On** or **Off**. At boot up, after the physical link is up, the device will attempt to obtain IPv4 settings from a BOOTP server. ***Note:*** *Overrides the configured IPv4 address/mask, gateway, hostname, and domain. When DHCP is **Enabled**, the system automatically uses DHCP, regardless of whether BOOTP is **Enabled**. Changing this value requires you to reboot the device.*
DHCP Client	Select to turn **On** or **Off**. At boot up, after the physical link is up, the PremierWave SE1000 unit will attempt to obtain IPv4 settings from a DHCP server and will periodically renew these settings with the server. ***Note:*** *Overrides BOOTP, the configured IPv4 address/mask, gateway, hostname, and domain. Changing this value requires you to reboot the device.* ***Note:*** *Within Web Manager, click **Renew** to renew the DHCP lease.*
IP Address	Enter the static IPv4 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 Disabled). Changing this value requires you to reboot the device. When DHCP or BOOTP is enabled, the PremierWave SE1000 device tries to obtain an IPv4 address from a DHCP or BOOTP server. If it cannot, the PremierWave SE1000 unit generates and uses an Auto IP address in the range of 169.254.xxx.xxx, with a network mask of 255.255.0.0.*
Default Gateway	Enter the IPv4 address of the router for this network. ***Note:*** *This setting will be used if Static IP is active (both DHCP and BOOTP are **Disabled**).*

Network Interface Settings (continued)	Description
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. 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 SE1000 embedded system on module 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 to 1500 bytes, the default being 1500 bytes.

To Configure Network 1 Interface Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

To View Network 1 Interface Status

Using Web Manager

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

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

Network 1 (Ethernet “eth0”) Link Settings

Physical link parameters can be configured for an Ethernet (eth0) Network Interface (see *Table 5-2*).

Table 5-2 Network 1 (eth0) Link Settings

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

Notes:

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

To Configure Network 1 Link Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

WAN MAC Address Filters

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

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

6: Line and Tunnel Settings

The PremierWave SE1000 embedded system on module contains three serial lines. All lines use standard RS232/RS485 serial ports, except Line 3 which is an emulated serial port over the USB Device (USB-CDC-ACM). All lines (except Line 3) can be configured to operate in the following modes:

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

Note: *External transceiver required for RS232, RS485, and RS422 signaling.*

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 SE1000 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 SE1000 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 SE1000 unit is rebooted, some terminal programs under Linux will automatically disconnect while others will not. If a terminal program does not disconnect automatically, when the PremierWave SE1000 device 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).

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	Set the interface type for the Line. The default is **RS232**, and **USB-CDC-ACM** for Line 3. Choices are: ◆ **RS232** ◆ **RS485 Full-Duplex** ◆ **RS485 Half-Duplex** ◆ **USB-CDC-ACM** (Line 3 only) = CDC-ACM over USB
Termination	Select to **Enable** or **Disable** Line Termination. The default is **Disable**. ***Note:*** *This setting is only relevant for Interface type RS485 Half-Duplex.*
State	Select to **Enable** or **Disable** the operational state of the Line. The default is **Enabled**.
Protocol	Set the operational protocol for the Line. The default is **Tunnel**. Choices are: ◆ **None** ◆ **Tunnel** = Serial-Network tunneling protocol.
Baud Rate	Set the Baud Rate (speed) of the Line. The default is **9600**. Any set speed between 300 and 921600 may be selected: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600. When selecting a Custom baud rate, you may manually enter any value between 300 and 5000000. ***Note:*** *The maximum baud rate in RS232 mode is 1000000 bps. Custom baud rates are not supported when a line is configured for Command Mode. For Interface type USB-CDC-ACM (Line 3 only), this setting is irrelevant.*
Parity	Set 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	Set 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	Set 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	Set the flow control for the Line. The default is **None**. ***Note:*** *For Interface type USB-CDC-ACM (Line 3 only), this setting is irrelevant. This field becomes available if RS232 or RS485 Full-Duplex is selected under Interface above.*

Line Settings	Description
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>. ***Note:*** *This field becomes available for configuration when Software is selected under Flow 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>. ***Note:*** *This field becomes available for configuration when Software is selected under Flow 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 msec).
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	Set 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). Also, custom baud rates are not supported in Command Mode.*
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 sent on the Serial Line and applies only if mode is “Use Serial String”. ***Note:*** *This field becomes available when Use Serial String is selected for Mode.*
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]. ***Note:*** *This field becomes available when Use Serial String is selected for Mode.*
Echo Serial String	Select **Enable** or **Disable** for Echo Serial String. Applies only if mode is “User Serial String”. Select enable to echo received characters backed out on the line while looking for the serial string. ***Note:*** *This field becomes available when Use Serial String is selected for Mode.*
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 Line 1, click **Line** in the menu and select **Line 1 -> Statistics**.

Using the CLI

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

Using XML

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

Tunnel Settings

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

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

Serial Settings

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

Table 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	Set the threshold (byte count). If the received serial data reaches this threshold, then the data will be sent on the network. Valid range is 100 to 1450 bytes. Default is 512.

Tunnel Packing Mode Settings (continued)	Description
Timeout	Set the timeout value, in milliseconds, after the first character is received on the serial line, before data is sent on the network. Valid range is 1 to 30000 milliseconds. Default is 1000.
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 Trailing Character is a single printable character or a control character that is injected into the outgoing data stream right after the Send Character. Disable the Trailing Character by blanking the field (setting it to <None>).

To Configure Tunnel Packing Mode Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

Accept Mode

In Accept Mode, the PremierWave SE1000 embedded system on module device listens (waits) for incoming connections from the network. A remote node on the network initiates the connection.

The configurable local port is the port the remote device connects to for this connection. There is no remote port or address. Supported serial lines and associated local port numbers progress sequentially in matching value. For instance, the default local port is 10001 for serial line 1 and the default local port for serial line 2 is 10002, and so on for the number of serial lines supported.

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

Table 6-5 Tunnel Accept Mode Settings

Tunnel Accept Mode Settings	Description
Mode	Set 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	Set the port number for use as the network local port. The default local port number for each supported serial line number progresses sequentially in equal value so that Tunnel X: 1000X. For example: ◆ Tunnel 1: 10001 ◆ Tunnel 2: 10002 ◆ Tunnel 3: 10003
Protocol	Select the protocol type for use with Accept Mode: ◆ SSH ◆ SSL ◆ TCP (default protocol) ◆ TCP AES ◆ Telnet ***Note:*** *Tunnel 3 does not support Telnet protocol.*
Credentials	Specifies the name of the set of RSA and/or DSA certificates and keys to be used for an SSL connection.
AES Encrypt Key	Specify the text or hexadecimal advanced encryption standard (AES) key for encrypting outgoing data for a TCP AES connection.
AES Decrypt Key	Specify the text or hexadecimal AES key for decrypting incoming data for a TCP AES connection.
TCP Keep Alive	Enter the time, in milliseconds, the PremierWave SE1000module waits during a silent TCP connection before checking if the currently connected network device is still on the network. If the unit gets no response after 1 attempt, it drops the connection. Enter 0 to disable.
Flush Serial	Set 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.

Tunnel Accept Mode Settings (continued)	Description
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** and a password is provided, the user will be prompted for the password upon connection.
Prompt for Password	Select **Enabled** or **Disabled** (to enable or disable). This option will only appear if a password is specified above.
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 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 SE1000 embedded system on module continues to attempt an outgoing connection on the network, until established (based on which connection method is selected in the configuration described in *Table 6-6*). If the connection attempt fails or the connection drops, then it retries after a timeout. The remote node on the network must listen for the Connect Mode's connection.

For Connect Mode to function, it must be enabled, have a remote station (node) configured, and a remote port configured (TCP or UDP). When established, Connect Mode is always on. Enter the remote station as an IPv4 or IPv6 address or DNS name. The PremierWave SE1000 embedded system on module device will not make a connection unless it can resolve the address. For Connect Mode using UDP, the PremierWave SE1000 embedded system on module module accepts packets from any device on the network. It will send packets to the last device that sent it packets.

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

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

Table 6-6 Tunnel Connect Mode Settings

Tunnel Connect Mode Settings	Description
Mode	Set the method to be used to attempt a connection to a remote host or device. Choices are: ◆ **Disable** = an outgoing connection is never attempted. (*default*) ◆ **Always** = a connection is attempted until one is made. If the connection gets disconnected, the deviceretries until it makes a connection. ◆ **Any Character** = a connection is attempted when any character is read on the serial line. ◆ **Start Character** = a connection is attempted when the start character for the selected tunnel is read on the serial line. ◆ **Modem Control Asserted** = a connection is attempted as long as the Modem Control pin (DSR) is asserted, until a connection is made. ◆ **Modem Emulation** = a connection is attempted when triggered by modem emulation AT commands.
Local Port	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. Once you start to edit Host 1, a box for Host 2 will show up. Editing Host 2 will cause a Host 3 box to appear. Up to 16 hosts are available. ***Note:*** *Tunnel 3 does not support Telnet protocol.*
Host Mode	Once a host is added, a box will appear that will allow you select whether all of the hosts are connected at once (Simultaneous) or if only the first host on the list is connected (Sequential), trying the next host in the list only if the first connection fails.

Tunnel Connect Mode Settings (continued)	Description
Reconnect Timer	Set the value of the reconnect timeout (in milliseconds) for outgoing connections established by the device. Valid range is 1 to 65535 milliseconds. Default is 15000.
Flush Serial Data	Set whether the serial Line data buffer is flushed upon a new network connection. Choices are: ◆ **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.
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)

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

To Configure the Terminal Network Connection

Using Web Manager

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

Using the CLI

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

Using XML

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

To Configure the Terminal Line Connection

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

Using Web Manager

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

Using the CLI

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

Using XML

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

Host Configuration

Table 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.*

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

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 SE1000 embedded system on module. There are configurable pins on the PremierWave SE1000 device.

You must configure the CPs by making them part of a group. A CP Group may consist of one or more CPs. This increases flexibility when incorporating the PremierWave SE1000 embedded system on module 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			<available>
CP2	Pin 16	Input	1	0	<available>
CP3	Pin 18	Input	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.

CPM – CPs Status	Description
Bit	Visual display of the bitwise 32 bit placeholders for a CP.
Level	A "**+**" symbol indicates the CP is asserted (the voltage is high). A "**-**"indicates the CP voltage is low.
I/O	Indicates the current status of the pin: ◆ **I** = input ◆ **O** = output ◆ **<blank>** = unassigned
Logic	An "**l**" 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: Network Services

DNS Settings

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

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

Table 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 SE1000 embedded system on module 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: ◆ **Enabled** (default) ◆ **Disabled**

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 file system is enabled. Saving the system log to a server that supports remote logging services (see RFC 3164) allows the administrator to save the complete system log history. The default port is 514.*

Table 9-3 Syslog Settings

Syslog Settings	Description
State	Select to enable or disable the syslog: ◆ **Enabled** ◆ **Disabled** (default)
Host	Enter the IP address of the remote server to which system logs are sent for storage.
Remote Port	Enter the number of the port on the remote server that supports logging services. The default is 514.

Syslog Settings (continued)	Description
Severity Log Level	Specify the minimum level of system message the PremierWave device should log. 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	Select to enable or disable the HTTP server: ◆ **Enabled** (default) ◆ **Disabled**
Port	Enter the port for the HTTP server to use. The default is **80**.
Secure Port	Enter the port for the HTTPS server to use. The default is **443**. The HTTP server only listens on the **HTTPS Port** when an SSL certificate is configured.
Secure Protocols	Select to enable or disable the following protocols: ◆ **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.

HTTP Settings (continued)	Description
Max Timeout	Enter the maximum time for the HTTP server to wait when receiving a request. This prevents Denial-of-Service (DoS) attacks. The default is **10** seconds.
Max Bytes	Enter the maximum number of bytes the HTTP server accepts when receiving a request. The default is **40** KB (this prevents DoS attacks). ***Note:*** You may need to increase this number in some cases where the browser is sending data aggressively within TCP windows size limit, when file (including firmware upgrade) is uploaded from webpage.
Logging State	Select to enable or disable HTTP server logging: ◆ **Enabled** (default) ◆ **Disabled**
Max Log Entries	Set the maximum number of HTTP server log entries. Only the last **Max Log Entries** are cached and viewable.
Log Format	Set the log format string for the HTTP server. Follow these **Log Format** rules: ◆ **%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.*
Auth Type	Select the authentication type: ◆ **None** = no authentication is necessary. ◆ **Basic** = encodes passwords using Base64. ◆ **Digest** = encodes passwords using MD5. ◆ **SSL** = can only be accessed over SSL (no password is required). ◆ **SSL/Basic** = is accessible only over SSL and encodes passwords using Base64. ◆ **SSL/Digest** = is accessible only over SSL and encodes passwords using MD5. ***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 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** or **Off** for RSS feeds to an RSS publisher. The default setting is off.
Persistent	Select **On** or **Off** for RSS feed to be written to a file (cfg_log.txt) and to be available across reboots. The default setting is off.
Max Entries	Set the maximum number of log entries. Only the last **Max Entries** are cached and viewable.
View	Click the button to view RSS feeds.

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

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">`

SNMP Settings

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

Table 9-7 SNMP Settings

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

To Configure SNMP Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

Discovery

The current statistics and configuration options for device discovery, including Query Port are available for the PremierWave SE1000 embedded system on module.

Table 9-8 Discovery Settings

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

To Configure Discovery

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

Using Web Manager

- To access the area with options to configure discovery, click **Discovery** in the menu.

Using the CLI

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

Using XML

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

SMTP Settings

Table 9-9 SMTP Settings

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

To Configure SMTP Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

Email Settings

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

Table 9-10 **Email Configuration**

Email – Configuration Settings	Description
From	Click this link to configure SMTP: *SMTP Settings (on page 58)*.
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 (;).
Reply To	Enter the email address to list in the Reply-To field of the email alert.

Email – Configuration Settings (continued)	Description
Subject	Enter the subject for the email alert.
Message File	Enter the path of the file to send with the email alert. This file appears within the message body of the email.
Priority	Select the priority level for the email alert: ◆ Urgent ◆ High ◆ Normal ◆ Low ◆ Very Low
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”>`

10: Updating Firmware

Obtaining Firmware

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

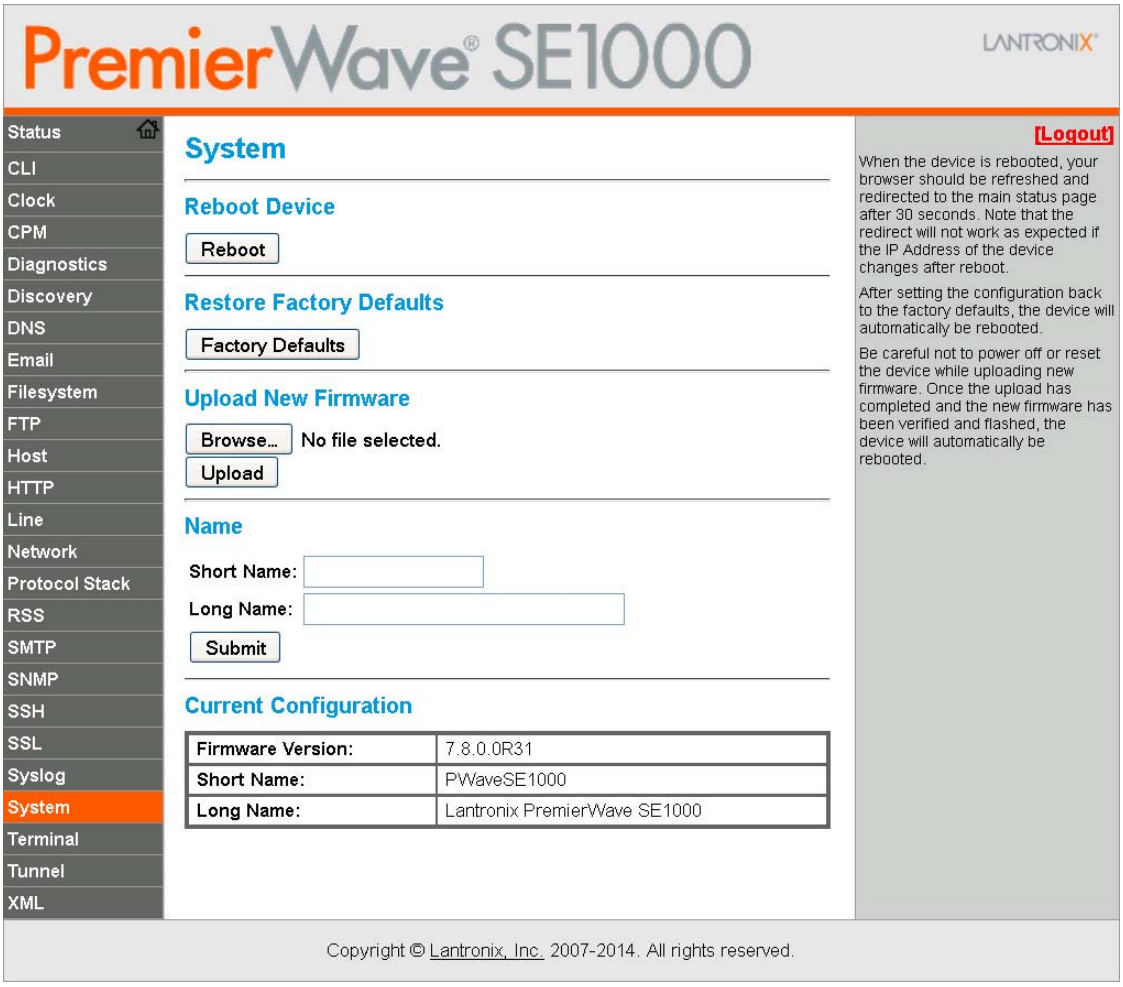
Loading New Firmware through Web Manager

Upload the firmware using the device web manager **System** page.

To upload new firmware:

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

Figure 10-1 Uploading New Firmware



2. Click **Browse** (under the **Upload New Firmware** heading) to browse to the firmware file.
3. Select the file and click **Open**.
4. Click **Upload** to install the firmware on the PremierWave SE1000 unit.
5. Click **OK** in the confirmation popup which appears. The firmware will be installed and the device will automatically reboot afterwards.
6. Close and reopen the web manager internet browser to view the device's updated web pages.

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

Loading New Firmware through FTP

Firmware may be updated by sending the file to the PremierWave SE1000 embedded system on module over an FTP connection. The destination file name on the PremierWave SE1000 unit must have a "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_se1000_7.8.0.0r31.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.
```

11: Security Settings

The PremierWave SE1000 device supports Secure Shell (SSH) and Secure Sockets Layer (SSL). SSH is a network protocol for securely accessing a remote device. SSH provides a secure, encrypted communication channel between two hosts over a network. It provides authentication and message integrity services.

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

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

Public Key Infrastructure

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

TLS (SSL)

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

SSH and some wireless authentication methods on the PremierWave SE1000 embedded system on module make use of SSL. The PremierWave SE1000 unit supports SSLv2, SSLv3, and TLS1.0.

TLS/SSL application hosts use separate digital certificates as a basis for authentication in both directions: to prove their own identity to the other party, and to verify the identity of the other party. In proving its own authenticity, the PremierWave SE1000 embedded system on module will use its own "personal" certificate. In verifying the authenticity of the other party, the PremierWave SE1000 device will use a "trusted authority" certificate.

In short:

- When using EAP-TLS, the PremierWave SE1000 embedded system on module needs a personal certificate with matching private key to identify itself and sign its messages.
- When using EAP-TLS, EAP-TTLS or PEAP, the PremierWave SE1000 unit needs the authority certificate(s) that can authenticate those it wishes to communicate with.

Digital Certificates

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

Trusted Authorities

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

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

Obtaining Certificates

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

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

Self-Signed Certificates

A few utilities exist to generate self-signed certificates or sign certificate requests. The PremierWave SE1000 embedded system on module also has the ability to generate its own self-signed certificate/key combo. You can use XML to export the certificate in PEM format, but you cannot export the key. Hence, the internal certificate generator can only be used for certificates that are to identify that particular PremierWave SE1000 module.

Certificate Formats

Certificates and private keys can be stored in several file formats. Best known are PKCS12, DER and PEM. Certificate and key can be in the same file or in separate files. Additionally, the key can be either be encrypted with a password or left in the clear. However, the PremierWave SE1000 embedded system on module currently only accepts separate PEM files, with the key unencrypted.

Several utilities exist to convert between the formats.

OpenSSL

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

OpenSSL is available in binary form for Linux and Windows.

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

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

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

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

SSH Settings

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

Two instances require configuration: when the PremierWave SE1000 device is the SSH server and when it is an SSH client. The SSH server is used by the CLI (Command Mode) and for tunneling in Accept Mode. The SSH client is for Mode.

To configure the PremierWave SE1000 embedded system on module as an SSH server, there are two requirements:

- **Defined Host Keys:** both private and public keys are required. These keys are used for the Diffie-Hellman key exchange (used for the underlying encryption protocol).
- **Defined Users**: these users are permitted to connect to the PremierWave SE1000 device SSH server.

SSH Server Host Keys

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

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

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

Table 11-1 SSH Server Host Keys

SSH Settings	Description
Private Key	Enter the path and name of the existing private key you want to upload. In Web Manager, you can also browse to the private key to be uploaded. Be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.

SSH Settings (continued)	Description
Public Key	Enter the path and name of the existing public key you want to upload. In Web Manager, you can also browse to the public key to be uploaded.
Key Type	Select a key type to use for the new key: ◆ RSA ◆ DSA
Bit Size	Select a bit length for the new key: ◆ 512 ◆ 768 ◆ 1024

Note: *SSH Keys from other programs may be converted to the required PremierWave SE1000 unit format. Use Open SSH to perform the conversion.*

SSH Client Known Hosts

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

Table 11-2 SSH Client Known Hosts

SSH Settings	Description
Server	Specify either a DNS Hostname or IP Address when adding public host keys for a Server. This Server name should match the name used as the Remote Address in .
Public RSA Key	Enter the path and name of the existing public RSA key you want to use with this user. In Web Manager, you can also browse to the public RSA key to be uploaded. If authentication is successful with the key, no password is required.
Public DSA Key	Enter the path and name of the existing public DSA key you want to use with this user. In Web Manager, you can also browse to the public DSA key to be uploaded.If authentication is successful with the key, no password is required.

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

SSH Server Authorized Users

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

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

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

Table 11-3 SSH Server Authorized Users

SSH Settings	Description
Username	Enter a new username or edit an existing one.
Password	Enter a new password or edit an existing one.
Public RSA Key	Enter the path and name of the existing public RSA key you want to use with this user. In Web Manager, you can also browse to the public RSA key to be uploaded. If authentication is successful with the key, no password is required.
Public DSA Key	Enter the path and name of the existing public DSA key you want to use with this user. In Web Manager, you can also browse to the public DSA key to be uploaded.If authentication is successful with the key, no password is required.

SSH Client Users

The SSH Client Users are used by all applications that play the role of an SSH Client. Specifically Mode. To configure the PremierWave SE1000 embedded system on module as an SSH client, an SSH client user must be both configured and also exist on the remote SSH server.

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

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

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

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

Table 11-4 SSH Client Users

SSH Settings	Description
Username	Enter the name that the device uses to connect to an SSH server.
Password	Enter the password associated with the username.
Remote Command	Enter the command that can be executed remotely. Default is shell, which tells the SSH server to execute a remote shell upon connection. This command can be changed to anything the remote host can perform.
Private Key	Enter the path and name of the existing private key you want to upload. In Web Manager, you can also browse to the private key to be uploaded. Be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.
Public Key	Enter the path and name of the existing public key you want to upload. In Web Manager, you can also browse to the public key to be uploaded.
Key Type	Select a bit length for the key: ◆ RSA ◆ DSA

SSH Settings (continued)	Description
Bit Size	Select the bit length of the new key: ◆ 512 ◆ 768 ◆ 1024 Using a larger Bit Size takes more time to generate the key. Approximate times are: ◆ 1 second for a 512 bit RSA key ◆ 1 second for a 768 bit RSA key ◆ 1 second for a 1024 bit RSA key ◆ 2 seconds for a 512 bit DSA key ◆ 2 seconds for a 768 bit DSA key ◆ 20 seconds for a 1024 bit DSA key ***Note:*** *Some SSH clients require RSA host keys to be at least 1024 bits long. This device generates keys up to 2048 bits long.*

To Configure SSH Settings

Using Web Manager

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

Using the CLI

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

Using XML

- Include in your file: `<configgroup name="ssh">`
  and
  `<configgroup name="ssh server">`
  and
  `<configgroup name="ssh client">`

SSL Settings

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

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

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

Certificate and Key Generation

The PremierWave SE1000 embedded system on module can generate self signed certificates and their corresponding keys. This can be done for both the rsa and dsa certificate formats. Certificates can be identified on the PremierWave SE1000 unit by a name provided at generation time.

Table 11-5 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, preferrably matching the host name or the ip address of the device, whichever will be the intended access approach. This is a required field.
Expires	Enter the expiration date, in mm/dd/yyyy format, for the new self-signed certificate. Example: An expiration date of May 9, 2012 is entered as 05/09/2012.
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.
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.

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 SE1000 embedded system on module to peers. Certificate and key pairs can be uploaded to the PremierWave SE1000 unit through either the CLI or XML import mechanisms. Certificates can be identified on the PremierWave SE1000 embedded system on module by a name provided at upload time.

Table 11-6 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 Certificate Type	Select the certificate type being uploaded: ◆ PEM ◆ PKCS7 ◆ PKCS12 ◆ None
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.
New Key Type	Select the key type being uploaded: ◆ PEM ◆ PKCS12 ◆ None

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. These certificates do not require a private key.

Table 11-7 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.
Authority Certificate Type	This field will be automatically updated depending upon extension of the certificate entered. If the field is NONE i.e., certificate is not supported then it will not load. If the field is PKCS12, In the Password: field corresponding PKCS12 password should be entered.
Delete	Click the **Delete** button beside a specific certificate authority to delete it.

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">`

12: Maintenance and Diagnostics Settings

Filesystem Settings

Use the file system to list, view, create, upload, copy, move, remove, and transfer files. The PremierWave SE1000 embedded system on module uses a flash file system to store 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 12-1 File Display Settings

File Display Commands	Description
ls	Displays a list of files on the PremierWave SE1000 device, and their respective sizes.
cat	Displays the specified file in ASCII format.
dump	Displays the specified file in a combination of hexadecimal and ASCII formats.
pwd	Print working directory.
cd	Change directories.
show tree	Display file/directory tree.

To Display Files

Using Web Manager

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

Using the CLI

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

Using XML

- Not applicable.

File Modification

The PremierWave SE1000 embedded system on module allows for the creation and removal of files on its filesystem.

Table 12-2 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 SE1000 device via the TFTP protocol. This can be useful for saving and restoring XML configuration files. Files can also be uploaded via HTTP.

Table 12-3 File Transfer Settings

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

Protocol Stack Settings

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

IP Settings

Table 12-4 **IP Protocol Stack Settings**

Protocol Stack IP Settings	Description
IP Time to Live	This value typically fills the Time To Live in the IP header. 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 Protocol Stack Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

ICMP Settings

Table 12-5 ICMP Protocol 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 Protocol Stack Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

ARP Settings

Table 12-6 ARP Protocol 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.
Remove	Click the **Remove** link beside a specific address to remove it.
Remove All	Click the **Remove All** link underneath all listed addresses to remove all the addresses.

To Configure ARP Network Stack Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

Diagnostics

The PremierWave SE1000 embedded system on module has several tools for diagnostics and statistics. Various options allow for the configuration or viewing of IP socket information, ping, traceroute, memory, and processes.

Hardware

To View Hardware Information

Using Web Manager

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

Using the CLI

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

Using XML

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

IP Sockets

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

To View the List of IP Sockets

Using Web Manager

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

Using the CLI

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

Using XML

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

Ping

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

Table 12-7 Ping Settings

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

Timeout	Enter the time, in seconds, for the PremierWave to wait for a response from the host before timing out. The default is **5** seconds.

To Ping a Remote Host

Using Web Manager

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

Using the CLI

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

Using XML

- Not applicable.

Traceroute

Here you can trace a packet from the PremierWave SE1000 embedded system on module to an Internet host, showing how many hops the packet requires to reach the host and how long each hop takes. If you visit a web site whose pages appear slowly, you can use traceroute to determine where the longest delays are occurring.

Table 12-8 Traceroute Settings

Diagnostics: Traceroute Settings	Description
Host	Enter the IP address or DNS hostname. This address is used to show the path between it and the PremierWave device when issuing the traceroute command.
Protocol	Specify the traceroute protocol.

To Perform a Traceroute

Using Web Manager

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

Using the CLI

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

Using XML

- Not applicable.

Log

Table 12-9 Log Settings

Diagnostics: Log	Description
Output	Select a diagnostic log output type: ◆ **Disable** - Turn off the logging feature. ◆ **Filesystem** - Directs logging to /log.txt. ◆
Max Length	Set the maximum length of the log.txt file. Valid length is 10 to 1000Kbytes. ***Note:*** *This setting becomes available when Filesystem is selected.*

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 SE1000 device shows all the processes currently running on the system. It shows the Process ID (PID), Parent Process ID (PPID), user, CPU percentage, percentage of total CPU cycles, and process command line information.

To View Process Information

Using Web Manager

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

Using the CLI

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

Using XML

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

Threads

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

To View Thread Information

Using Web Manager

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

Using the CLI

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

Clock

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

Table 12-10 Clock Settings

Clock	Description
Method	Select a clock change method: ◆ **Manual:** this option allows you to directly set the date and time. ◆ **SNTP:** this option keeps the time synchronized with the NTP Server.
Date	Use the drop-down menu to select the **Year**, **Month** and **Day**. This option becomes available when the **Manual** method is selected.
Time (24 hour)	Use the drop-down menu to select the **Hour**, **Min** and **Sec**. This option becomes available when the **Manual** method is selected.

Time Zone	Select the **Time Zone** of the device according to Coordinated Universal Time (UTC). Syslog and other applications may use UTC. The UTC offset form is HHMM (H=hour, M=minute). Device will make seasonal changes required for daylight savings time.

To Specify Clock Setting Method

Using Web Manager

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

Using the CLI

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

Using the XML

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

System Settings

The PremierWave SE1000 embedded system on module system settings allow for rebooting the device, restoring factory defaults, uploading new firmware and updating a system's short and long name.

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

Table 12-11 System Settings

System Settings	Description
Reboot Device	Reboots the device.
Restore Factory Defaults	Restores the device to the original factory settings. All configuration will be lost. The PremierWave unit automatically reboots upon setting back to the defaults.
Upload New Firmware	FTP to the PremierWave device. Write the new firmware file to firmware.rom on the PremierWave unit. The device automatically reboots upon the installation of new firmware. See the section, *FTP Settings on page 52*.
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”>`

13: Management Interface Settings

Command Line Interface Settings

The Command Line Interface settings allow you to control how users connect to and interact with the command line of the PremierWave SE1000 embedded system on module. It is possible to configure access via the Telnet protocols, in addition to general CLI options.

Basic CLI Settings

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

Table 13-1 CLI Configuration Settings

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

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 SE1000 embedded system on module telnet over the Telnet protocol.

Table 13-2 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">`

XML Settings

The PremierWave SE1000 embedded system on module allows for the configuration of units using an XML configuration record (XCR). Export a current configuration for use on other PremierWave SE1000unit 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 SE1000 unit or another. The XML data can be dumped to the screen or exported to a file on the file system.

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

Table 13-3 XML Exporting Configuration

XML Export Configuration Settings	Description
Export to browser	Select this option to export the XCR data in the selected fields to the browser. Use the “xcr dump” command to export the data to the browser.
Export to local file	Select this option to export the XCR data to a file on the device. If you select this option, enter a file name for the XML configuration record. Use the “xcr export” command to export the data to a local file.
Export secrets	Select to export secret password and key information. Use only with a secure link, and save only in secure locations. ***Note:*** *Only use with extreme caution.*
Comments	Select this option to include descriptive comments in the XML.
Lines to Export	Select instances to be exported in the line, serial, tunnel and terminal groups.
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 13-4 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 Filesystem

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

Line(s) from single line Settings on the Filesystem

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

Table 13-5 Import Configuration from Filesystem Settings

Import Configuration from Filesystem Settings	Description
Filename	Enter the name of the file on the PremierWave unit (local to its filesystem) that contains XCR data.
Lines to Import	Select filter instances to be imported in the line, serial, tunnel and terminal groups. This affects both Whole Groups to Import and Text List selections.
Whole 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.

14: Branding the PremierWave SE1000 Device

This chapter describes how to brand your PremierWave SE1000 embedded system on module by using Web Manager and Command Line Interface (CLI). It contains the following sections on 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 SE1000 unit file system.

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

1. FTP to the PremierWave SE1000 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://<PremierWaveSE1000 hostname>/config/index.html` and `http://<PremierWaveSE1000 hostname>/config/style.css`.
5. Modify the file as required or create a new one with the same name.
6. To customize the product logo, save the image of your choice as `logo.gif`
7. Put the file(s) by using `put <filename>`.
8. Type `quit`. The overriding files appear in the file system's http/config directory.
9. Restart any open browser to view the changes.
10. If you wish to go back to the default files in the firmware image, simply delete the overriding files from the file system.

Short and Long Name Customization

You can customize the short and long names in your PremierWave SE1000 embedded system on modulPremierWave SE1000 embedded system on module. The names display in the CLI show command and in the System web page in the Current Configuration table. The short name is used for the show command. Both names display in the CLI Product Type field.

Table 14-1 Short and Long Name Settings

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

To Customize Short or Long Names

Using Web Manager

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

Using the CLI

- To enter the command level: `enable`

Using XML

- Include in your file:

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

  and

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

Appendix A: Compliance

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

Manufacturer's Name & Address:

Lantronix, Inc.
167 Technology Drive, Irvine, CA 92618 USA

Product Name Model:

PremierWave® SE1000 Embedded System on Module

Conforms to the following standards or other normative documents:

- FCC Part 15 Class B
- RSS-210
- RSS-Gen Issue 2
- ICES-003 Issue 4
- IPv6 Ready Certified
  - EN55022
  - EN61000-4-2
  - EN61000-4-3
  - EN61000-4-4
  - EN61000-4-5
  - EN61000-4-6
  - EN61000-4-11
  - IEC 60950-1:2006 +A11:2009

Manufacturer's Contact:

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

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)
DSC	0	0	0	0	0	0
EDS	0	0	0	0	0	0
IntelliBox	0	0	0	0	0	0
MatchPort	0	0	0	0	0	0
Micro	0	0	0	0	0	0
MSS100	0	0	0	0	0	0
PremierWave	0	0	0	0	0	0
SCS	0	0	0	0	0	0
SecureBox	0	0	0	0	0	0
SLB	0	0	0	0	0	0
SLC	0	0	0	0	0	0
SLP	0	0	0	0	0	0
Spider and Spider Duo	0	0	0	0	0	0
UBox	0	0	0	0	0	0
UDS1100 and 2100	0	0	0	0	0	0
WiBox	0	0	0	0	0	0
WiPort	0	0	0	0	0	0
xDirect	0	0	0	0	0	0
xPico	0	0	0	0	0	0
xPico Wi-Fi	0	0	0	0	0	0
XPort	0	0	0	0	0	0
XPort Pro	0	0	0	0	0	0
xPress DR & xPress-DR+	0	0	0	0	0	0
xPrintServer	0	0	0	0	0	0
xSenso	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 B: Lantronix Technical Support

Lantronix offers many resources to support our customers and products at http://www.lantronix.com/support. For instance, ask a question, find firmware downloads, access the FTP site and search through tutorials, FAQs, bulletins, warranty information, extended support services, and product documentation.

To contact technical support or sales, look up your local office at http://www.lantronix.com/about/contact.html. When you report a problem, please provide the following information:

- Your name, company name, address, and phone number
- Lantronix product and model number
- Lantronix MAC address or serial number
- Firmware version and current configuration
- Description of the problem
- Status of the unit when the problem occurred (please try to include information on user and network activity at the time of the problem).

Appendix C: 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.

Scientific Calculator

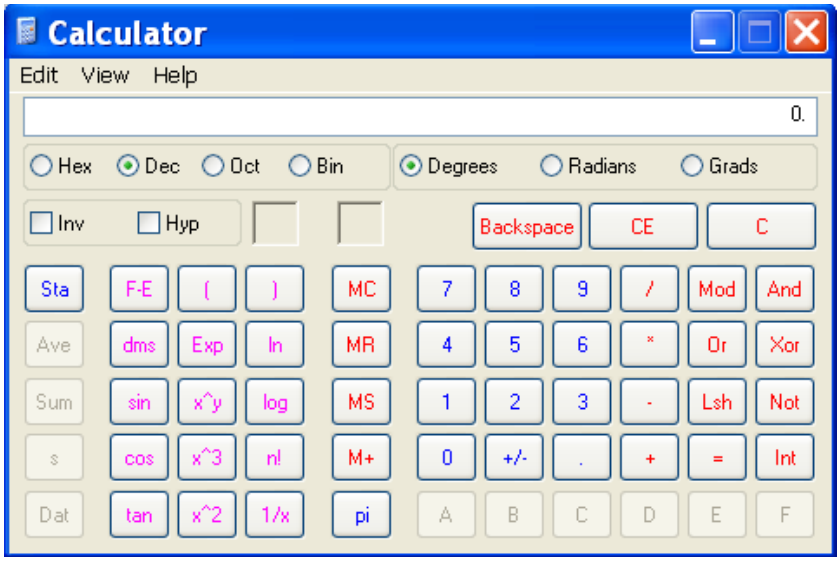
Another simple way to convert binary to hexadecimal is to use a scientific calculator, such as the one available on the Windows operating systems. For example:

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

Table C-1 Binary to Hexadecimal Conversion

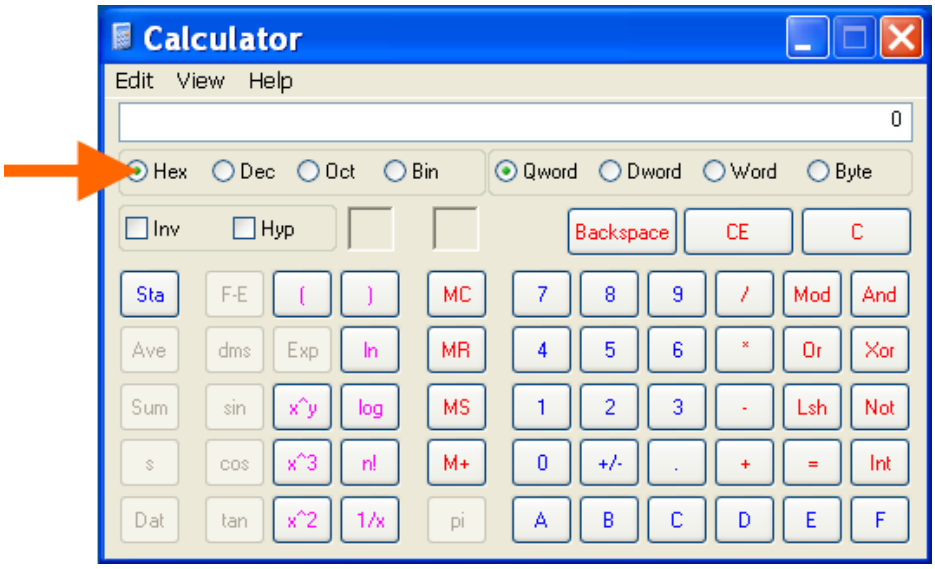
Decimal	Binary	Hex
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Figure C-2 Windows Scientific Calculator



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

Figure C-3 Hexadecimal Values in the Scientific Calculator



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 USB device port of the PremierWave SE1000 embedded system on module.

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 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"
```