PremierWave® XC HSPA+
Intelligent Gateway User Guide
Intellectual Property

© 2017 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

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

Patented: patents.lantronix.com; additional patents pending

Windows and Internet Explorer are registered trademarks of Microsoft Corporation. Mozilla and Firefox are registered trademarks of the Mozilla Foundation. Chrome is a trademark of Google Inc. Safari is a registered trademark of Apple Inc. Wi-Fi is a trademark of Wi-Fi Alliance Corporation. 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.
7535 Irvine Center Drive
Suite 100
Irvine, CA 92618, USA

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

Technical Support

Online: www.lantronix.com/support

Sales Offices

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

Disclaimer

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Rev.</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2016</td>
<td>F</td>
<td>Updated document to firmware release 8.0.0.0R19. Changes include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added Modbus, IPv6, and Initial Send content.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updated Flash and SNMP information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Removed Query Port content.</td>
</tr>
<tr>
<td>May 2013</td>
<td>A</td>
<td>Initial document for firmware release 7.7.0.0R27.</td>
</tr>
<tr>
<td>April 2014</td>
<td>B</td>
<td>Updated document to firmware release 7.8.0.0.</td>
</tr>
<tr>
<td>August 2014</td>
<td>C</td>
<td>Updated document to firmware release 7.9.0.0.</td>
</tr>
<tr>
<td>February 2017</td>
<td>D</td>
<td>Updated document to firmware release 8.0.0.0. Changes include adding IPv6, TCP Keep Alive, IKEv2, log verbosity, cellular modem IO, and cellular network traffic information.</td>
</tr>
</tbody>
</table>
## Table of Contents

Intellectual Property ................................................. 2  
Warranty .......................................................... 2  
Contacts .......................................................... 2  
Disclaimer .......................................................... 2  
Revision History ...................................................... 3  
List of Figures ....................................................... 11  
List of Tables ....................................................... 12  

1: Using This Guide ....................................................... 15  
Purpose and Audience ............................................... 15  
Summary of Chapters ............................................... 15  
Additional Documentation ......................................... 16  

2: Introduction .......................................................... 17  
Key Features ......................................................... 17  
Applications ......................................................... 18  
Protocol Support .................................................... 18  
Troubleshooting Capabilities ........................................ 19  
Configuration Methods ............................................... 19  
Addresses and Port Numbers ......................................... 19  
  Hardware Address ................................................ 19  
  IP Address ....................................................... 20  
  Port Numbers .................................................... 20  
  Product Information Label ........................................ 20  

3: Installation of the PremierWave XC HSPA+ Device .............. 21  
Package Contents .................................................. 21  
User-Supplied Items ................................................ 21  
Hardware Components ............................................. 22  
  Front/Top Panel ............................................... 22  
  Back Panel ..................................................... 26  
Installing the PremierWave XC HSPA+ Unit Device ............... 26  

4: Device Discovery and Quick Setup .................................. 29  
Accessing the PremierWave XC HSPA+ Device Using UPnP .......... 29  
Accessing the PremierWave XC HSPA+ Device Using DeviceInstaller .......... 30  
Device Detail Summary ............................................. 30
## 5: Configuration Using Web Manager

- Accessing Web Manager
- Device Status Page
- Web Manager Components
- Navigating Web Manager

## 6: Network Settings

- Network 1 Status
- Network 1 (eth0) Interface Settings
  - To Configure Network 1 Interface Settings
- Network 1 (eth0) Link Settings
  - To Configure Network 1 Link Settings
- Network 1 (eth0) QoS
  - To Configure Network 1 QoS Settings
- Network 1 (eth0) Failover
  - To Configure Network 1 Failover Settings
- Network 2 Status
- Network 2 (Cellular “wwan0”) Interface Settings
  - To Configure Network 2 Interface Settings
- Network 2 (Cellular “wwan0”) Link Settings
  - To Configure Network 2 Link Settings
- Network 2 (Cellular “wwan0”) QoS
  - To Configure Network 2 QoS Settings
- Gateway Status
- WAN
- WAN MAC Address Filters
  - To Configure Gateway WAN Settings
- Port Forwarding
  - To Configure Gateway Port Forwarding Settings
- Static Routes
  - To Configure Gateway Static Route Settings
- DHCP Server
  - To Configure Gateway DHCP Server Settings
- Static Lease Listing
- Routing Protocols
  - To Configure Gateway Routing Protocol Settings
- Virtual IP
  - To Configure Gateway Virtual IP
- DDNS
  - To Configure Gateway WAN Settings
- VPN
To Configure VPN Settings
GRE Settings
To Configure Tunnel Serial Settings

7: Cellular
To Configure Cellular Settings
Typical Cellular Error (errcodes)

8: Input/Output Ports
Relay Output
To Configure Relay Settings
Digital Input
To Configure Digital Input Settings

9: Action Settings
Alarms and Reports
Actions
To Configure Action Settings
Python
IDE
Applications
To Configure Application Settings

10: Line and Tunnel Settings
Line Statistics
Line Settings
To Configure Line Settings
To Configure Line Command Mode
Tunnel Statistics
To View Tunnel Statistics
Tunnel Settings
Serial Settings
To Configure Tunnel Serial Settings
Packing Mode
To Configure Tunnel Packing Mode Settings
Accept Mode
To Configure Tunnel Accept Mode Settings
Connect Mode
Connecting Multiple Hosts
Host List Promotion
Disconnect Mode
To Configure Tunnel Disconnect Mode Settings
11: Terminal and Host Settings

Terminal Settings
To Configure the Terminal Network Connection
To Configure the Terminal Line Connection
Host Configuration
To Configure Host Settings

12: Network Services

DNS Settings
To View or Configure DNS Settings:
FTP Settings
To Configure FTP Settings
Syslog Settings
To View or Configure Syslog Settings
HTTP Settings
To Configure HTTP Settings
To Configure HTTP Authentication
RSS Settings
To Configure RSS Settings
SNMP Settings
To Configure SNMP Settings
Discovery
To Configure Discovery
SMTP Settings
To Configure SMTP Settings
Email Settings
To View, Configure, and Send Email

13: SMS Settings

Inbound SMS
Outbound SMS
To Configure Inbound SMS
To Configure Outbound SMS

14: Updating Firmware

Obtaining Firmware
Loading New Firmware through Web Manager
Loading New Firmware through FTP
15: Security Settings

Public Key Infrastructure .................................................................................................................. 99
TLS (SSL) ........................................................................................................................................ 99
Digital Certificates ............................................................................................................................ 100
Trusted Authorities ............................................................................................................................. 100
Obtaining Certificates ......................................................................................................................... 100
Self-Signed Certificates ..................................................................................................................... 100
Certificate Formats ............................................................................................................................ 100
OpenSSL ............................................................................................................................................ 101

SSH Settings ..................................................................................................................................... 101
  SSH Server Host Keys ....................................................................................................................... 101
  SSH Client Known Hosts ..................................................................................................................... 102
  SSH Server Authorized Users ........................................................................................................... 102
  SSH Client Users ............................................................................................................................... 103
  To Configure SSH Settings .............................................................................................................. 104

SSL Settings ..................................................................................................................................... 105
  Create a New Credential .................................................................................................................... 105
  To Create a New Credential .............................................................................................................. 105
  Upload Certificate ............................................................................................................................. 106
  Certificate and Key Generation ......................................................................................................... 106
  To Configure an Existing SSL Credential ....................................................................................... 107
  Trusted Authorities ............................................................................................................................ 108

16: Maintenance and Diagnostics Settings

Filesystem Settings ............................................................................................................................. 109
  Statistics .......................................................................................................................................... 109
  To View Statistics .............................................................................................................................. 109
  File Display ..................................................................................................................................... 109
  To Display Files ................................................................................................................................. 110
  File Modification ............................................................................................................................... 110
  File Transfer .................................................................................................................................... 110
  To Transfer or Modify Filesystem Files ............................................................................................ 111

Protocol Stack Settings ...................................................................................................................... 111
  IP Settings ....................................................................................................................................... 111
  To Configure IP Protocol Stack Settings .......................................................................................... 112
  ICMP Settings .................................................................................................................................. 112
  To Configure ICMP Protocol Stack Settings .................................................................................... 112
  To View ICMP Protocol Stack Settings ............................................................................................ 112
  ARP Settings ..................................................................................................................................... 113
  To Configure ARP Network Stack Settings ...................................................................................... 113

Diagnostics ......................................................................................................................................... 114
  Hardware .......................................................................................................................................... 114
To View Hardware Information ................................................................. 114
IP Sockets ................................................................................................. 114
To View the List of IP Sockets ................................................................. 114
Ping ......................................................................................................... 114
To Ping a Remote Host .......................................................................... 115
Traceroute ............................................................................................... 115
To Perform a Traceroute ........................................................................ 115
Log .......................................................................................................... 116
To Configure the Diagnostic Log Output .............................................. 116
Memory .................................................................................................. 116
To View Memory Usage ........................................................................ 116
Processes ............................................................................................... 117
To View Process Information .............................................................. 117
Threads .................................................................................................. 117
To View Thread Information ............................................................... 117
Clock ...................................................................................................... 118
To Specify Clock Setting Method ......................................................... 118
System Settings .................................................................................... 119
To Reboot or Restore Factory Defaults .............................................. 119

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

18: Branding the PremierWave XC HSPA+ Device ......................... 126
Web Manager Customization ............................................................ 126
Short and Long Name Customization ................................................. 127
To Customize Short or Long Names .................................................... 127
List of Figures

Figure 2-1 PremierWave Unit Product Label ......................................................... 20
Figure 3-1 PremierWave XC HSPA+ Unit ............................................................... 22
Figure 3-5 PremierWave XC HSPA+ Male DB9 DTE Serial Ports ......................... 24
Figure 3-6 PremierWave XC HSPA+ Pinout Configuration for RS-232 .................. 24
Figure 3-7 PremierWave XC HSPA+ Pinout Configuration for Full Duplex RS-422/485 (4-wire) ... 25
Figure 3-8 PremierWave XC HSPA+ Pinout Configuration for Half Duplex RS-422/485 (2-wire) ... 25
Figure 3-11 PremierWave XC HSPA+ Bottom/Back Panel View ......................... 26
Figure 3-13 SIM Card Insertion ............................................................................. 27
Figure 3-14 PremierWave XC HSPA+ Unit Dimensions in Inches (in) ................. 28
Figure 5-1 Device Status Page ............................................................................. 33
Figure 5-2 Components of the Web Manager Page ............................................. 34
Figure 14-1 Uploading New Firmware ................................................................... 97
Figure D-2 Windows Scientific Calculator ......................................................... 137
Figure D-3 Hexadecimal Values in the Scientific Calculator ............................. 137
List of Tables

Table 3-2 PremierWave XC HSPA+ LEDs and Descriptions ........................................... 22
Table 3-3 Fault Conditions Indicated by Blink Patterns .................................................. 23
Table 3-4 Cellular Signal Strength Indicator .................................................................... 23
Table 3-9 Left Ethernet LED ............................................................................................. 25
Table 3-10 Right Ethernet LED ........................................................................................ 25
Table 3-12 PremierWave XC HSPA+ Connections (Side) .................................................. 26
Table 5-3 Web Manager Pages ......................................................................................... 35
Table 6-1 Network Interface Settings .............................................................................. 38
Table 6-2 Network 1 (eth0) Link Settings ........................................................................ 41
Table 6-3 Network 1 (eth0) QoS Settings ........................................................................ 42
Table 6-4 Adding or Deleting Network 1 (eth0) QoS Settings ......................................... 42
Table 6-5 Network 1 (eth0) Failover Settings ................................................................ 43
Table 6-6 Network 2 (wwan0) Interface Settings ............................................................. 44
Table 6-7 Network 2 (wlan0) Link Settings .................................................................... 45
Table 6-8 Network 2 (wwan0) QoS Settings .................................................................... 46
Table 6-9 Adding or Deleting Network 2 (wwan0) QoS Settings ....................................... 46
Table 6-10 WAN Configuration ....................................................................................... 47
Table 6-11 Adding a New MAC Address Filters .............................................................. 48
Table 6-12 Port Forwarding Rules List ............................................................................. 49
Table 6-13 Adding a New Port Forwarding Rule ............................................................... 49
Table 6-14 Static Route Setting Routes .......................................................................... 49
Table 6-15 Adding a New Static Route ............................................................................ 50
Table 6-16 DHCP Settings ............................................................................................... 50
Table 6-17 Static Lease Listing ....................................................................................... 51
Table 6-18 Add a Static Lease ......................................................................................... 51
Table 6-19 Routing Protocol Settings ............................................................................. 52
Table 6-20 Virtual IP Settings ......................................................................................... 52
Table 6-21 Adding a Virtual IP ....................................................................................... 53
Table 6-22 DDNS Configuration ..................................................................................... 53
Table 6-23 VPN Configuration ....................................................................................... 54
Table 6-24 GRE Settings ................................................................................................. 56
Table 8-1 Relay Output Settings ..................................................................................... 60
Table 8-2 Digital Input Settings ...................................................................................... 61
Table 9-1 Action Settings ............................................................................................... 62
Table 9-2 Script Settings ................................................................................................. 65
1: Using This Guide

Purpose and Audience

This guide provides the information needed to configure, use, and update the Lantronix® PremierWave® XC HSPA+ intelligent gateway. It is intended for software developers and system integrators who are installing this product into their designs.

Summary of Chapters

The remaining chapters in this guide include:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2: Introduction</td>
<td>Main features of the product and the protocols it supports. Includes technical specifications.</td>
</tr>
<tr>
<td>3: Installation of the PremierWave XC HSPA+ Device</td>
<td>Instructions for installing the PremierWave XC HSPA+ device.</td>
</tr>
<tr>
<td>4: Device Discovery and Quick Setup</td>
<td>Instructions for viewing the device and configuration using UPnP and the DeviceInstaller™ utility.</td>
</tr>
<tr>
<td>5: Configuration Using Web Manager</td>
<td>Instructions for accessing Web Manager and using it to configure settings for the device.</td>
</tr>
<tr>
<td>6: Network Settings</td>
<td>Instructions for configuring network settings.</td>
</tr>
<tr>
<td>7: Cellular</td>
<td>Instructions for configuring cellular settings.</td>
</tr>
<tr>
<td>8: Input/Output Ports</td>
<td>Instructions for configuring relay output and digital input settings.</td>
</tr>
<tr>
<td>9: Action Settings</td>
<td>Instructions for configuring alarm settings.</td>
</tr>
<tr>
<td>10: Line and Tunnel Settings</td>
<td>Instructions for configuring line and tunnel settings.</td>
</tr>
<tr>
<td>11: Terminal and Host Settings</td>
<td>Instructions for configuring terminal and host settings.</td>
</tr>
<tr>
<td>12: Network Services</td>
<td>Instructions for configuring DNS, FTP, HTTP and Syslog settings.</td>
</tr>
<tr>
<td>13: SMS Settings</td>
<td>Instructions for configuring SMS Settings.</td>
</tr>
<tr>
<td>14: Updating Firmware</td>
<td>Instructions for obtaining and updating the latest firmware for the device.</td>
</tr>
<tr>
<td>15: Security Settings</td>
<td>Instructions for configuring SSL security settings.</td>
</tr>
<tr>
<td>16: Maintenance and Diagnostics Settings</td>
<td>Instructions to view statistics, files, and diagnose problems.</td>
</tr>
<tr>
<td>17: Management Interface Settings</td>
<td>Instructions for configuring CLI and XML settings.</td>
</tr>
<tr>
<td>18: Branding the PremierWave XC HSPA+ Device</td>
<td>Instructions on how to brand your device.</td>
</tr>
</tbody>
</table>

Appendix A: Technical Specifications | Technical specifications for the device. |
Appendix B: Compliance | Lantronix compliance information. |
Appendix C: Lantronix Technical Support | Instructions for contacting Lantronix Technical Support. |
Appendix D: Binary to Hexadecimal Conversions | Instructions for converting binary values to hexadecimals. |
Additional Documentation

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

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PremierWave XC HSPA+ Intelligent Gateway Command Reference</td>
<td>Instructions for accessing Command Mode (the command line interface) using a Telnet connection, SSH connection or through the port. Detailed information about the commands. Also provides details for XML configuration and status.</td>
</tr>
<tr>
<td>PremierWave XC HSPA+ Intelligent Gateway Quick Start</td>
<td>Instructions for getting the PremierWave XC HSPA+ device up and running.</td>
</tr>
<tr>
<td>DeviceInstaller™ Utility Online Help</td>
<td>Instructions for using the Windows® operating system-based utility to locate the intelligent gateway and to view its current settings.</td>
</tr>
<tr>
<td>Com Port Redirector Quick Start and Online Help</td>
<td>Instructions for using the Windows operating system-based utility to create virtual com ports.</td>
</tr>
<tr>
<td>Secure Com Port Redirector User Guide</td>
<td>Instructions for using the Windows operating system-based utility to create secure virtual com ports.</td>
</tr>
</tbody>
</table>
2: Introduction

The PremierWave XC HSPA+ intelligent gateway is an industrial grade GSM/GPRS 3.5G cellular solution that enables customers to quickly connect their machines and assets for out-of-the-box Internet access, remote monitoring, control and cloud platform connectivity.

With highly configurable and easy to use software offering enterprise level security, the PremierWave XC HSPA+ intelligent gateway makes it possible to combine multiple application use cases in a compact, ruggedized platform.

Key Features

Communicate with Industrial Equipment and Machines Remotely and Securely
- Setup secure communication channels with serial and Ethernet based devices

Cellular Routing
- Ethernet to Cellular Routing
- NAT, Port Forwarding, Firewall

WAN Failover and Failback Support
- Support mission critical applications with a secondary path to the internet via cellular WAN

Device Server Application Suite
- Control and monitor serial port based devices over the IP network
- Supporting multiple virtual serial connections
- Multiple connection modes and configuration options to enable transparent tunneling of hundreds of serial protocols

Event Triggers and Actions
- Multiple configurable actions for pre-defined event triggers
- Simple PLC operations and system state change notifications
- Actions include sending email, posting to a Web Service, sending SMS, triggering relay output

Enterprise Class Management Features
- Powerful and flexible Web browser based UI
- CLI for advanced administration tasks
- XML for batch configuration and status

Advanced SMS Features
- SMS Control and Status Features
- SMS Actions on Event Triggers
- Number White-listing by application

Global Cellular Coverage
- Penta-band UMTS/HSPA+ (800/850/900/1900/2100 MHz)
- Quad Band GSM/GPRS/EDGE (850/900/1800/1900 MHz)
Industrial Grade

- **Temperature Range**: Operating temperature at -40°C to +70°C. Storage temperature at -40°C to +85°C

**Wide Voltage Range**: 9 - 30VDC input voltage through locking barrel connector

Flexible Connectivity Options

- **Serial Ports**: Two RS-232/422/485 ports with support from 300 to 921 kbps data rate
- **Ethernet port**: Auto-Sensing and Auto MDIX (cross-over) 10/100
- **Digital Inputs**: Two configurable inputs suitable for TTL input levels and tolerant up to 30VDC input voltage
- **Relay Output**: One independently isolated mechanical form-C relay
- **USB**: One USB host port

Applications

The PremierWave XC HSPA+ intelligent gateway is very suitable for these application scenarios:

**Remote Monitoring/Control**
- Data Display Services/Digital Signage
- Oil and Gas Exploration
- Smart Metering
- Street Lighting
- Gas Station Pump Control
- Irrigation Pump Control
- Industrial Controls and Instrumentation
- Fixed Telemetry
- Railway Maintenance
- Food and Beverage Temperature Control
- Security and Access Control Panels
- In-home Monitoring

**Out-of-Band Connectivity**
- Point-of-Sale/Kiosks
- Call Boxes

**Business Continuity Solutions**
- Primary WAN Link
- Secondary WAN Failover/Failback

Protocol Support

The PremierWave XC HSPA+ intelligent gateway contains a full-featured IP networking stack:

- ARP, HTTP, HTTPS, SMTP AUTH, SNMP v1/v2c/v3, UDP/IP, TCP/IP, SSH, SSL, TLS, RSS, UPnP, ICMP, BOOTP, DHCP, Auto IP, Telnet, SNTP, FTP, FTPS, DNS, TFTP, XML and Syslog for network communications and management
- FTP and HTTP/HTTPS web server for firmware upgrades and uploading/downloading files
- TCP/IP, UDP/IP, Telnet, SSH, SSL, TCP AES and UDP AES for command/response based data acquisition application or alarm triggered connection
- HTTP/HTTPS web based monitoring of input readings, chart and data logging
- SMTP AUTH, SMS, HTTP/HTTPS Post, FTP/FTPS Put and SNMP Traps for alarm-triggered notification
- SNTP and Cellular Network for device clock synchronization
Troubleshooting Capabilities

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

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

Configuration Methods

After installation, the PremierWave XC HSPA+ 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 XC HSPA+ intelligent gateway 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 32.)
- **DeviceInstaller**: Configure the IP address and related settings and view current settings on the PremierWave XC HSPA+ intelligent gateway using a Graphical User Interface (GUI) on a PC attached to a network. You will need the latest version of the Lantronix® DeviceInstaller™ utility. (See Accessing the PremierWave XC HSPA+ Device Using DeviceInstaller on page 30.)
- **Command Mode**: There are a few methods for accessing Command Mode (CLI): making a Telnet connection, or connecting a PC or other host running a terminal emulation program to the unit’s serial port. (See the PremierWave XC HSPA+ Intelligent Gateway Command Reference for instructions and available commands.)
- **XML**: The PremierWave XC HSPA+ intelligent gateway 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 XC HSPA+ Intelligent Gateway Command Reference for instructions and commands).

Addresses and Port Numbers

**Hardware Address**

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

- 00-80-A3-14-1B-18
- 00:80:A3:14:1B:18
**IP Address**

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

**Port Numbers**

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

The following is a list of the default server port numbers running on the PremierWave XC HSPA+ intelligent gateway:

- TCP Port 22: SSH Server (Command Mode configuration)
- TCP Port 23: Telnet Server (Command Mode configuration)
- TCP Port 80: HTTP (Web Manager Configuration)
- TCP Port 21: FTP
- UDP Port 30718: LDP (Lantronix Discovery Protocol) port
- TCP/UDP Port 10001: Tunnel 1 (see note below)
- 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
- International Mobile Equipment Identity (IMEI) Number
- Serial Number (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.
3: Installation of the PremierWave XC HSPA+ Device

This chapter describes how to install the PremierWave XC HSPA+ intelligent gateway. It contains the following sections:

- Package Contents
- User-Supplied Items
- Hardware Components
- Installing the PremierWave XC HSPA+ Unit Device

Package Contents

The PremierWave XC HSPA+ package includes the following items:

- PremierWave XC HSPA+ intelligent gateway
- RJ-45 Ethernet Straight CAT5 cable
- Two External antennas with an SMA connector
- One Power Supply 12 VDC with international adapters (PXC2102H2-01-S) or One DC Power Cable (PXC2101H2-01-02-S)
- Mounting components (DIN rail mounting adapter, cover plates, and rubber feet)
- PremierWave XC HSPA+ Quick Start Guide

User-Supplied Items

To complete your installation, you need the following items:

- RS-232/422/485 serial devices that require network connectivity
- Devices and sensors that require network connectivity.
  - A serial cable, as listed below, for each serial device. One end of the cable must have a female DB9 connector for the serial port.
  - A null modem cable to connect the serial port to another DTE device.
  - A straight-through modem cable to connect the serial port to a DCE device.
- An available connection to your Ethernet network and an Ethernet cable.
- A working AC power outlet if the unit will be powered from an AC outlet using the included 12 VDC power supply
- If the unit uses the DC power cable (PXC2102H2-01-02-S) then a DC power supply with terminal blocks or screw terminals
- A network SIM card (and data services) from a service provider
Hardware Components

Front/Top Panel

*Figure 3-1* shows the top panel view of the PremierWave unit. *Table 3-2*, *Table 3-3*, and *Table 3-4* list and explain the behavior of the LEDs on the top panel.

**LED Indicators:** 1 Power LED, 2 Serial Activity LEDs, 1 USB LED, 1 Cellular Status LED, 5 Signal Strength LEDs (two of which are dual-colored), 1 Diagnostic LED, and 2 Ethernet LEDs (on the RJ45 port).

*Figure 3-1 PremierWave XC HSPA+ Unit*

![Figure 3-1 PremierWave XC HSPA+ Unit](image)

*Table 3-2 PremierWave XC HSPA+ LEDs and Descriptions*

<table>
<thead>
<tr>
<th>LED</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>GREEN - displays a solid light when power is properly supplied</td>
</tr>
<tr>
<td></td>
<td>OFF - no power supplied</td>
</tr>
<tr>
<td>Cellular (Cell) Status</td>
<td>GREEN - displays solid when there is a connection to the packet domain on the cellular network (e.g., a data or GPRS/UMTS/HSPA connection)</td>
</tr>
<tr>
<td></td>
<td>AMBER - displays solid when there is a connection to the cellular network (e.g., a GSM connection)</td>
</tr>
<tr>
<td></td>
<td>OFF - indicates WWAN (cellular) interface is inactive or disabled</td>
</tr>
<tr>
<td>Serial 1</td>
<td>GREEN - flashes when Serial port 2 is transmitting data</td>
</tr>
<tr>
<td></td>
<td>AMBER - flashes when Serial port 2 is receiving data</td>
</tr>
<tr>
<td></td>
<td>OFF - when no data is being transmitted or received through Serial port 2</td>
</tr>
<tr>
<td>Serial 2</td>
<td>GREEN - flashes when Serial port 2 is transmitting data</td>
</tr>
<tr>
<td></td>
<td>AMBER - flashes when Serial port 2 is receiving data</td>
</tr>
<tr>
<td></td>
<td>OFF - when no data is being transmitted or received through Serial port 2</td>
</tr>
<tr>
<td>USB</td>
<td>GREEN - displays a solid light when a USB device is connected to and is functioning properly</td>
</tr>
<tr>
<td></td>
<td>OFF - when no USB device is connected</td>
</tr>
<tr>
<td>Signal Strength</td>
<td>Indicates cellular signal strength when connection is established (see Table 3-2)</td>
</tr>
</tbody>
</table>
Table 3-3 Fault Conditions Indicated by Blink Patterns

Note: The fault LED blink patterns in this table are listed in order of priority.

<table>
<thead>
<tr>
<th>Fault Conditions</th>
<th>Blink Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Ethernet link when eth0 (Ethernet Network) is enabled.</td>
<td>Long, long, short, short, 2 seconds off (pattern repeats)</td>
</tr>
<tr>
<td>No IP obtained from Ethernet network when eth0 interface is enabled.</td>
<td>Long, long, short, short, 2 seconds off (pattern repeats)</td>
</tr>
<tr>
<td>No cellular link (no SIM detected)</td>
<td>Long (pattern repeats)</td>
</tr>
<tr>
<td>No IP obtained from cellular network when wwan0 (Cellular Network) is enabled.</td>
<td>Long, long, long, long, short, 2 seconds off (pattern repeats)</td>
</tr>
<tr>
<td>No cellular link when wwan0 (Cellular Network) is enabled.</td>
<td>Long, long, long, long, short, 2 seconds off (pattern repeats)</td>
</tr>
<tr>
<td>When the internal device temperature is above operating limit.</td>
<td>Long, short, short, short, 2 seconds off (pattern repeats)</td>
</tr>
<tr>
<td>When the internal device temperature is below operating limit.</td>
<td>Short, short, short, short, 2 seconds off (pattern repeats)</td>
</tr>
<tr>
<td>Primary power source (barrel connector) is under-volt (below 9 volts).</td>
<td>Long, short (pattern repeats)</td>
</tr>
<tr>
<td>Secondary power source (terminal) is under-volt (below 9 volts).</td>
<td>Long, short, short, short (pattern repeats)</td>
</tr>
</tbody>
</table>

Table 3-4 Cellular Signal Strength Indicator

<table>
<thead>
<tr>
<th>Signal Strength</th>
<th>Color &amp; Number of LED Signal Bars</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greater than or equal to -64 dBm</td>
<td>5 Green</td>
</tr>
<tr>
<td>Greater than or equal to -85 dBm and less than -64 dBm</td>
<td>4 Green</td>
</tr>
<tr>
<td>Greater than or equal to -75 dBm and less than -85 dBm</td>
<td>3 Green</td>
</tr>
<tr>
<td>Greater than or equal to -86 dBm and less than -75 dBm</td>
<td>2 Amber</td>
</tr>
<tr>
<td>Greater than or equal to -112 dBm and less than -86 dBm</td>
<td>1 Amber</td>
</tr>
<tr>
<td>Less than -113 dBm or unmeasurable</td>
<td>All Off</td>
</tr>
</tbody>
</table>

Notes:

- For Table 3-3 above, a “long” blink is 0.7 seconds of light followed by 0.3 seconds of no light. A “short” blink is a light that is on for only 0.2 seconds and followed by 0.2 seconds of no light.
- The diagnostic blink patterns reflect the highest priority fault condition. Also, the Diagnostic LED will give an initial, identifying blink pattern to indicate the type of diagnostic information it will display. All power and other non-network related diagnostic patterns, with the exception of Temperature events and No SIM Card events, begin with one long blink. All wired LAN related diagnostics patterns begin with two long blinks. All cellular-related diagnostics patterns begin with four long blinks.
The PremierWave device has two male DB9 serial ports that support RS-232/422/485. Figure 3-5 shows the front view of the device. The default serial port settings are 9600 baud, 8 bits, no parity, 1 stop bit, no flow control.

**Figure 3-5 PremierWave XC HSPA+ Male DB9 DTE Serial Ports**

![Diagram of the PremierWave XC HSPA+ Male DB9 DTE Serial Ports](image)

**Figure 3-6 PremierWave XC HSPA+ Pinout Configuration for RS-232**

![Diagram of the PremierWave XC HSPA+ Pinout Configuration for RS-232](image)
Figure 3-7 PremierWave XC HSPA+ Pinout Configuration for Full Duplex RS-422/485 (4-wire)

Figure 3-8 PremierWave XC HSPA+ Pinout Configuration for Half Duplex RS-422/485 (2-wire)

Ethernet LEDs

The Ethernet port (see Figure 3-11) has two LEDs that indicate the status of the connection as described in the Table 3-9 and Table 3-10 below:

<table>
<thead>
<tr>
<th>Color/Status</th>
<th>Solid Light</th>
<th>Blinking Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>100 Mbps Link</td>
<td>100 Mbps Activity</td>
</tr>
<tr>
<td>Amber</td>
<td>10 Mbps Link</td>
<td>10 Mbps Activity</td>
</tr>
</tbody>
</table>

Table 3-9 Left Ethernet LED

<table>
<thead>
<tr>
<th>Color/Status</th>
<th>Solid Light</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Full Duplex</td>
</tr>
<tr>
<td>OFF</td>
<td>Half Duplex</td>
</tr>
</tbody>
</table>

Table 3-10 Right Ethernet LED

The Ethernet port can connect to an Ethernet (10 Mbps) or Fast Ethernet (100 Mbps) network.

Reset Button

You can reset the PremierWave XC HSPA+ intelligent gateway to factory defaults, including clearing the network settings. The IP address, gateway, and netmask are set to 00s. To reset the unit to factory defaults, perform the following steps.

1. Place the end of a paper clip or similar object into the reset opening (see Figure 3-5) and press and hold down micro switch during a power cycle for 10-15 seconds.
2. Remove the paper clip to release the button. The unit will continue the boot process restoring it back to the original factory default settings.

**Back Panel**

On the PremierWave device is a Power Connector and RJ-45 Ethernet port as shown in *Figure 3-11.*

![Figure 3-11 PremierWave XC HSPA+ Bottom/Back Panel View](image)

**Table 3-12 PremierWave XC HSPA+ Connections (Side)**

<table>
<thead>
<tr>
<th>Connector</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relay Output</td>
<td>Outputs Support 1A 24V</td>
</tr>
<tr>
<td>Inputs</td>
<td>Inputs accept voltage 0 to 30 VDC.</td>
</tr>
<tr>
<td></td>
<td><strong>ON</strong></td>
</tr>
<tr>
<td></td>
<td>Max 30 VDC</td>
</tr>
<tr>
<td></td>
<td>Min 2 VDC</td>
</tr>
<tr>
<td></td>
<td><strong>OFF</strong></td>
</tr>
<tr>
<td></td>
<td>Max 0.7 VDC</td>
</tr>
<tr>
<td></td>
<td>Min 0 VDC</td>
</tr>
</tbody>
</table>

**Installing the PremierWave XC HSPA+ Unit Device**

Be sure to place or mount the device securely on a flat horizontal or vertical surface. The device comes with brackets for mounting it, for example, on a wall. If using AC power, do not use outlets controlled by a wall switch.

**Observe the following guidelines when connecting the devices:**

- The PremierWave unit serial ports support RS-232/422/485.
- Use a null modem cable to connect the serial port to another DTE device. Use a straight-through (modem) cable to connect the serial port to a DCE device.
- Connect your RJ-45 Ethernet cable to the RJ-45 port of the unit.
- The PremierWave device supports a power range of 9 to 30 VDC.
3: Installation of the PremierWave XC HSPA+ Device

**Note:** As soon as you plug the device into power, the device powers up automatically, the self-test begins, and LEDs would indicate the device’s status.

**Perform the following steps to install your device:**

1. With the power unplugged, insert your SIM card.
2. Connect an RJ-45 Ethernet cable between the unit and your Ethernet network.
3. Connect the antennas to the SMA connectors on the back. Do note that the safe distance due to RF exposure from antenna is 2 cm.

**Note:** Antennas must be installed prior to powering on the unit. Do not remove or connect the antennas while the unit power is on.

4. Plug the PremierWave XC device into the power outlet by using the power supply that was included in the packaging.

![Figure 3-13 SIM Card Insertion](image)
Figure 3-14 PremierWave XC HSPA+ Unit Dimensions in Inches (in)
4:  **Device Discovery and Quick Setup**

Software embedded within the PremierWave XC HSPA+ intelligent gateway 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 XC HSPA+ Device Using UPnP*
2.  *Accessing the PremierWave XC HSPA+ Device Using DeviceInstaller*

**Accessing the PremierWave XC HSPA+ Device Using UPnP**

This section covers the steps for locating a PremierWave XC HSPA+ unit and viewing its properties and device details using UPnP (Network Discovery). You may also use the DeviceInstaller utility to discover PremierWave XC HSPA+ units. See *Accessing the PremierWave XC HSPA+ Device Using DeviceInstaller on page 30.*

The PremierWave XC HSPA+ 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 XC HSPA+ 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 XC HSPA+ 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 XC HSPA+ 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 XC HSPA+ devices will be listed like other network devices.
2. Right click your device and select **Properties** to view the device properties.
Accessing the PremierWave XC HSPA+ Device Using DeviceInstaller

This section covers the steps for locating a PremierWave XC HSPA+ 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.
- You may also use UPnP to discover PremierWave XC HSPA+ units. See Accessing the PremierWave XC HSPA+ Device Using UPnP on page 29.
- 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.

<table>
<thead>
<tr>
<th>Current Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Shows the PremierWave XC HSPA+ device name.</td>
</tr>
<tr>
<td>DHCP Device Name</td>
<td>Displays one of the names the PremierWave XC HSPA+ unit will send to the DHCP server if it is configured to obtain an address in this manner.</td>
</tr>
<tr>
<td>Group</td>
<td>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.</td>
</tr>
</tbody>
</table>
### 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 device family type as “PremierWave”.
Short Name | Shows “premierwave_xc_hspa” by default.
Long Name | Shows “Lantronix PremierWave XC HSPA+” by default.
Type | Shows the device type as “PremierWave XC HSPA+”.
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.
IPV6 Link Local Address | Shows the current PremierWave IPv6 link local address.
IPV6 Global Address | Shows the current PremierWave IPv6 global address.
IP Address was Obtained | Appears “Dynamically” if the PremierWave device automatically received an IP address (e.g., from DHCP). Appears “Statically” if the IP address was configured manually.
- 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.
Interfaces | Shows information about the Ethernet (eth0) and wireless (wlan0) interfaces for your PremierWave unit. Click the + sign beside eth0 or wlan0, and then the Status and Configuration subcategories to view status and configuration information on these interfaces.
Number of Serial Ports | Shows the number of serial ports on unit.
Number of Relay Outputs | Shows the number of relay outputs on the intelligent gateway.
Supports Configurable Pins | Shows False, indicating configurable pins are not available on the PremierWave unit.
Supports Email Triggers | Shows True, indicating email triggers are available on the 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 upgradeable as newer versions become available.
5: Configuration Using Web Manager

This chapter describes how to configure the PremierWave XC HSPA+ intelligent gateway using Web Manager, the Lantronix browser-based configuration tool. The unit’s configuration is stored in non-volatile memory and is retained without power. All changes take effect immediately, unless otherwise noted. It contains the following sections:

◆ Accessing Web Manager
◆ Device Status Page
◆ Web Manager Components
◆ Navigating Web Manager

Accessing Web Manager

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

To access Web Manager, perform the following steps:

1. Open a standard web browser. Lantronix supports the latest versions of Internet Explorer, Mozilla Firefox, Safari or Chrome web browsers.

2. Enter the IP address or hostname of the PremierWave XC HSPA+ unit in the address bar. The IP address may have been assigned manually using DeviceInstaller (see the PremierWave XC HSPA+ Intelligent Gateway 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 Home page displays with a brief summary of current status, including product information and network settings.
Device Status Page

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

**Figure 5-1 Device Status Page**

<table>
<thead>
<tr>
<th>Status</th>
<th>Device Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td></td>
</tr>
<tr>
<td>Apps</td>
<td></td>
</tr>
<tr>
<td>Cellular</td>
<td></td>
</tr>
<tr>
<td>CLI</td>
<td></td>
</tr>
<tr>
<td>Clock</td>
<td></td>
</tr>
<tr>
<td>Diagnostics</td>
<td></td>
</tr>
<tr>
<td>Digital Input</td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td></td>
</tr>
<tr>
<td>Filesystem</td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td>GRE</td>
<td></td>
</tr>
<tr>
<td>Host</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td></td>
</tr>
<tr>
<td>Line</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td></td>
</tr>
<tr>
<td>Protocol Stack</td>
<td></td>
</tr>
<tr>
<td>Relay</td>
<td></td>
</tr>
<tr>
<td>RSS</td>
<td></td>
</tr>
<tr>
<td>SMS</td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td></td>
</tr>
<tr>
<td>SSL</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td></td>
</tr>
<tr>
<td>Terminal</td>
<td></td>
</tr>
<tr>
<td>Tunnel</td>
<td></td>
</tr>
<tr>
<td>VPN</td>
<td></td>
</tr>
<tr>
<td>XML</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Product Information</strong></td>
<td></td>
</tr>
<tr>
<td>Product Type:</td>
<td>PremierWave XC HSPA+ (premierwave_xc_hspa+)</td>
</tr>
<tr>
<td>Firmware Version:</td>
<td>8.0.0.9R13</td>
</tr>
<tr>
<td>Cellular Firmware Version:</td>
<td>03.001 [01.000.124]</td>
</tr>
<tr>
<td><strong>Build Date</strong>:</td>
<td>Jan 5 14:33:44 PST 2017</td>
</tr>
<tr>
<td><strong>Serial Number</strong>:</td>
<td>02BDA39A0170</td>
</tr>
<tr>
<td><strong>Uptime</strong>:</td>
<td>5 days 07:09:03</td>
</tr>
<tr>
<td><strong>Current Date/Time</strong>:</td>
<td>Sat Jan 06 07:09:06 UTC 2007</td>
</tr>
<tr>
<td><strong>Temperature</strong>:</td>
<td>32.0°C</td>
</tr>
<tr>
<td><strong>Permanent Config</strong>:</td>
<td>Saved</td>
</tr>
<tr>
<td><strong>Alerts</strong>:</td>
<td>Alarm (wwan0 link state change)</td>
</tr>
<tr>
<td><strong>Duration</strong>:</td>
<td>5 days 07:08:39</td>
</tr>
<tr>
<td><strong>Network Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Name servers</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Primary DNS</strong>:</td>
<td>172.19.1.1</td>
</tr>
<tr>
<td><strong>Secondary DNS</strong>:</td>
<td>172.19.1.2</td>
</tr>
<tr>
<td><strong>Interface eth0</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Link</strong>:</td>
<td>Auto 10/100 Mbps Auto Half/Full (100 Mbps Full)</td>
</tr>
<tr>
<td><strong>MAC Address</strong>:</td>
<td>00:80:A3:3A:01:70</td>
</tr>
<tr>
<td><strong>Hostname</strong>:</td>
<td>&lt;None&gt;</td>
</tr>
<tr>
<td><strong>MTU</strong>:</td>
<td>1500</td>
</tr>
<tr>
<td><strong>IP Address</strong>:</td>
<td>172.19.100.51/16 &lt;DHCP&gt;</td>
</tr>
<tr>
<td><strong>Network Mask</strong>:</td>
<td>255.255.0.0 &lt;DHCP&gt;</td>
</tr>
<tr>
<td><strong>Default Gateway</strong>:</td>
<td>172.19.0.1 &lt;DHCP&gt;</td>
</tr>
<tr>
<td><strong>Domain</strong>:</td>
<td>eng.lantronix.com &lt;DHCP&gt;</td>
</tr>
<tr>
<td><strong>IPv6 Link-local Address</strong>:</td>
<td>fe80::206:a3ff:fe9a:1705/64</td>
</tr>
<tr>
<td><strong>IPv6 Default Gateway</strong>:</td>
<td>fe80::6600:11ff:fe06:386e:fe80:20c:299fe80:64/64</td>
</tr>
<tr>
<td><strong>IPv6 Domain</strong>:</td>
<td>eng.lantronix.com &lt;DHCP&gt;</td>
</tr>
<tr>
<td><strong>Interface wwan0</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Packet Domain Status</strong>:</td>
<td>registered on foreign network (roaming)</td>
</tr>
<tr>
<td><strong>IP Address</strong>:</td>
<td>&lt;None&gt;</td>
</tr>
<tr>
<td><strong>Line Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Line 1</strong>:</td>
<td>R3232.5600. None, B. None</td>
</tr>
<tr>
<td><strong>Line 2</strong>:</td>
<td>R3232.5600. None, B. None</td>
</tr>
<tr>
<td><strong>Tunneling Connect Mode</strong>:</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Accept Mode</strong>:</td>
<td>Waiting</td>
</tr>
<tr>
<td><strong>Tunnel 1</strong>:</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Tunnel 2</strong>:</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>VPN</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Status</strong>:</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>IP Address</strong>:</td>
<td>&lt;None&gt;</td>
</tr>
</tbody>
</table>
Web Manager Components

The layout of a typical Web Manager page is below.

**Figure 5-2 Components of the Web Manager Page**

- **Header:** Information and Help Area
- **Menu Bar:** Links to subpages
- **Footer:** Logout button
- **Configuration and/or Status Area:** Items to configure

**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 XC HSPA+ 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 5-3 Web Manager Pages

<table>
<thead>
<tr>
<th>Web Manager Page</th>
<th>Description</th>
<th>See Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Shows product information, network, line, and tunneling settings.</td>
<td>33</td>
</tr>
<tr>
<td>Actions</td>
<td>Allows you to view and configure the actions for a specific alarm or report.</td>
<td>62</td>
</tr>
<tr>
<td>Applications</td>
<td>Allows you to view and configure Application settings.</td>
<td>65</td>
</tr>
<tr>
<td>Cellular</td>
<td>Shows cellular statistics and lets you change the current CLI configuration settings.</td>
<td>58</td>
</tr>
<tr>
<td>CLI</td>
<td>Shows Command Line Interface (CLI) statistics and lets you change the current CLI configuration settings.</td>
<td>120</td>
</tr>
<tr>
<td>Clock</td>
<td>Allows you to view and configure the current date, time and time zone as it displays in web manager.</td>
<td>118</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>Lets you perform various diagnostic procedures.</td>
<td>114</td>
</tr>
<tr>
<td>Digital Input</td>
<td>Allows you to view and configure digital input, shows current input status and allows you to scale and modify display of both digital inputs.</td>
<td>64</td>
</tr>
<tr>
<td>Web Manager Page (continued)</td>
<td>Description</td>
<td>See Page</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Discovery</td>
<td>Allows you to view and modify the configuration and statistics for device discovery.</td>
<td>91</td>
</tr>
<tr>
<td>DDNS</td>
<td>Allows you to view and configure DDNS settings.</td>
<td>53</td>
</tr>
<tr>
<td>DNS</td>
<td>Shows the current configuration of the DNS subsystem and the DNS cache.</td>
<td>85</td>
</tr>
<tr>
<td>Email</td>
<td>Shows email statistics and lets you clear the email log, configure email settings, and send an email.</td>
<td>92</td>
</tr>
<tr>
<td>Filesystem</td>
<td>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.</td>
<td>109</td>
</tr>
<tr>
<td>FTP</td>
<td>Shows statistics and lets you change the current configuration for the File Transfer Protocol (FTP) server.</td>
<td>86</td>
</tr>
<tr>
<td>Gateway</td>
<td>Shows statistics and lets you change the current configuration for the gateway.</td>
<td>47</td>
</tr>
<tr>
<td>GRE</td>
<td>Allows you to view and configure GRE settings.</td>
<td>56</td>
</tr>
<tr>
<td>Host</td>
<td>Lets you view and change settings for a host on the network.</td>
<td>83</td>
</tr>
<tr>
<td>HTTP</td>
<td>Shows HyperText Transfer Protocol (HTTP) statistics and lets you change the current configuration and authentication settings.</td>
<td>87</td>
</tr>
<tr>
<td>Line</td>
<td>Shows statistics and lets you change the current configuration and Command mode settings of a serial line.</td>
<td>67</td>
</tr>
<tr>
<td>Network</td>
<td>Shows status and lets you configure the network interface.</td>
<td>38</td>
</tr>
<tr>
<td>Protocol Stack</td>
<td>Lets you perform lower level network stack-specific activities.</td>
<td>111</td>
</tr>
<tr>
<td>Query Port</td>
<td>Lets you change configuration settings for the query port.</td>
<td>114</td>
</tr>
<tr>
<td>Relay</td>
<td>Allows you to view and configure relay output, shows current relay output statuses and allows you to modify display of both relays.</td>
<td>80</td>
</tr>
<tr>
<td>RSS</td>
<td>Lets you change current Really Simple Syndication (RSS) settings.</td>
<td>89</td>
</tr>
<tr>
<td>SMS</td>
<td>Shows and allows modification to the current configuration of SMS.</td>
<td>94</td>
</tr>
<tr>
<td>SMTP</td>
<td>Shows and allows modification of the current configuration of SMTP.</td>
<td>92</td>
</tr>
<tr>
<td>SNMP</td>
<td>Shows and allows modification of the current configuration of SNMP.</td>
<td>92</td>
</tr>
<tr>
<td>SSH</td>
<td>Lets you change the configuration settings for SSH server host keys, SSH server authorized users, SSH client known hosts, and SSH client users.</td>
<td>101</td>
</tr>
<tr>
<td>SSL</td>
<td>Lets you upload an existing certificate or create a new self-signed certificate.</td>
<td>105</td>
</tr>
<tr>
<td>Syslog</td>
<td>Lets you specify the severity of events to log and the server and ports to which the syslog should be sent.</td>
<td>86</td>
</tr>
<tr>
<td>System</td>
<td>Lets you reboot device, restore factory defaults, upload new firmware, and change the device long and short names.</td>
<td>119</td>
</tr>
<tr>
<td>Terminal</td>
<td>Lets you change current settings for a terminal.</td>
<td>82</td>
</tr>
<tr>
<td>Tunnel</td>
<td>Lets you change the current configuration settings for an incoming tunnel connection.</td>
<td>70</td>
</tr>
<tr>
<td>Virtual IP</td>
<td>Allows you to view and configure Virtual IP settings.</td>
<td>52</td>
</tr>
<tr>
<td>VPN</td>
<td>Lets you view and configure VPN settings.</td>
<td>54</td>
</tr>
<tr>
<td>Web Manager Page (continued)</td>
<td>Description</td>
<td>See Page</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>XML</td>
<td>Lets you export XML configuration and status records, and import XML configuration records.</td>
<td>122</td>
</tr>
</tbody>
</table>
6: **Network Settings**

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

The PremierWave XC HSPA+ contains one Ethernet and one Cellular interface. The Ethernet interface is called Network 1 or eth0, and the Cellular interface is also called Network 2 or wwan0.

**Notes:**

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

**Network 1 Status**

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

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

**Network 1 (eth0) Interface Settings**

*Table 6-1* shows the network interface settings that can be configured.

<table>
<thead>
<tr>
<th>Network Interface Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select to enable or disable the interface.</td>
</tr>
<tr>
<td>IPv4 State</td>
<td>Select to enable or disable the IPv4 state.</td>
</tr>
</tbody>
</table>
### Network Interface Settings (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| **BOOTP Client**         | Select to turn **On** or **Off**. At boot up, after the physical link is up, the PremierWave 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 XC HSPA+ 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. |
| **Priority**             | Priority ranges from 0-10.  
  **Note:** Lower priority number means higher preference. |
| **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 XC HSPA+ device tries to obtain an IPv4 address from a DHCP or BOOTP server. If it cannot, the PremierWave XC HSPA+ 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**). |
| **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 XC HSPA+ intelligent gateway MAC address. |
| **Primary DNS**          | Enter the IP address of the primary Domain Name Server.  
  **Note:** This setting will be used when either Static IP or Auto IP is active, or if DHCP/BOOTP is active and no DNS server was acquired from the server. |
| **Secondary DNS**        | Enter the IP address of the secondary Domain Name Server.  
  **Note:** This setting will be used when either Static IP or Auto IP is active, or if DHCP/BOOTP is active and no DNS server was acquired from the server. |
| **MTU**                  | When DHCP is enabled, the MTU size is (usually) provided with the IP address. When not provided by the DHCP server, or using a static configuration, this value is used. The MTU size can be from 576 to 1500 bytes. |
To Configure Network 1 Interface Settings

Using Web Manager

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

Using the CLI

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

Using XML

- Include in your file: `<configgroup name="interface" instance="eth0">`
Network 1 (eth0) Link Settings

Physical link parameters can be configured for an Ethernet (eth0) Network Link (see Table 6-2).

Table 6-2 Network 1 (eth0) Link Settings

<table>
<thead>
<tr>
<th>Network 1 Ethernet (eth0) Link Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>Select the Ethernet link speed. (Default is Auto)</td>
</tr>
<tr>
<td></td>
<td>- Auto = Auto-negotiation of Link Speed</td>
</tr>
<tr>
<td></td>
<td>- 10 Mbps = Force 10 Mbps</td>
</tr>
<tr>
<td></td>
<td>- 100 Mbps = Force 100 Mbps</td>
</tr>
<tr>
<td>Duplex</td>
<td>Select the Ethernet link duplex mode. (Default is Auto)</td>
</tr>
<tr>
<td></td>
<td>- Auto = Auto-negotiation of Link Duplex</td>
</tr>
<tr>
<td></td>
<td>- Half = Force Half Duplex</td>
</tr>
<tr>
<td></td>
<td>- Full = Force Full Duplex</td>
</tr>
</tbody>
</table>

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">`

Network 1 (eth0) QoS

QoS (Quality of Service) can be enabled and configured for both Network 1 (eth0) and Network 2 (wwan0). If enabled, the router will control the flow of outbound traffic according to the user-defined filters. In other words, QoS improves performance by allowing the user to prioritize applications. Filters can be defined to prioritize traffic based on the source or destination network, source or destination port, or the source MAC address. Up to 32 user-defined filters can be added. The following are predefined priority classes:
- Network Control and Internetwork Control are typically used for network control packets such as ICMP and have the highest priorities.
Move bandwidth allocation is a minimum 5% each to Network control.
Voice: Bandwidth allocation is minimum 30%.
Video: Bandwidth allocation is minimum 20%.
Critical Applications: Bandwidth allocation is minimum 15%.
Excellent Effort: Bandwidth allocation is minimum 10%.
Best Effort: Bandwidth allocation is minimum 10%.
Background: Bandwidth allocation is minimum 5% and has the lowest priority.

Table 6-3 shows the network QoS settings that can be configured including adding new filters.

### Table 6-3 Network 1 (eth0) QoS Settings

<table>
<thead>
<tr>
<th>Network 1 (eth0) Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Click to enable or disable state.</td>
</tr>
<tr>
<td>Import filters</td>
<td>Click to enable or disable import filters to import configurations from other interfaces.</td>
</tr>
<tr>
<td>Uplink Speed</td>
<td>Enter the maximum uplink speed. Set 0 to set speed to default.</td>
</tr>
<tr>
<td>Delete</td>
<td>Click the checkbox to the left of any existing QoS filter to be deleted and click the Submit button.</td>
</tr>
<tr>
<td>Filter type</td>
<td>Select the filter type from the drop-down window:</td>
</tr>
<tr>
<td></td>
<td>✦ Network</td>
</tr>
<tr>
<td></td>
<td>✦ Port</td>
</tr>
<tr>
<td>Network</td>
<td>Enter the Network, if the Network filter type is selected.</td>
</tr>
<tr>
<td>Ports</td>
<td>Enter the Port, if the Port filter type is selected.</td>
</tr>
<tr>
<td>Priority</td>
<td>Select the priority of the filter from the drop-down menu.</td>
</tr>
</tbody>
</table>

### Table 6-4 Adding or Deleting Network 1 (eth0) QoS Settings

<table>
<thead>
<tr>
<th>Adding or Deleting Network 1 (eth0) Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Click the checkbox to the left of any existing QoS filter to be deleted and click the Submit button.</td>
</tr>
<tr>
<td>Filter type</td>
<td>Select the filter type from the drop-down window:</td>
</tr>
<tr>
<td></td>
<td>✦ Network</td>
</tr>
<tr>
<td></td>
<td>✦ Port</td>
</tr>
<tr>
<td>Network</td>
<td>Enter the Network, if the Network filter type is selected.</td>
</tr>
<tr>
<td>Ports</td>
<td>Enter the Port, if the Port filter type is selected.</td>
</tr>
<tr>
<td>Priority</td>
<td>Select the priority of the filter from the drop-down menu.</td>
</tr>
<tr>
<td>Submit</td>
<td>Click Submit after adding information for a new filter.</td>
</tr>
</tbody>
</table>

### To Configure Network 1 QoS Settings

**Using Web Manager**

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

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

Using XML

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

Network 1 (eth0) Failover

The PremierWave XC HSPA+ intelligent gateway provides Cellular WAN network failover, in the form of a "dead remote host reachability" mechanism (essentially a ping against a known host). If the remote host is determined to be not reachable, the device will failover to the Wi-Ficellular interface. If the remote host is determined to be reachable, the device will failback to the Ethernet interface.

<table>
<thead>
<tr>
<th>Network 1 (Failover) Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Click to enable or disable state.</td>
</tr>
<tr>
<td>Failover Interface</td>
<td>Always select wwan0 in the PremierWave XC HSPA+ intelligent gateway.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Enter the remote host to test reachability.</td>
</tr>
<tr>
<td>Method</td>
<td>Select ICMP or TCP based ping.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Indicate the interval to wait for ping response from remote host.</td>
</tr>
<tr>
<td>Interval</td>
<td>Indicate the interval in which to test reachability</td>
</tr>
<tr>
<td>Failover Threshold</td>
<td>Indicate the allowed number of failed pings – after which the device will failover to the cellular interface.</td>
</tr>
<tr>
<td>Failback Threshold</td>
<td>Indicate the number of successful pings – after which the device will failback to the Ethernet interface.</td>
</tr>
</tbody>
</table>

To Configure Network 1 Failover Settings

Using Web Manager

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

Using the CLI

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

Using XML

- Include in your file: <configgroup name="network failover" instance="eth0">
Network 2 Status

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

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

Network 2 (Cellular “wwan0”) Interface Settings

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

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

This page is used to configure the wwan0 interface on the device. To see the effect of these items after a reboot, view the Status page.

**Table 6-6 Network 2 (wwan0) Interface Settings**

<table>
<thead>
<tr>
<th>Network 2 (wwan0) Interface Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select to enable or disable the interface.</td>
</tr>
</tbody>
</table>
| Priority                              | It ranges from 0-10.  
*Note:* Lower priority number means higher preference. |
| Connection Mode                       |  
- The **Always On** connection mode keeps the device always connected to the cellular network.  
- The **On Demand** connection mode leaves the link quiescent until an application attempts to make use of the cellular network connection. Be aware that in this mode, the first attempt to initiate a connection from the device server may fail, since a new IP address may need to be negotiated.  
- The **Shoulder Tap** connection mode requires a short message (SMS) to make the link active. See the SMS Inbound configuration for details on the message syntax requirements. |
| Idle Timeout                          | If the connection mode is 'On Demand' or 'Shoulder Tap' and there is no network activity for Idle Timeout duration the device will automatically disconnect from the cellular network. |
| 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. |
To Configure Network 2 Interface Settings

Using Web Manager

✦ To modify network 2 wwan0 interface information, click Network on the menu and select Network 2 > Interface > Configuration.

Using the CLI

✦ To enter the cellular command level: enable -> config -> if 2

Using XML

✦ Include in your file: configgroup name = "cellular interface" instance = "wwan0">

Network 2 (Cellular “wwan0”) Link Settings

This page shows configuration of an wwan0 link on the device.

Table 6-7  Network 2 (wlan0) Link Settings

<table>
<thead>
<tr>
<th>Network 2 Link Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APN</td>
<td>Enter the configurable network identifier used by a mobile device when connecting to a GSM carrier.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the Username for dial up to cellular carrier, if required.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the Password for dial up to cellular carrier, if required.</td>
</tr>
<tr>
<td>Dialup String</td>
<td>Enter the modem string used for making connection to carrier.</td>
</tr>
<tr>
<td>Roaming</td>
<td>Enable or disable the network roaming.</td>
</tr>
</tbody>
</table>

To Configure Network 2 Link Settings

Using Web Manager

✦ To modify network 2 wwan0 interface information, click Network on the menu and select Network 2 > Link > Configuration.

Using the CLI

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

Using XML

✦ Include in your file: <configgroup name = "wwan0 link" instance = "wlan0">
Network 2 (Cellular “wwan0”) QoS

QoS (Quality of Service) can be enabled and configured for both Network 1 (eth0) and Network 2 (wwan0). If enabled, the router will control the flow of outbound traffic according to the user-defined filters. In other words, QoS improves performance by allowing the user to prioritize applications. Filters can be defined to prioritize traffic based on the source or destination network, source or destination port, or the source MAC address. Up to 32 user-defined filters can be added. The following are predefined priority classes:

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

*Table 6-8* shows the network QoS settings that can be configured including adding new filters.

<table>
<thead>
<tr>
<th>Network 2 (QoS) Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Click to enable or disable state.</td>
</tr>
<tr>
<td>Import filters</td>
<td>Click to enable or disable import filters to import configurations from other interfaces.</td>
</tr>
<tr>
<td>Uplink Speed</td>
<td>Enter the maximum uplink speed. Set 0 to set speed to default.</td>
</tr>
</tbody>
</table>

*Table 6-9* Adding or Deleting Network 2 (wwan0) QoS Settings

<table>
<thead>
<tr>
<th>Adding or Deleting Network 2 (QoS) Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Click the checkbox to the left of any existing QoS filter to be deleted and click the Submit button.</td>
</tr>
</tbody>
</table>
| Filter type                                 | Select the filter type from the drop-down window:  
  - Mac Address  
  - Network  
  - Port |
| MAC Address                                 | Enter the MAC address, if the MAC Address filter type is selected. |
| Network                                     | Enter the Network, if the Network filter type is selected. |
| Ports                                       | Enter the Port, if the Port filter type is selected. |
| Priority                                    | Select the priority of the filter from the drop-down menu. |
To Configure Network 2 QoS Settings

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

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

**Using XML**
- Include in your file: `<configgroup name="cellular" instance="wwan0">

**Gateway**

The PremierWave XNXC HSPA+ intelligent gateway can be configured as a cellular wireless router with DHCP server functionality.

**Status**

This page displays the current configuration and statistics information for the gateway.
- To view gateway status: click **Gateway** on the menu and select **Status**.

**WAN**

*Table 6-10  WAN Configuration*

<table>
<thead>
<tr>
<th>Gateway Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating Mode</strong></td>
<td>Select the type of operating mode:</td>
</tr>
<tr>
<td></td>
<td>◆ <strong>Disabled</strong>: prevents the device to be used as a gateway; use the device</td>
</tr>
<tr>
<td></td>
<td>normally.</td>
</tr>
<tr>
<td></td>
<td>◆ <strong>Gateway</strong>: allows the device to be used as a router with NAT.</td>
</tr>
<tr>
<td></td>
<td>◆ <strong>Router</strong>: allows the device to be used as a router without NAT.</td>
</tr>
<tr>
<td><strong>Firewall</strong></td>
<td>Select to enable or disable firewall:</td>
</tr>
<tr>
<td></td>
<td>◆ <strong>Enabled</strong>: enables the device firewall.</td>
</tr>
<tr>
<td></td>
<td>◆ <strong>Disabled</strong>: disable the device firewall.</td>
</tr>
<tr>
<td><strong>MAC Address filter</strong></td>
<td>Select to enable or disable the MAC address filter.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>Specify the WAN interface. Generally wwan0 (cellular) interface.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Assign a static IP address to the gateway.</td>
</tr>
<tr>
<td><strong>IPv6 Address</strong></td>
<td>Assign a static IPv6 address to the gateway.</td>
</tr>
<tr>
<td><strong>Primary DNS</strong></td>
<td>Enter the IP address of the primary Domain Name Server.</td>
</tr>
</tbody>
</table>

_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.
### Network Settings

**WAN MAC Address Filters**

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

*Table 6-11 Adding a New MAC Address Filters*

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

**To Configure Gateway WAN Settings**

**Using Web Manager**

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

**Using the CLI**

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

**Using XML**

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

**Port Forwarding**

Port forwarding allows remote computers (for example, computers on the Internet) to connect to a specific computer or service within a private local-area network (LAN). Port Forwarding rules apply to inbound traffic and will not work under these conditions:

- The IP of the cellular device is not directly reachable from outside of the cellular providers network. The port forwarding rules will not work if the device does not receive any traffic.
- Hosts within the cellular providers network cannot reach the device.
- The port is blocked by the cellular provider.
- If traffic to certain ports is blocked before it reaches the PremierWave device, the port forwarding rules will still not work even with a public and accessible IP.
6: Network Settings

To Configure Gateway Port Forwarding Settings

**Using Web Manager**

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

**Using the CLI**

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

**Using XML**

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

**Static Routes**

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

**Table 6-14 Static Route Setting Routes**

<table>
<thead>
<tr>
<th>Static Route Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Enables the static route.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the static route.</td>
</tr>
<tr>
<td>Name</td>
<td>User friendly name for the route. Click on the [Edit] icon to make changes.</td>
</tr>
<tr>
<td>Route</td>
<td>Network or Host for the route.</td>
</tr>
<tr>
<td>Applied</td>
<td>If the route was successfully applied. Routing table updates require a reboot and route needs to be valid as per other device configurable.</td>
</tr>
</tbody>
</table>
Table 6-15 Adding a New Static Route

<table>
<thead>
<tr>
<th>Adding New Static Route Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the user friendly name for the route.</td>
</tr>
<tr>
<td>Network</td>
<td>Enter the Network or Host for the route.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Enter the Gateway for the route.</td>
</tr>
<tr>
<td>Interface</td>
<td>Select the Interface for the route.</td>
</tr>
<tr>
<td>Metric</td>
<td>Enter the priority for the route. Lower metric means higher priority.</td>
</tr>
<tr>
<td>Add</td>
<td>Click Add after adding new route information.</td>
</tr>
</tbody>
</table>

To Configure Gateway Static Route Settings

*Using Web Manager*

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

*Using the CLI*

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

*Using XML*

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

**DHCP Server**

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

Table 6-16 DHCP Settings

<table>
<thead>
<tr>
<th>DHCP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lease time</td>
<td>Enter the duration for which lease is initially assigned. Clients must renew after this duration.</td>
</tr>
</tbody>
</table>
| State             | Enable or Disable the DHCP server for the DHCP settings.  
  - **Enabled**: DHCP server is enabled.  
  - **Disabled**: DHCP server is disabled. |
| Start IP Address  | View or edit the Start IP Address of address pool. |
| End IP Address    | View or edit the End IP Address of address pool. |
| State             | Enable or Disable the DHCP server for the DHCPv6 settings.  
  - **Enabled**: DHCP server is enabled.  
  - **Disabled**: DHCP server is disabled. |
| Start IPv6 Address| Start IPv6 Address of address pool. |
| End IPv6 Address  | End IPv6 Address of address pool. |
To Configure Gateway DHCP Server Settings

*Using Web Manager*

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

*Using the CLI*

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

*Using XML*

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

**Static Lease Listing**

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

**Table 6-17 Static Lease Listing**

<table>
<thead>
<tr>
<th>Static Lease List Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Click checkbox beside existing static lease MAC Address/IP Address to delete, if available and if desired.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC Address of existing static leases are listed here.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Static IP Address of existing static leases are listed here.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>Static IPv6 Address of existing static leases are listed here.</td>
</tr>
</tbody>
</table>

**Table 6-18 Add a Static Lease**

<table>
<thead>
<tr>
<th>Add a Static Lease Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Enter the MAC Address of the static lease to be added.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter static IP address of the static lease to be added.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>Enter static IPv6 address of the static lease to be added.</td>
</tr>
<tr>
<td>Add</td>
<td>Click <strong>Add</strong> after adding new static lease information.</td>
</tr>
</tbody>
</table>

**Routing Protocols**

The PremierWave XC HSPA+ intelligent gateway allows the configuration of routing protocols. Routing protocols specify how routers communicate with each other, disseminating information that enables the selection of routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. Each router has a prior knowledge of networks directly attached to it. A routing protocol shares this information among immediate neighbors first, then through the network. This way, routers gain knowledge of the topology of the network. The PremierWave device supports RIP and OSPF protocols.
Table 6-19  Routing Protocol Settings

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

To Configure Gateway Routing Protocol Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

Virtual IP

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

Table 6-20  Virtual IP Settings

<table>
<thead>
<tr>
<th>Virtual IP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled (checkbox)</td>
<td>Uncheck the Enabled checkbox adjacent to a virtual IP address to enable it. Keep the checkbox checked to keep the virtual IP address enabled. A virtual IP address is enabled by default.</td>
</tr>
</tbody>
</table>
To Configure Gateway Virtual IP

Using Web Manager

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

Using the CLI

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

Using XML

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

### DDNS

The PremierWave XC HSPA+ intelligent gateway displays and allows configuration of the DDNS.

<table>
<thead>
<tr>
<th><strong>Table 6-22 DDNS Configuration</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DDNS Settings</strong></td>
</tr>
<tr>
<td>State</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>User Name</td>
</tr>
<tr>
<td>Password</td>
</tr>
<tr>
<td>Host Name</td>
</tr>
<tr>
<td>Interval</td>
</tr>
<tr>
<td>Update DDNS (button)</td>
</tr>
</tbody>
</table>
To Configure Gateway WAN Settings

Using Web Manager

❖ To view or configure DDNS information, click DDNS in the menu.

Using the CLI

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

Using XML

❖ Not any.

VPN

The PremierWave XC HSPA+ intelligent gateway provides the option to configure a virtual private network (VPN) to extend a private network across a public network. Data may be sent and received across a shared or public network as if directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.

<table>
<thead>
<tr>
<th>Table 6-23 VPN Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VPN Settings</strong></td>
</tr>
<tr>
<td>Show details (link)</td>
</tr>
<tr>
<td><strong>CONFIGURATION</strong></td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>State</td>
</tr>
<tr>
<td>Connection Type</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>IKEv2</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Authentication Mode</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>VPN Settings</td>
</tr>
<tr>
<td>------------------------------</td>
</tr>
<tr>
<td><strong>Mode Configuration</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td>Tunnel</td>
</tr>
<tr>
<td>Transport</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
</tr>
<tr>
<td><strong>REMOTE NETWORK</strong></td>
</tr>
<tr>
<td>Endpoint</td>
</tr>
<tr>
<td>Subnet</td>
</tr>
<tr>
<td>ID</td>
</tr>
<tr>
<td>Router/Next Hop</td>
</tr>
<tr>
<td><strong>LOCAL NETWORK</strong></td>
</tr>
<tr>
<td>Subnet</td>
</tr>
<tr>
<td>ID</td>
</tr>
<tr>
<td>Router/Next Hop</td>
</tr>
<tr>
<td><strong>KEY MANAGEMENT</strong></td>
</tr>
<tr>
<td>Perfect Forward Secrecy (PFS)</td>
</tr>
<tr>
<td>Pre-shared key (PSK)</td>
</tr>
<tr>
<td><strong>ISAKMP PHASE 1 (IKE)</strong></td>
</tr>
<tr>
<td>Aggressive Mode</td>
</tr>
<tr>
<td>NAT Traversal</td>
</tr>
<tr>
<td>Encryption</td>
</tr>
<tr>
<td>Authentication</td>
</tr>
<tr>
<td>DH Group</td>
</tr>
<tr>
<td>IKE Lifetime</td>
</tr>
<tr>
<td><strong>ISAKMP PHASE 2 (ESP)</strong></td>
</tr>
<tr>
<td>Encryption</td>
</tr>
<tr>
<td>Authentication</td>
</tr>
<tr>
<td>DH Group</td>
</tr>
<tr>
<td>SA Lifetime</td>
</tr>
</tbody>
</table>
To Configure VPN Settings

**Using Web Manager**

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

**Using the CLI**

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

**Using XML**

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

**GRE Settings**

GRE tunneling is available on the PremierWave XC HSPA+ intelligent gateway, providing more capabilities than IP-in-IP tunneling. For example, it supports transporting multicast traffic and IPv6 through a GRE tunnel.

### Table 6-24  GRE Settings

<table>
<thead>
<tr>
<th>GRE Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the user-defined name of the GRE tunnel.</td>
</tr>
<tr>
<td>State</td>
<td>Select to enable and disable GRE tunnel.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Assign an IP address/mask for the GRE tunnel.</td>
</tr>
<tr>
<td>MTU</td>
<td>Enter the number of bytes indicating the largest physical packet size that</td>
</tr>
<tr>
<td></td>
<td>the network can transmit.</td>
</tr>
<tr>
<td>Local Network</td>
<td>Select the local network to use the GRE tunnel. Select <strong>vpn</strong> to use the</td>
</tr>
<tr>
<td></td>
<td>VPN network. Select <strong>any</strong> to use any available interface to remote host.</td>
</tr>
<tr>
<td>Remote Host</td>
<td>Enter the remote IP address to use for the GRE tunnel.</td>
</tr>
<tr>
<td>Remote Network</td>
<td>Enter the remote network to use for the GRE tunnel.</td>
</tr>
</tbody>
</table>
To Configure Tunnel Serial Settings

**Using Web Manager**

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

**Using the CLI**

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

**Using XML**

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

The Cellular page displays the configuration and status for the Cellular module.

<table>
<thead>
<tr>
<th>Cellular Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN Lock</td>
<td>Enable to prevent unauthorized use of the SIM card.</td>
</tr>
<tr>
<td>PIN</td>
<td>Enter PIN combination to enable PIN Lock. Caution: If you enter the PIN incorrectly 3 times, the SIM card will lock, and you will need a PIN Unblocking Key (PUK) to unlock your SIM card. PUK is required to unlock SIM cards that have become locked following 3 successive incorrect PIN entries. Caution: If you enter the PUK incorrectly 10 times, the SIM card will be permanently locked and no longer operable.</td>
</tr>
<tr>
<td>Allowed Bands</td>
<td>Select the allowed bands, determining the frequency band usage of the device. Select/Unselect individual bands to restrict the allowed bands to a specific band or band combination.</td>
</tr>
<tr>
<td>Antenna Diversity</td>
<td>Select to enable or disable. Antenna Diversity controls the RX receiver antenna diversity support to achieve verification of received paths and support of CTIA 3.0 diversity tests (relevant for application approval).</td>
</tr>
<tr>
<td></td>
<td><strong>Enabled</strong> uses both antennas for RX operation. Enables RX diversity functionality by activating both antennas for RX operation. This setting becomes effective after next restart of the device.</td>
</tr>
<tr>
<td></td>
<td><strong>Disabled</strong> uses only the primary antenna for RX operation. Disables RX diversity functionality. Activate only the first antenna for RX operation, i.e., use the primary antenna for reception. The secondary (diversity) receiver path is switched off. This setting becomes effective after next restart of the device.</td>
</tr>
</tbody>
</table>

To Configure Cellular Settings

Using Web Manager

- Click Cellular on the menu.

Using the CLI

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

Using XML

- Include in your file: `<configgroup name = "cellular">`
Typical Cellular Error (errcodes)

The following is a list of common errors that may appear in the Cellular module.

- PH-SIM PIN required
- PH-FSIM PIN required
- PH-FSIM PUK required
- SIM not inserted
- SIM PIN required
- SIM PUK required
- SIM failure
- SIM busy
- SIM wrong
- incorrect password
- SIM PIN2 required
- SIM PUK2 required
8: Input/Output Ports

Relay Output

Note: When the relay is energized/turned on, the relay is closed, connecting both relay ports on the I/O connector through the relay. When the relay is turned off, the signal path is open, disconnecting the relay ports on the I/O connector.

Table 8-1 Relay Output Settings

<table>
<thead>
<tr>
<th>Relay Output Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>This field is found in the Relay Status page. Indicates state of the relay. Select On or Off to change the state of the relay.</td>
</tr>
<tr>
<td>Title</td>
<td>Enter the relay title as it will appear in web manager, XML and CLI. Leave this field blank to utilize the default &quot;Relay N&quot;, where N is the relay number. For example, you can name the reading, “Buzzer”, if a buzzer is connected to the PremierWave device.</td>
</tr>
<tr>
<td>Latch</td>
<td>Enable or disable Latch controls which determine how a relay will be turned off.</td>
</tr>
<tr>
<td></td>
<td>Selecting Enabled will require a user to explicitly reset latched relay and then turn it off.</td>
</tr>
<tr>
<td></td>
<td>Selecting Disabled, the relay will automatically turn off after any and all of the alarm triggers are no longer active.</td>
</tr>
</tbody>
</table>

To Configure Relay Settings

Using Web Manager

To configure relay output, go to the Setup tab/page and click Relay > Relay 1 > Status in the menu.

To change relay state, go to the Setup tab/page and click Relay > Relay 1 > Configuration in the menu.

Using the CLI

To enter the relay command level: enable -> config -> relays -> relay <number>

Using XML

Include in your file: <configgroup name="relay" instance="<number>"
Digital Input

Table 8-2 contains additional configuration options for Digital Input 1 and Digital Input 2 settings:

<table>
<thead>
<tr>
<th>Digital Input Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>This field is found in the Digital Input Status page. Indicates state of the digital input.</td>
</tr>
<tr>
<td>Title</td>
<td>Fill in Title to customize how the digital input status will appear in the CLI, Web Manager, and XML status. Leave Title blank for the default title of &quot;Digital Input N&quot;, where N is the digital input number.</td>
</tr>
<tr>
<td>Normal State</td>
<td>Select Normal State to Low or High. When input state changes, Normal State is used to compare with the input state. If the states are different, an alarm will be triggered which is configured under &quot;Action&quot; menu.</td>
</tr>
</tbody>
</table>

To Configure Digital Input Settings

Using Web Manager

- To modify digital input information, click Digital Input on the menu, select either Digital Input 1 or Digital Input 2, and click the Configuration link.

Using the CLI

- To enter the digital input command level: enable -> config -> action -> digital input 1 state change
- To enter the digital input command level: enable -> config -> action -> digital input 2 state change
- To enter the digital input command level: enable -> config -> digital inputs -> digital input <number>

Using XML

- Include in your file: <configgroup name = "action" instance = "digital input 1 state change">
- Include in your file: <configgroup name = "action" instance = "digital input 2 state change">
- Include in your file: <configgroup name="digital input" instance="<number>

Table 8-2  Digital Input Settings
9: **Action Settings**

Actions can be configured for alarms and reports available in the PremierWave XC HSPA+ intelligent gateway.

**Alarms and Reports**

PremierWave XC HSPA+ intelligent gateway updates the action settings page to display and configure the alarms. The following alarm and report actions are available in PremierWave XC HSPA+ device:

- eth0 link state change
- wwan0 link state change
- Digital input 1 state change
- Digital input 2 state change
- Device temperature change
- Cellular temperature change
- On scheduled reboot

*Note:* One or more types of “action” can be configured and triggered when an event occurs. The “on scheduled reboot” alarm state will be on at the time of a scheduled reboot and will remain on till the device actually reboots (in approximately 30 seconds). These are not applicable for “on scheduled reboot” alarm: Email Alarm Reminder Interval, Normal Email, Normal Message, Normal Reminder Interval, SNMP Reminder Interval, SNMP Normal Message, and Delay.

**Actions**

*Table 9-1* contains the configuration options for all the alarms and reports listed above.

<table>
<thead>
<tr>
<th><strong>Table 9-1 Action Settings</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action Settings</strong></td>
</tr>
<tr>
<td>Delay</td>
</tr>
<tr>
<td>Email</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
To Configure Action Settings

**Using Web Manager**

- To view Action status information, click **Action** on the menu and select **Status**.
- To modify Action information, click **Action** on the menu and select a specific action from the drop-down menu. **Alarms and Reports (on page 62)** lists the options.

**Using the CLI**

- To enter the `eth0 link state change` command level: `enable -> config -> action -> eth0 link state change`

### Action Settings

<table>
<thead>
<tr>
<th>Action Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FTP Put</strong></td>
<td>Use FTP Put to put a file on configured FTP server. Filename will be used to upload to remote FTP server. The IP <strong>Address</strong> or hostname is the FTP server to connect. Port number is port on which FTP server is listening on. Use Protocol to connect to FTP server. FTPS is a SSL encrypted communication channel and SSL Trusted Authorities must be setup with FTP server SSL certificate. Username is used to logon to FTP server. If FTP server does not require authentication, use anonymous. Password is used to logon to FTP server. If FTP server does not require authentication, a common practice is to use user’s email address. If the alarm stays on or off longer than the <strong>Reminder Interval</strong>, another FTP Put is performed. In <strong>Sequential</strong> mode, connections will be attempted starting with number 1 until a connection is successful. In <strong>Simultaneous</strong> mode, all possible connections will be made.</td>
</tr>
<tr>
<td><strong>HTTP Post</strong></td>
<td>Use HTTP Post post to configured HTTP server. The URL appears behind the HTTP server IP address or hostname. E.g. <code>http://some_http_server/some_url</code> The IP <strong>Address</strong> or hostname is the HTTP server to connect to. Port number is the port which HTTP server is listening on. Use Protocol to connect to HTTP server. HTTPS is a SSL encrypted communication channel and SSL Trusted Authorities must be setup with HTTP server SSL certificate. Username used to logon to HTTP server if authentication is required. Password used to logon to HTTP server if authentication is required. If the alarm stays on or off longer than the <strong>Reminder Interval</strong>, another HTTP Post is performed. In <strong>Sequential</strong> mode, connections will be attempted starting with number 1 until a connection is successful. In <strong>Simultaneous</strong> mode, all possible connections will be made.</td>
</tr>
<tr>
<td><strong>Relay</strong></td>
<td>Select a Relay to switch on when this alarm is activated. Select “None” so this alarm state will have no effect on any Relay.</td>
</tr>
<tr>
<td><strong>GPRS Roaming</strong></td>
<td>Select to enable or disable GPRS roaming when this alarm is on. Select No Change so this alarm <strong>State</strong> will have no effect on GPRS roaming.</td>
</tr>
<tr>
<td><strong>SMS</strong></td>
<td>Use SMS to send SMS to a configured <strong>Recipient</strong>. The contents of <strong>Alarm Message</strong> will be placed into the SMS body when an alarm SMS is sent. If the alarm stays on longer than the <strong>Reminder Interval</strong>, another alarm SMS is sent. The contents of <strong>Normal Message</strong> will be placed into the SMS body when a normal SMS is sent. If the alarm stays off longer than the Reminder Interval, another normal SMS is sent.</td>
</tr>
<tr>
<td><strong>SNMP Trap</strong></td>
<td>Use SNMP Trap to send SNMP trap to configured trap destinations. Check to enable or disable the <strong>State</strong>. The contents of <strong>Alarm Message</strong> are included when an alarm SNMP trap is sent. If the alarm stays on longer than the <strong>Reminder Interval</strong>, another alarm SNMP Trap is sent. The contents of <strong>Normal Message</strong> are included when a normal SNMP trap is sent. If the alarm stays off longer than the Reminder Interval, another normal SNMP Trap is sent.</td>
</tr>
</tbody>
</table>
To enter the wwan0 link state change command level: enable -> config -> action -> wwan0 link state change

To enter digital input 1 state change command level: enable -> config -> action -> digital input 1 state change

To enter digital input 2 state change command level: enable -> config -> action -> digital input 2 state change

To enter device temperature change command level: enable -> config -> action -> device temperature change

To enter cellular temperature change command level: enable -> config -> action -> cellular temperature change

To enter cellular temperature change on scheduled reboot command level: enable -> config -> action -> on scheduled reboot

**Using XML**

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

Include in your file: `<configgroup name = "action" instance = "wwan0 link state change">

Include in your file: `<configgroup name = "digital input 1 state change">

Include in your file: `<configgroup name = "digital input 2 state change">

Include in your file: `<configgroup name = "device temperature change">

Include in your file: `<configgroup name = "cellular temperature change">

Include in your file: `<configgroup name = "action" instance = "on scheduled reboot">

**Python**

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

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

**IDE**

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

The PremierWave XC HSPA+ intelligent gateway supports the ability to install and uninstall user-defined Python scripts and packages and will include the following:

<table>
<thead>
<tr>
<th>bin</th>
<th>python</th>
</tr>
</thead>
<tbody>
<tr>
<td>lib</td>
<td>libpython{version}.so</td>
</tr>
<tr>
<td></td>
<td>&lt;ltrx python sdk&gt;</td>
</tr>
<tr>
<td></td>
<td>libpython{version} &quot;python precompiled scripts&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;python shared libraries&quot;</td>
</tr>
</tbody>
</table>

Table 9-2 contains the setting options for configuring, installing, uninstalling and running external applications via Python scripts.

Caution: Use extreme caution when installing and running scripts.

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

**Using Web Manager**

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

**Using the CLI**

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

**Using XML**

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

<table>
<thead>
<tr>
<th>Script Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>Enter the package file name pathway in the file system and click the Install button to install it.</td>
</tr>
</tbody>
</table>
10: Line and Tunnel Settings

The PremierWave XC HSPA+ intelligent gateway has two tunnels through which you may view statistics or configure the Accept Mode. The PremierWave XC HSPA+ intelligent gateway contains two serial lines. All lines use standard RS232/RS485 serial ports. All lines can be configured to operate in the following modes:

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

Line Statistics

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

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

Using Web Manager

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

Using the CLI

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

Using XML

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

Line Settings

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

To Configure Line Settings

Using Web Manager

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

Using the CLI

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

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

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

<table>
<thead>
<tr>
<th>Line Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>Interface</td>
<td>Set the interface type for the Line. The default is RS232. Choices are:</td>
</tr>
<tr>
<td></td>
<td>- RS232</td>
</tr>
<tr>
<td></td>
<td>- RS485 Full-Duplex</td>
</tr>
<tr>
<td></td>
<td>- RS485 Half-Duplex</td>
</tr>
<tr>
<td>State</td>
<td>Select to enable or disable the operational state of the Line. The default is Enabled.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Set the operational protocol for the Line. The default is Tunnel. Choices are:</td>
</tr>
<tr>
<td></td>
<td>- None</td>
</tr>
<tr>
<td></td>
<td>- Tunnel = Serial-Network tunneling protocol.</td>
</tr>
<tr>
<td>Baud Rate</td>
<td>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 500000.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The maximum baud rate in RS232 mode is 1000000 bps. Custom baud rates are not supported when a line is configured for Command Mode.</td>
</tr>
<tr>
<td>Parity</td>
<td>Set the Parity of the Line. The default is None.</td>
</tr>
<tr>
<td>Data Bits</td>
<td>Set the number of data bits for the Line. The default is 8.</td>
</tr>
<tr>
<td>Stop Bits</td>
<td>Set the number of stop bits for the Line. The default is 1.</td>
</tr>
<tr>
<td>Flow Control</td>
<td><strong>Note:</strong> Set the flow control for the Line. The default is None.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field becomes available if RS232 or RS485 Full-Duplex is selected under Interface above.</td>
</tr>
<tr>
<td>Gap Timer</td>
<td>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).</td>
</tr>
<tr>
<td>Threshold</td>
<td>Set the number of threshold bytes which need to be received in order for the driver to forward received characters.</td>
</tr>
</tbody>
</table>
### Table 10-2 Line Command Mode Settings

<table>
<thead>
<tr>
<th>Line Command Mode Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mode</strong></td>
<td>Set the Command Mode state of the Line. When in Command Mode, a CLI session operates exclusively on the Line. Choices are:</td>
</tr>
<tr>
<td></td>
<td>♦ Always</td>
</tr>
<tr>
<td></td>
<td>♦ User Serial String</td>
</tr>
<tr>
<td></td>
<td>♦ Disabled</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td><strong>Wait Time</strong></td>
<td>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”.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field becomes available when Use Serial String is selected for Mode.</td>
</tr>
<tr>
<td><strong>Serial String</strong></td>
<td>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].</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field becomes available when Use Serial String is selected for Mode.</td>
</tr>
<tr>
<td><strong>Echo Serial String</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field becomes available when Use Serial String is selected for Mode.</td>
</tr>
<tr>
<td><strong>Signon Message</strong></td>
<td>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].</td>
</tr>
</tbody>
</table>

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

### To Configure Line Command Mode

#### Using Web Manager

- To configure a specific line, click Line in the menu and select Line 1 -> Configuration (Table 10-1).
- To configure a specific line in Command Mode, click Line in the menu and select Line 1 -> Command Mode (Table 10-2).

#### Using the CLI

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

#### Using XML

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

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

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

To View Tunnel Statistics

**Using Web Manager**

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

**Using the CLI**

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

**Using XML**

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

Tunnel Settings

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

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

Serial Settings

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

<table>
<thead>
<tr>
<th><strong>Table 10-3 Tunnel Serial Settings</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tunnel Serial Settings</strong></td>
</tr>
<tr>
<td><strong>Line Settings</strong></td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th><strong>Table 10-4 Tunnel Packing Mode Settings</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tunnel Packing Mode Settings</strong></td>
</tr>
<tr>
<td>-------------------------------------</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Threshold</strong></td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
</tr>
</tbody>
</table>
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 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 10-5 Tunnel Accept Mode Settings

<table>
<thead>
<tr>
<th>Tunnel Accept Mode Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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 |
| **Protocol**                | Select the protocol type for use with Accept Mode:  
  - **SSH**  
  - **SSL**  
  - **TCP** *(default protocol)*  
  - **TCP AES**  
  - **Telnet** |
| **Credentials**             | Specifies the name of the set of RSA and/or DSA certificates and keys to be used for an SSL connection. |
| **AES Encrypt Key**         | Specify the text or hexadecimal advanced encryption standard (AES) key for encrypting outgoing data for a TCP AES connection. |
| **AES Decrypt Key**         | Specify the text or hexadecimal AES key for decrypting incoming data for a TCP AES connection. |
| **TCP Keep Alive Idle Time**| Enter the time, in milliseconds, the PremierWave XC HSPA+ module waits during a silent TCP connection before checking if the currently connected network device is still on the network. |
| **TCP Keep Alive Interval** | Enter, in milliseconds, the amount of time between two successive keep alive probes if no acknowledgment to the previous keep alive probe is not received. |
| **TCP Keep Alive Probes**   | Specify the number of TCP Keep Alive probes (after the TCP Initial Keep Alive probe) to send before closing the connection if no response is received. Valid values are between 1 and 16. Blank the display field to restore the default. |
## 10: Line and Tunnel Settings

<table>
<thead>
<tr>
<th>Tunnel Accept Mode Settings (continued)</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Initial Send**                       | Enter the Initial Send string indicating whether it is in Text or Binary form. This Initial Send data will be sent out to the network upon connection establishment, before any data, from the Line. It may contain one or more directives in the form `%<char>`. The binary form allows square braces [] to enclose one or more character designations separated by commas. Use straight decimals up to 255 or hexadecimal numbers prefixed with `0x` up to `0xFF` within the square braces. To specify an open brace in binary mode, use two in a row. Example (in binary mode): `AB [255, 0xFF [C [D]]` results in a string containing binary values where the dots appear: `AB..C[D]`. **Directives:**  
  - `%i` local IP address  
  - `%m` MAC address  
  - `%n` network interface name  
  - `%p` local port  
  - `%s` serial number  
  - `%` % |
| **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. |
| **Block Network**                      | Set whether Block Network is enabled for debugging purposes. Choices are:  
  - **Enabled** = if Enabled, incoming characters from the network will not be processed. Instead, they will be buffered and will eventually flow off the network side.  
  - **Disabled** = this is the default setting; incoming characters from the network will be processed. 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. |
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 intelligent gateway unit continues to attempt an outgoing connection on the network, until established (based on which connection method is selected in the configuration described in Table 10-6). 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 v6 address or DNS name. The PremierWave device will not make a connection unless it can resolve the address.

For Connect Mode using UDP, the PremierWave 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.*

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>
<thead>
<tr>
<th>Tunnel Connect Mode Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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 device retries until it makes a connection.  
  - **Any Character** = a connection is attempted when any character is read on the serial line.  
  - **Start Character** = a connection is attempted when the start character for the selected tunnel is read on the serial line.  
  - **Modem Control Asserted** = a connection is attempted as long as the Modem Control pin (DSR) is asserted, until a connection is made.  
  - **Modem Emulation** = a connection is attempted when triggered by modem emulation AT commands.  
| **Local Port**              | 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. |

---

**Table 10-6 Tunnel Connect Mode Settings**
Click on the displayed information to expand it for editing. If <None> is displayed, clicking it will allow you to configure a new host. At least one Host is required to enable Connect Mode as this information is necessary to connect to that host. Once you start to edit Host 1, a box for Host 2 will show up. Editing Host 2 will cause a Host 3 box to appear. Up to 32 hosts are available.

Complete the following fields to configure a host:

- **Address**: enter the address for the remote host connection. Either a DNS address or an IP address maybe provided.
- **Port**: designate the TCP or UDP port on the remote host for connection.
- **Protocol**: select the desired security protocol. SSH is recommended for circumstances with high security concerns. When using SH, both the SSH server host keys and the SSH server authorized users must be configured.
- **TCP Initial Keep Alive**: specify the amount of time to wait before the first Keep Alive probe is sent to the remote host in order to keep the TCP connection up during idle transfer periods. Set to 0 to disable and blank the display field to restore the default.
- **TCP Keep Alive Interval**: specify the amount of time to wait before probing the remote host, after the initial probe, in order to keep the TCP connection up during idle transfer periods. Blank the display field to restore the default.
- **TCP Keep Alive Probes**: specify the number of TCP Keep Alive probes (after the TCP Initial Keep Alive Probe) to send before closing the connection if no response is received. Valid values are between 1 and 16. Blank the display field to restore the default.
- **TCP User Timeout**: specify the amount of time the TCP segments will be retransmitted before the connection is closed.
- **Initial Send**: enter the Initial Send string for data sent out of the network upon connection establishment (before any data from the Line). The string may contain one or more Directives of the form %<char> and can be entered in Text or Binary form.

**Notes:**

- If the keep alive idle time (the initial keep alive probe) expires, the user timeout is expired, and there are probes in flight, the connection will be reset. For this reason, it is recommended that if keep alive is used in conjunction with the user timeout, the keep alive timeouts be larger than the user timeout. If they are smaller, what will typically be seen is that the initial probe will be sent, then at the interval where the next probe would normally be sent, the connection will be reset, with no additional probes sent. Also note that the probe count can be disregarded in these cases: if the keep alive timers are significantly smaller than the user timeout, probes will continue to be sent for an unreachable host until the user timeout expires.
- If there is data in flight when the TCP retransmission timeout kicks in, the user timeout is checked as a limiting condition only when the timer expirations would normally be checked during RTO handling. In other words, the user timeout will not be an exact limit; in practice, it will always take somewhat longer for the connection to be closed. The longer the user timeout is, the more likely it will expire between exponentially slower retransmissions, and the connection will not experience an error until the next retransmission timeout is checked. Also note that the user timeout expiration during retransmission returns an error to the application; it does not automatically reset the connection as happens with keep alive timeout. It is up to the application (e.g., tunneling) to close the connection (this happens almost immediately with tunneling).
To Configure Tunnel Connect Mode Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

Connecting Multiple Hosts

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

- **Sequential** – Sequential host lists establish a prioritized list of tunnels. The host specified as Host 1 will be attempted first. If that fails, it will proceed to Host 2, 3, etc., in the order they are specified. When a connection drops, the cycle starts again with Host 1 and proceeds in order. Establishing the host order is accomplished with host list promotion (see **Host List Promotion on page 78**). Sequential is the default Host Mode.

<table>
<thead>
<tr>
<th><strong>Tunnel Connect Mode Settings (continued)</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reconnect Timer</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
| **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. |
Simultaneous – A tunnel will connect to all hosts accepting a connection. Simultaneous connections occur at the same time to all listed hosts. The device can support a maximum of 64 total aggregate connections.

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

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

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

Table 10-7 Tunnel Disconnect Mode Settings

<table>
<thead>
<tr>
<th>Tunnel Disconnect Mode Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stop Character</strong></td>
<td>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: &lt;control&gt;J or 0xA(hexadecimal) or \10(decimal). Disable the Stop Character by blanking the field to set it to &lt;None&gt;.</td>
</tr>
<tr>
<td><strong>Modem Control</strong></td>
<td>Set whether Modem Control enables disconnect when the Modem Control pin is not asserted on the Serial Line. Choices are: ✦ Enabled ✦ Disabled (default)</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>Enter the number of milliseconds a tunnel may be idle before disconnection. The value of zero disables the idle timeout.</td>
</tr>
<tr>
<td><strong>Flush Serial Data</strong></td>
<td>Set whether to flush the Serial Line when the Tunnel is disconnected. Choices are: ✦ Enabled ✦ Disabled (default)</td>
</tr>
</tbody>
</table>

To Configure Tunnel Disconnect Mode Settings

Using Web Manager
✦ To configure the Disconnect Mode for a specific tunnel, click Tunnel in the menu and select Tunnel 1 -> Disconnect Mode.

Using the CLI
✦ To enter the Tunnel 1 Disconnect command level: enable -> tunnel 1 -> disconnect
Using XML

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

Modem Emulation

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

### Table 10-8 Tunnel Modem Emulation Settings

<table>
<thead>
<tr>
<th>Tunnel Modem Emulation Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| Echo Pluses                    | Set whether the pluses will be echoed back during a "pause +++ pause" escape sequence on the Serial Line. Choices are:  
  - Enabled                        
  - Disabled (default)             |
| Echo Commands                  | Set whether characters read on the Serial Line will be echoed, while the Line is in Modem Command Mode. Choices are:  
  - Enabled                        
  - Disabled (default)             |
| Verbose Response               | Set whether Modem Response Codes are sent out on the Serial Line. Choices are:  
  - Enabled                        
  - Disabled (default)             |
| Response Type                  | Select a representation for the Modem Response Codes sent out on the Serial Line. Choices are:  
  - Text (ATV1) (default)          
  - Numeric (ATV0)                 |
| Error Unknown Commands         | Set whether the Error Unknown Commands is enabled (ATU0) and ERROR is returned on the Serial Line for unrecognized AT commands. Otherwise (ATU1) OK is returned for unrecognized AT commands. Choices are:  
  - Enabled                        
  - Disabled (default)             |
| Incoming Connection            | Set how and if requests are answered after an incoming RING (ATS0=2). Choices are:  
  - Disabled (default)             
  - Automatic                      
  - Manual                         |
| Connect String                 | Enter the customized Connect String sent to the Serial Line with the Connect Modem Response Code. |
| Display Remote IP              | Set whether the Display Remote IP is enabled so that the incoming RING sent on the Serial Line is followed by the IP address of the caller. Choices are:  
  - Enabled                        
  - Disabled (default)             |
To Configure Tunnel Modem Emulation Settings

**Using Web Manager**

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

**Using the CLI**

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

**Using XML**

- Include in your file: `<configgroup name="tunnel modem" instance="1">`
11: 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 11-1  Terminal on Network and Line Settings

<table>
<thead>
<tr>
<th>Terminal on Network and Line Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Type</td>
<td>Enter text to describe the type of terminal. The text will be sent to a host via IAC. &lt;br&gt;<strong>Note:</strong> IAC means, “interpret as command.” It is a way to send commands over the network such as <strong>send break</strong> or <strong>start echoing</strong>. IAC is only supported in Telnet.</td>
</tr>
<tr>
<td>Login Connect Menu</td>
<td>Select the interface to display when the user logs in. Choices are: &lt;br&gt;◆ <strong>Enabled</strong> = shows the Login Connect Menu. &lt;br&gt;◆ <strong>Disabled</strong> = shows the CLI (default)</td>
</tr>
<tr>
<td>Exit Connect Menu</td>
<td>Select whether to display a choice for the user to exit the Login Connect Menu and reach the CLI. Choices are: &lt;br&gt;◆ <strong>Enabled</strong> = a choice allows the user to exit to the CLI. &lt;br&gt;◆ <strong>Disabled</strong> = there is no exit to the CLI (default)</td>
</tr>
<tr>
<td>Send Break</td>
<td>Enter a Send Break control character, e.g., &lt;control&gt; 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). &lt;br&gt;<strong>Note:</strong> This configuration option is only available for Line Terminals.</td>
</tr>
<tr>
<td>Break Duration</td>
<td>Enter how long the break should last in milliseconds, up to 10000. Default is 500. &lt;br&gt;<strong>Note:</strong> This configuration option is only available for Line Terminals.</td>
</tr>
<tr>
<td>Echo</td>
<td>Select whether to enable echo: &lt;br&gt;◆ <strong>Enabled</strong> &lt;br&gt;◆ <strong>Disabled</strong> &lt;br&gt;<strong>Note:</strong> 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.</td>
</tr>
</tbody>
</table>
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 11-2 Host Configuration

<table>
<thead>
<tr>
<th>Host Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocol to use to connect to the host. Choices are: Telnet, SSH. <strong>Note:</strong> SSH keys must be loaded or created on the SSH page for the SSH protocol to work.</td>
</tr>
</tbody>
</table>
To Configure Host Settings

**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.

---

**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">`
12: 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 12-1 DNS Settings

<table>
<thead>
<tr>
<th>Setting / Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 XC HSPA+ intelligent gateway firmware. A configurable option is provided to enable or disable access via this protocol.

Table 12-2 FTP Settings

<table>
<thead>
<tr>
<th>FTP Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| State        | Select to enable or disable the FTP server:  
  - Enabled (default)  
  - Disabled |

To Configure FTP Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

Syslog Settings

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

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

Table 12-3 Syslog Settings

<table>
<thead>
<tr>
<th>Syslog Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
To View or Configure Syslog Settings

**Using Web Manager**

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

**Using the CLI**

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

**Using XML**

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

### HTTP Settings

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

<table>
<thead>
<tr>
<th>HTTP Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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. |
| **Secure Credentials** | Specify the name of the set of RSA and/or DSA certificates and keys to be used for the secure connection. |
To Configure HTTP Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

<table>
<thead>
<tr>
<th>HTTP Settings (continued)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Timeout</td>
<td>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.</td>
</tr>
<tr>
<td>Max Bytes</td>
<td>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.</td>
</tr>
<tr>
<td>Logging State</td>
<td>Select to enable or disable HTTP server logging:  ◆ Enabled (default) ◆ Disabled</td>
</tr>
<tr>
<td>Max Log Entries</td>
<td>Set the maximum number of HTTP server log entries. Only the last Max Log Entries are cached and viewable.</td>
</tr>
<tr>
<td>Log Format</td>
<td>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 &lt;version&gt;')  ◆ %s - return status</td>
</tr>
<tr>
<td>Authentication Timeout</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 12-5  HTTP Authentication Settings

<table>
<thead>
<tr>
<th>HTTP Authentication Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
| Submit (button)             | Click the Submit button after entering the HTTP authentication information. |
| Delete (button)             | Click the Delete button to delete the HTTP authentication information. |

To Configure HTTP Authentication

**Using Web Manager**

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

**Using the CLI**

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

**Using XML**

- Include in your file: `<configgroup name="http authentication uri" instance="uri name">`

RSS Settings

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

Table 12-6  RSS Settings

<table>
<thead>
<tr>
<th>RSS Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSS Feed</td>
<td>Select On or Off for RSS feeds to an RSS publisher. The default setting is off.</td>
</tr>
<tr>
<td>Persistent</td>
<td>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.</td>
</tr>
<tr>
<td>Max Entries</td>
<td>Set the maximum number of log entries. Only the last Max Entries are cached and viewable.</td>
</tr>
</tbody>
</table>
### RSS Settings

<table>
<thead>
<tr>
<th>RSS Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Click the button to view RSS feeds.</td>
</tr>
<tr>
<td>Clear</td>
<td>Click the button to clear RSS feed data.</td>
</tr>
</tbody>
</table>

#### To Configure RSS Settings

**Using Web Manager**

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

**Using the CLI**

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

**Using XML**

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

## SNMP Settings

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

### Table 12-7 SNMP Settings

<table>
<thead>
<tr>
<th>SNMP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select to enable or disable the SNMP agent state.</td>
</tr>
<tr>
<td>Version</td>
<td>Select the SNMP version used by the SNMP agent.</td>
</tr>
<tr>
<td>Read Community</td>
<td>Specify the read community used by the agent (defaults to public community).</td>
</tr>
<tr>
<td>Write Community</td>
<td>Specify the write community used by the agent (defaults to private community).</td>
</tr>
<tr>
<td>System Contact</td>
<td>Specify the system contact.</td>
</tr>
<tr>
<td>System Name</td>
<td>Update the system name, as necessary. The default system name is “”.</td>
</tr>
<tr>
<td>System Description</td>
<td>Update the system description, as necessary. The default system information includes the manufacturer name, model name, version and the serial number of the device.</td>
</tr>
<tr>
<td>System Location</td>
<td>Specify a system location for the SNMP setting.</td>
</tr>
<tr>
<td>Lantronix MIB File</td>
<td>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.</td>
</tr>
<tr>
<td>MIB File</td>
<td>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.</td>
</tr>
</tbody>
</table>

#### To Configure SNMP Settings
**Using Web Manager**

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

**Using the CLI**

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

**Using XML**

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

**Discovery**

The current statistics and configuration options for device discovery, including UPnP query port are available for the PremierWave XC HSPA+ intelligent gateway.

**Table 12-8 Discovery Settings**

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

**To Configure Discovery**

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

**Using Web Manager**

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

**Using the CLI**

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

**Using XML**

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

Table 12-9 SMTP Settings

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

To Configure SMTP Settings

Using Web Manager

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

Using the CLI

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

Using XML

- Include in your file: `<configgroup name="smtp">`
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">`
13: **SMS Settings**

SMS settings allows the user to view and configure inbound/outbound SMS to/from the device. Adding a number to the SMS whitelist allows the SMS from the number to trigger one or more control functions on the device. The following control functions are available:

- **Shoulder-Tap** function can be used to bring up the cellular connection. Since this function has only one action ("on"), the message text should be "shoulder-tap".

- **Relay Control** function can be used to turn a relay on or off. To turn a relay on, the text should be "relay 1 on", or on a device with a single relay, just "relay on". To turn a relay off, the text should be "relay 1 off", or on a device with a single relay, just "relay off".

**Inbound SMS**

**Table 13-1 Inbound SMS Settings**

<table>
<thead>
<tr>
<th>Inbound SMS Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Click beside an existing SMS Sender Configuration to delete it.</td>
</tr>
<tr>
<td>Number</td>
<td>View the sender number of an existing SMS sender.</td>
</tr>
<tr>
<td>Shoulder Tap</td>
<td>Check to allow incoming SMS with content containing ‘shoulder tap’ from this sender to start the cellular interface.</td>
</tr>
<tr>
<td>Relay Control</td>
<td>Check to allow incoming SMS with content containing ‘relay N On/Off’ from this sender to open and close the device relays.</td>
</tr>
</tbody>
</table>

**Table 13-2 Adding a New SMS Settings**

<table>
<thead>
<tr>
<th>Inbound SMS Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Enter the new SMS Sender number to be added.</td>
</tr>
<tr>
<td>Whitelists</td>
<td>Check to select a specific whitelist to be associated with newly added SMS sender number:</td>
</tr>
<tr>
<td></td>
<td>- Shoulder Tap</td>
</tr>
<tr>
<td></td>
<td>- Relay Control</td>
</tr>
<tr>
<td>Add (button)</td>
<td>Click the Add button after entering the new SMS sender information.</td>
</tr>
</tbody>
</table>

**Outbound SMS**

**Table 13-3 Outbound SMS Settings**

<table>
<thead>
<tr>
<th>Outbound SMS Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Center Default Number</td>
<td>Displays the Message Center number as configured in the SIM.</td>
</tr>
<tr>
<td>Message Center Override Number</td>
<td>Enter a number to override the existing Message Center number.</td>
</tr>
<tr>
<td>Band</td>
<td>Select a band from the drop-down menu:</td>
</tr>
<tr>
<td></td>
<td>- Circuit Switched only</td>
</tr>
<tr>
<td></td>
<td>- Packet Domain only</td>
</tr>
<tr>
<td></td>
<td>- Circuit Switched preferred</td>
</tr>
<tr>
<td></td>
<td>- Packet Domain preferred</td>
</tr>
<tr>
<td>Note:</td>
<td>Check with your service provider for supported bands.</td>
</tr>
</tbody>
</table>
To Configure Inbound SMS

**Using Web Manager**

- To view and configure inbound SMS, click **SMS** in the menu and select **Inbound**.

**Using the CLI**

- To enter the command level:  `enable -> configure -> sms -> inbound`

**Using the XML**

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

To Configure Outbound SMS

**Using Web Manager**

- To view and configure outbound SMS, click **SMS** in the menu and select **Outbound**

**Using the CLI**

- To enter the command level:  `enable -> configure -> sms -> outbound`

**Using the XML**

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

### Outbound SMS Settings | Description
--- | ---
Number | Enter the Recipient Number.
Encoding | Select the SMS encoding mode:
| ➤ ASCII 7-bit
| ➤ ASCII 8-bit
| ➤ UCS-2
Message | Enter the SMS message content.
| Note: Entering more than 70 characters in the SMS message may cause splitting of text messages.
Remaining Characters | Displays remaining characters.

Note: Entering more than 70 characters in the SMS message may cause splitting of text messages.
14: 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.
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 XC HSPA+ 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 XC HSPA+ intelligent gateway over an FTP connection. The destination file name on the PremierWave XC HSPA+ unit must have a "firmware.rom" type of format. The device will reboot upon successful completion of the firmware upgrade.

Example FTP session:

```bash
$ 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_xc_hspa_8_0_0_0R15
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.
```
15: Security Settings

The PremierWave XC HSPA+ 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 authentication methods on the PremierWave XC HSPA+ intelligent gateway make use of SSL. The PremierWave XC HSPA+ 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 XC HSPA+ intelligent gateway will use its own "personal" certificate. In verifying the authenticity of the other party, the PremierWave XC HSPA+ device will use a "trusted authority" certificate.

In short:

- When using EAP-TLS, the PremierWave XC HSPA+ intelligent gateway 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 XC HSPA+ 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 XC HSPA+ intelligent gateway 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 XC HSPA+ module.

Certificate Formats

Certificates and private keys can be stored in several file formats. Best known are PKCS12, DER and PEM. Certificate and key can be in the same file or in separate files. Additionally, the key can be either be encrypted with a password or left in the clear. However, PremierWave XC HSPA+ intelligent gateway 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.

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

To configure the PremierWave XC HSPA+ intelligent gateway 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 XC HSPA+ 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 15-1 SSH Server Host Keys

<table>
<thead>
<tr>
<th>SSH Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Key</td>
<td>Click <strong>Choose File</strong> to browse to and select the existing private key you want to upload. In Web Manager, you can also browse to the private key to be uploaded. Be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.</td>
</tr>
</tbody>
</table>
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 15-2 SSH Client Known Hosts

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

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

SSH Server Authorized Users

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

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

Note: When uploading the security keys, ensure the keys are not compromised in transit.
Table 15-3  SSH Server Authorized Users

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

**SSH Client Users**

The SSH Client Users are used by all applications that play the role of an SSH Client. Specifically Tunneling in Connect Mode. To configure the PremierWave XC HSPA+ intelligent gateway 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 15-4  SSH Client Users

<table>
<thead>
<tr>
<th>SSH Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter the name that the device uses to connect to an SSH server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password associated with the username.</td>
</tr>
<tr>
<td>Remote Command</td>
<td>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.</td>
</tr>
<tr>
<td>Private Key</td>
<td>Click Choose File to browse to and select the existing private key you want to upload. In Web Manager, you can also browse to the private key to be uploaded. Be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.</td>
</tr>
<tr>
<td>Public Key</td>
<td>Click Choose File to browse to and select the existing public key you want to upload. In Web Manager, you can also browse to the public key to be uploaded.</td>
</tr>
<tr>
<td>Key Type</td>
<td>Select a bit length for the key:</td>
</tr>
<tr>
<td></td>
<td>• RSA</td>
</tr>
<tr>
<td></td>
<td>• DSA</td>
</tr>
</tbody>
</table>
15: Security Settings

Table 15-5  Create New Keys

<table>
<thead>
<tr>
<th>SSH Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add/Edit (button)</td>
<td>Click the Add/Edit button after completing the Username, Password, and Remote Command fields above, and selecting the key and key type.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SSH Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter the name that the device uses to connect to an SSH server.</td>
</tr>
<tr>
<td>Key Type</td>
<td>Select a bit length for the key:</td>
</tr>
<tr>
<td></td>
<td>• RSA</td>
</tr>
<tr>
<td></td>
<td>• DSA</td>
</tr>
<tr>
<td>Bit Size</td>
<td>Select the bit length of the new key:</td>
</tr>
<tr>
<td></td>
<td>• 512</td>
</tr>
<tr>
<td></td>
<td>• 768</td>
</tr>
<tr>
<td></td>
<td>• 1024</td>
</tr>
<tr>
<td></td>
<td>Using a larger Bit Size takes more time to generate the key. Approximate times are:</td>
</tr>
<tr>
<td></td>
<td>• 1 second for a 512 bit RSA key</td>
</tr>
<tr>
<td></td>
<td>• 1 second for a 768 bit RSA key</td>
</tr>
<tr>
<td></td>
<td>• 1 second for a 1024 bit RSA key</td>
</tr>
<tr>
<td></td>
<td>• 2 seconds for a 512 bit DSA key</td>
</tr>
<tr>
<td></td>
<td>• 2 seconds for a 768 bit DSA key</td>
</tr>
<tr>
<td></td>
<td>• 20 seconds for a 1024 bit DSA key</td>
</tr>
<tr>
<td></td>
<td>Note: Some SSH clients require RSA host keys to be at least 1024 bits long. This device generates keys up to 2048 bits long.</td>
</tr>
<tr>
<td>Submit (key)</td>
<td>Click the Submit button after entering the information for the new key.</td>
</tr>
</tbody>
</table>

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="state">`
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.

Create a New Credential

After creating a new credential, you can either establish your credential through Certificate and Key Generation or Upload Certificate.

Table 15-6  Create a New Credentials

<table>
<thead>
<tr>
<th>Upload Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create new credential</td>
<td>Enter the name of the new credential to be created.</td>
</tr>
<tr>
<td>Submit (key)</td>
<td>Click the Submit button after entering the new credential name.</td>
</tr>
</tbody>
</table>

To Create a New Credential

Using Web Manager

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

Using the CLI

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

Using XML

- Not applicable.
Upload Certificate

SSL certificates identify the PremierWave XC HSPA+ intelligent gateway to peers. Certificate and key pairs can be uploaded to the PremierWave XC HSPA+ unit through either the CLI or XML import mechanisms. Certificates can be identified on the PremierWave XC HSPA+ intelligent gateway by a name provided at upload time.

Table 15-7  Upload Certificate Settings

<table>
<thead>
<tr>
<th>Upload Certificate Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New Certificate</strong></td>
<td>Click Choose File to browse to and select the new certificate file to be uploaded. The SSL certificate to be uploaded. RSA or DSA certificates are allowed. The format of the certificate must be PEM. It must start with &quot;-----BEGIN CERTIFICATE-----&quot; and end with &quot;-----END CERTIFICATE-----&quot;. Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.</td>
</tr>
</tbody>
</table>
| **New Certificate Type**   | Choose the new certificate type to be uploaded:  
  - PEM  
  - PKCS7  
  - PKCS12 |
| **New Private Key**        | Click Choose File to browse to and select the certificate type being uploaded. The key needs to belong to the certificate entered above. The format of the file must be PEM. It must start with "-----BEGIN RSA PRIVATE KEY-----" and end with "-----END RSA PRIVATE KEY-----". Read DSA instead of RSA in case of a DSA key. Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload. |
| **New Key Type**           | Click Choose File to browse to and select the key type being uploaded:  
  - PEM  
  - Encrypted PEM  
  - PKCS12 |

Certificate and Key Generation

The PremierWave XC HSPA+ intelligent gateway 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 XC HSPA+ unit by a name provided at generation time.

Table 15-8  Certificate and Key Generation Settings

<table>
<thead>
<tr>
<th>Certificate Generation Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Country (2 Letter Code)</strong></td>
<td>Enter the 2-letter country code to be assigned to the new self-signed certificate. Examples: US for United States and CA for Canada</td>
</tr>
<tr>
<td><strong>State/Province</strong></td>
<td>Enter the state or province to be assigned to the new self-signed certificate.</td>
</tr>
<tr>
<td><strong>Locality (City)</strong></td>
<td>Enter the city or locality to be assigned to the new self-signed certificate.</td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>Enter the organization to be associated with the new self-signed certificate.</td>
</tr>
</tbody>
</table>
To Configure an Existing SSL Credential
Follow these steps after a new credential has been established via Create a New Credential on page 105.

Using Web Manager

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

Using the CLI

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

Using XML

- Include in your file:

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

One or more authority certificates are needed to verify a peer’s identity. These certificates do not require a private key.

Table 15-9 Trusted Authority Settings

<table>
<thead>
<tr>
<th>Trusted Authorities Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority</td>
<td>Click Choose File to browse to and select the SSL authority certificate. RSA or DSA certificates are allowed. The format of the authority certificate can be PEM or PKCS7. PEM files must start with “-----BEGIN CERTIFICATE-----” and end with “-----END CERTIFICATE-----”. Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.</td>
</tr>
<tr>
<td>Authority Certificate Type</td>
<td>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.</td>
</tr>
<tr>
<td>Delete</td>
<td>Click the Delete button beside a specific certificate authority to delete it.</td>
</tr>
<tr>
<td>Delete All</td>
<td>Click the Delete All button to delete all existing certificate authorities.</td>
</tr>
</tbody>
</table>

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:

```xml
<configgroup name="ssl">
    <configitem name="trusted authority" instance="#"/>
    <configitem name="intermediate authority" instance="#"/>
</configgroup>
```
16: Maintenance and Diagnostics Settings

Filesystem Settings

Use the file system to list, view, create, upload, copy, move, remove, and transfer files. The PremierWave XC HSPA+ intelligent gateway uses a flash file system to store files.

Statistics

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

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

When the USB drive is connected to one of the two USB ports on the device, it will be automatically mounted and accessed using the filesystem. USB drives can be simultaneously connected to both the USB ports. If the USB mount option is disabled, USB drive will not be mounted.

<table>
<thead>
<tr>
<th>Filesystem Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>Displays a list of files on the PremierWave XC HSPA+ device, and their respective sizes.</td>
</tr>
<tr>
<td>USB Auto Mount</td>
<td>Click to enable or disable USB auto mount.</td>
</tr>
</tbody>
</table>

Table 16-1 File Statistics

To View Statistics

**Using Web Manager**

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

File Display

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

<table>
<thead>
<tr>
<th>File Display Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ls</td>
<td>Displays a list of files on the PremierWave XC HSPA+ device, and their respective sizes.</td>
</tr>
<tr>
<td>cat</td>
<td>Displays the specified file in ASCII format.</td>
</tr>
<tr>
<td>dump</td>
<td>Displays the specified file in a combination of hexadecimal and ASCII formats.</td>
</tr>
<tr>
<td>pwd</td>
<td>Print working directory.</td>
</tr>
<tr>
<td>cd</td>
<td>Change directories.</td>
</tr>
<tr>
<td>show tree</td>
<td>Display file/directory tree.</td>
</tr>
</tbody>
</table>

Table 16-2 File Display Settings
To Display Files

**Using Web Manager**

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

**Using the CLI**

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

**Using XML**

- Not applicable.

File Modification

The PremierWave XC HSPA+ intelligent gateway allows for the creation and removal of files on the Filesystem.

<table>
<thead>
<tr>
<th>File Modification Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rm</td>
<td>Removes the specified file from the file system.</td>
</tr>
<tr>
<td>touch</td>
<td>Creates the specified file as an empty file.</td>
</tr>
<tr>
<td>cp</td>
<td>Creates a copy of a file.</td>
</tr>
<tr>
<td>mkdir</td>
<td>Creates a directory on the file system.</td>
</tr>
<tr>
<td>rmdir</td>
<td>Removes a directory from the file system.</td>
</tr>
<tr>
<td>format</td>
<td>Format the file system and remove all data.</td>
</tr>
</tbody>
</table>

File Transfer

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

<table>
<thead>
<tr>
<th>File Transfer Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>Type in a <strong>File</strong> or <strong>Directory</strong> name and click the <strong>Create</strong> button. The newly created File or Directory will appear above.</td>
</tr>
<tr>
<td>Upload File</td>
<td>Click <strong>Choose File</strong> to browse to location of the file to be uploaded via HTTP. Click <strong>Upload</strong> to upload the chosen file.</td>
</tr>
<tr>
<td>Copy File</td>
<td>Enter the <strong>Source</strong> and <strong>Destination</strong> name for file to be copied and click the <strong>Copy</strong> button.</td>
</tr>
<tr>
<td>Move</td>
<td>Enter the <strong>Source</strong> and <strong>Destination</strong> name for file to be moved and click the <strong>Move</strong> button.</td>
</tr>
</tbody>
</table>
To Transfer or Modify Filesystem Files

**Using Web Manager**

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

**Using the CLI**

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

**Using XML**

- Not applicable.

### Protocol Stack Settings

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

### IP Settings

**Table 16-5 IP Protocol Stack Settings**

<table>
<thead>
<tr>
<th>Protocol Stack Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Time to Live</td>
<td>This value typically fills the Time To Live in the IP header. SNMP refers to this value as &quot;ipDefaultTTL&quot;. Enter the number of hops to be transmitted before the packet is discarded.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Protocol Stack ICMP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Click to enable or disable the processing of ICMP messages. This includes both incoming and outgoing messages.</td>
</tr>
</tbody>
</table>

To Configure ICMP Protocol Stack Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

To View ICMP Protocol Stack Settings

Using Web Manager

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

- Not applicable.

Using XML

- Not applicable.

ARP Settings

Table 16-7 ARP Protocol Stack Settings

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

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 XC HSPA+ intelligent gateway 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 16-8 Ping Settings

<table>
<thead>
<tr>
<th>Diagnostics: Ping Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the IP address or host name for the PremierWave unit to ping.</td>
</tr>
<tr>
<td>Count</td>
<td>Enter the number of ping packets PremierWave device should attempt to send to the Host. The default is 5.</td>
</tr>
</tbody>
</table>
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 XC HSPA+ intelligent gateway 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 16-9 Traceroute Settings**

<table>
<thead>
<tr>
<th>Diagnostics: Traceroute Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>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.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the traceroute protocol from the drop-down menu.</td>
</tr>
<tr>
<td>Submit (button)</td>
<td>Click the <strong>Submit</strong> button after entering traceroute information.</td>
</tr>
</tbody>
</table>

To Perform a Traceroute

**Using Web Manager**

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

**Using the CLI**

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

**Using XML**

- Not applicable.
Log

### Table 16-10 Log Settings

<table>
<thead>
<tr>
<th>Diagnostics: Log</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Log Output**   | Select a diagnostic log output type:  
|                  | ✦ **Disable** - Turn off the logging feature.  
|                  | ✦ **Filesystem** - Directs logging to /log.txt.  
|                  | ✦ **Line (1 or 2)** - Directs logging to the selected serial line. |
| **Log Max Length** | Set the maximum length of the log.txt file in Kbytes.  
|                  | *Note: This setting becomes available when Filesystem is selected.* |
| **Log Verbosity Level** | Select the **Verbosity Level** from the drop-down menu to specify the verbosity of system messages logged to the Syslog Host. |
| **Log Cellular Modem IO** | Select to enable or disable the logging of commands and responses with the cellular modem. |
| **Save Cellular Network Traffic** | Select to enable or disable the saving of cellular network traffic to the filesystem.  
|                  | IF this option is enabled, the output goes to PPP-YYY-MM-DD_HH.MM.pcap.  
|                  | PPP-YYY-MM-DD_HH.MM is the time at which capture was started. |

### 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:

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

To View Process Information

Using Web Manager

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

Using the CLI

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

Using XML

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

Threads

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

To View Thread Information

Using Web Manager

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

Using the CLI

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

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

<table>
<thead>
<tr>
<th>Clock</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method</td>
<td>Select a clock change method from the drop-down menu:</td>
</tr>
<tr>
<td></td>
<td>✷ Manual: this option allows you to directly set the date and time.</td>
</tr>
<tr>
<td></td>
<td>✷ SNTP: this option keeps the time synchronized with the NTP Server.</td>
</tr>
<tr>
<td></td>
<td>✷ Cellular Network: this option allows the time to be synchronized with the cellular network.</td>
</tr>
<tr>
<td>Date</td>
<td>Use the drop-down menu to select the Year, Month and Day. This option becomes available when the Manual method is selected.</td>
</tr>
<tr>
<td>Time (24 hour)</td>
<td>Use the drop-down menu to select the Hour, Min and Sec. This option becomes available when the Manual method is selected.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>Set NTP Server to an NTP server’s IP address or hostname. This option becomes available when the SNTP method is selected.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Select the geographical time zone from the drop-down list.</td>
</tr>
</tbody>
</table>

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 XC HSPA+ intelligent gateway 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>
<thead>
<tr>
<th>Table 16-12 System Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Settings</strong></td>
</tr>
<tr>
<td>State</td>
</tr>
<tr>
<td>Current date and time</td>
</tr>
<tr>
<td>Schedule</td>
</tr>
<tr>
<td>Time (24 hour)</td>
</tr>
<tr>
<td>Interval</td>
</tr>
<tr>
<td>Reboot Device</td>
</tr>
<tr>
<td>Restore Factory Defaults</td>
</tr>
<tr>
<td>Upload New Firmware</td>
</tr>
<tr>
<td>Short Name</td>
</tr>
<tr>
<td>Long Name</td>
</tr>
<tr>
<td>Submit (button)</td>
</tr>
</tbody>
</table>

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">`
17: 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 XC HSPA+ intelligent gateway. It is possible to configure access via the Telnet and SSH protocols, in addition to general CLI options.

Basic CLI Settings

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

<table>
<thead>
<tr>
<th>Table 17-1 CLI Configuration Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command Line Interface Configuration Settings</strong></td>
</tr>
<tr>
<td>Login Password</td>
</tr>
<tr>
<td>Enable Level Password</td>
</tr>
<tr>
<td>Quit Connect Line</td>
</tr>
<tr>
<td>Inactivity Timeout</td>
</tr>
<tr>
<td>Line Authentication</td>
</tr>
</tbody>
</table>

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 XC HSPA+ intelligent gateway telnet over the Telnet protocol.

Table 17-2 Telnet Settings

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

To Configure Telnet CLI Settings

Using Web Manager

♦ To configure Telnet settings, click CLI in the menu and select Configuration.

Using the CLI

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

Using XML

♦ Include in your file:

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

SSH CLI Settings

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

Table 17-3 SSH Settings

<table>
<thead>
<tr>
<th>SSH Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH State</td>
<td>Select to enable or disable CLI access via SSH.</td>
</tr>
<tr>
<td>SSH Port</td>
<td>Specify the SSH Port and override the default, as needed. Blank the field to restore the default.</td>
</tr>
<tr>
<td>SSH Max Sessions</td>
<td>Specify the maximum number of concurrent SSH sessions that will be allowed.</td>
</tr>
</tbody>
</table>
To Configure SSH Settings

Using Web Manager

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

Using the CLI

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

Using XML

- Include in your file:
  
  ```
  <configgroup name="ssh"> and <configitem name="state">
  ```

XML Settings

The PremierWave XC HSPA+ intelligent gateway allows for the configuration of units using an XML configuration record (XCR). Export a current configuration for use on other PremierWave XC HSPA+ unit or import a saved configuration file.

XML: Export Configuration

You can export the current system configuration in XML format. The generated XML file can be imported later to restore a configuration. It can also be modified and imported to update the configuration on this PremierWave XC HSPA+ 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>
<thead>
<tr>
<th>XML Export Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export to browser</td>
<td>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.</td>
</tr>
<tr>
<td>Export to local file</td>
<td>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.</td>
</tr>
<tr>
<td>Export secrets</td>
<td>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.</td>
</tr>
<tr>
<td>Comments</td>
<td>Select this option to include descriptive comments in the XML.</td>
</tr>
<tr>
<td>Lines to Export</td>
<td>Select instances to be exported in the line, serial, tunnel and terminal groups. Click Clear All to clear all checkmarks, or Select All to check all checkmarks.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Table 17-5 Exporting Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>XML Export Status Settings</strong></td>
</tr>
<tr>
<td>Export to browser</td>
</tr>
<tr>
<td>Export to local file</td>
</tr>
<tr>
<td>Lines to Export</td>
</tr>
<tr>
<td>Groups to Export</td>
</tr>
<tr>
<td>Export (button)</td>
</tr>
</tbody>
</table>

To Export in XML Format

Using Web Manager

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

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

Using XML

- Not applicable.

XML: Import Configuration

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

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

Configuration from External File

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

Configuration from Filesystem

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

Line(s) from single line Settings on the Filesystem

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

<table>
<thead>
<tr>
<th>Table 17-6 Import Configuration from Filesystem Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Import Configuration from Filesystem Settings</strong></td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Filename</strong></td>
</tr>
<tr>
<td><strong>Lines to Import</strong></td>
</tr>
<tr>
<td><strong>Whole Groups to Import</strong></td>
</tr>
<tr>
<td><strong>Export (button)</strong></td>
</tr>
</tbody>
</table>
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.
18: Branding the PremierWave XC HSPA+ Device

This chapter describes how to brand your PremierWave XC HSPA+ intelligent gateway by using Web Manager and Command Line Interface (CLI). It contains the following sections on customization:

- Web Manager Customization
- Short and Long Name Customization

Web Manager Customization

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

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

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

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

1. FTP to the PremierWave XC HSPA+ 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).
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 PremierWave_logo.gif and PremierWave.png.
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 XC HSPA+ intelligent gateway. The names display in the CLI show command and in the System web page in the Current Configuration table. The short name is used for the show command. Both names display in the CLI Product Type field.

Note: See System Settings (on page 119) for additional configuration options available on the Systems page.

<table>
<thead>
<tr>
<th>Name Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Name</td>
<td>Enter a short name for the system name. A maximum of 32 characters are allowed.</td>
</tr>
<tr>
<td>Long Name</td>
<td>Enter a long name for the system name. A maximum of 64 characters are allowed.</td>
</tr>
</tbody>
</table>

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:
  ```xml
  <configitem name="short name"/>
  and
  <configitem name="long name"/>
  ```
Appendix A: Technical Specifications

Network

Cellular
- UMTS/HSPA+ (850/800/900/1900/2100 MHz)
- GSM/GPRS/EDGE (850/900/1800/1900 MHz)
- Transfer Rates - up to 14.4 Mbps (downlink), up to 7.2Mbps (uplink)
- SMS Inbound - Shoulder Tap, Relay Control, Tunneling*
- SMS Outbound - Event Notification, Tunneling*
- 1 Secure SIM Slot
- 2 x Omni-Directional Penta-band Antennas

Ethernet
- 10BaseT and 100Base-TX Link (auto sensing – MDIX, full and half duplex support)
- RJ-45 Connector with LEDs (operation and link)
- 1.5 KV Isolation

Serial Interface
- Software selectable RS-232/422/485
- Software selectable RS-485 termination
- Serial data rates from 300 to 921 Kbps
- Characters: 7 or 8 data bits
- Parity: Odd, Even, None
- Stop Bits: 1 or 2
- Modem Control: DTR, DSR/DCD
- Flow Control: XON/XOFF (SW), CTS/RTS (HW)

Serial Connector
- 2 x DB9M (DTE) with 15KV ESD protection per port

USB Interface
- USB Mass Storage Device Support
Appendix A: Technical Specifications

USB Connector
- 1 x USB Type A Host Connector (USB 2.0)

I/O Interface

Input
- Connection: Sensors/Events
- Voltage acceptance: 0 to 30 VDC
- Digital input event: User configurable
- Optical: 1.5 KV

Output
- Software: Turn Relay Output ON and OFF
- Automatic Event Trigger: ON or OFF (possible events include loss of cellular link, loss of Ethernet link, digital input event)
- Relay Output Response: User configurable
- Support 1A @24V

I/O Connectors
- 2 x Digital Input, 1 x Relay Output (Terminal Block)

LED Indicators
- Cellular Mode, Signal Strength, Serial RX/TX, USB Connection, System Status, Power, Ethernet Speed, Ethernet Activity

Routing/Gateway
- NAT, Port Forwarding, SPI Firewall
- WAN Failover/Failback
- Multiple Ethernet LAN Hosts
- Multihoming
Protocol Support

- Network Services: SMTP Client, RSS, Telnet Server/Client, SNTP, FTP Server/Client, SFTP Server/Client, TFTP Server, Syslog
- Network Management: SNMP v1/v2c/v3*
- Network Security: HTTPS Server/Client, SSH Server/Client, SSL Server/Client, TLS, IPSec*
- Network Protocols: ARP, HTTP, UDP/IP, TCP/IP, ICMP, BOOTP, DHCP, Auto IP, DNS
- Discovery Protocols: UPnP
- Industrial Protocols*: Modbus TCP, Modbus RTU, Modbus ASCII

Event Triggers and Actions

- Events: Cellular Link State Change, Ethernet Link State Change, Digital Input State Change
- Actions: SMS, Email, HTTP Post, FTP Put, Relay Output, SNMP, Trap

Security

- SSL v3, SSH v2, Client & Server, Supports up to 2048-bit certificates
- Encryption: AES, 3DES, RC4
- Authentication: SHA-1, MDS, Base-64 User Access Lists

Management

- Web Browser (SSL option for secure login)
- CLI (over Serial Ports, Telnet or SSH)
- XML Configuration Records via CLI or FTP
- Supports SNMP

Software

- Lantronix Device Server Application Suite
- DeviceInstaller
Appendix A: Technical Specifications

Power
- Input Voltage: 9-30 VDC
- Power Consumption: 3.6 Watts (typical)
- Power Supply (100 - 240 VAC, 50-60 Hz, 12 VDC @ 1.8A) with locking barrel connector and regional adapters, -40° to +75°C

Environmental
- Operating Temperature: -40° to +70°C
- Storage Temperature: -40° to +85°C
- Relative Humidity: 5% to 95% non-condensing
- IP Rating: 30

Dimensions
- Size: (L x W x H): 109 mm x 109 mm x 30 mm (4.3 in x 4.3 in x 1.2 in)
- Weight: 0.24 kg (0.55 lb)
Appendix B: Compliance

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

Manufacturer's Name & Address:
Lantronix, Inc.
7535 Irvine Center Drive, Suite 100, Irvine, CA 92618 USA

Product Name Model:
PremierWave XC HSPA+ Intelligent Gateway This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Note: Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

This radio transmitter (PremierWave XC HSPA+, 3867A-PWXCHSPA) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Approved Antenna. Taoglas, TG.09.113, Hinged Monopole, 2.8dBi peak gain.

Note: En vertu de la réglementation d' Industrie Canada, cet émetteur de radio ne peut fonctionner à l'aide d'une antenne d'un type et un maximum (ou moins) gain approuvé pour l'émetteur par Industrie Canada. Pour réduire risque d'interférence aux autres utilisateurs, le type d'antenne et son gain doivent être choisis afin que la puissance isotope rayonnée équivalente (PIRE) ne dépasse pas ce qui est nécessaire pour une communication réussie.

Cet émetteur radio (PremierWave XC HSPA+, 3867A-PWXCHSPA) a été approuvé par Industrie Canada pour fonctionner avec les types d'antennes énumérés ci-dessous avec le gain maximal admissible et impédance d'antenne requise pour chaque type d'antenne indiqué. Types d'antennes pas inclus dans cette liste, ayant un gain supérieur au gain maximal indiqué pour ce type, sont strictement interdits pour une utilisation avec cet appareil.

Approuvé antenne. Taoglas, TG.09.113, Monopole charnière, un gain maximal 2.8dBi
Conforms to the following standards or other normative documents:

**Safety**
- Low Voltage Directive (2006/95/EC)
- IEC 60950-1:2005/A1:2010
- EN 60950-1:+A11+A1+A12:2011
- CSA C22.2 No. 60950-1-03, 1st Edition, 2006-07
- EN 62311 (2008)

**Emissions and Immunity**

**US**
- FCC 22H (2013)
- FCC 24E (2013)
- FCC 15.107 (2013) Class B

**Canada**
- RSS-132 (2013)
- RSS-133 (2013)
- RSS-210 (2010)

**Europe**
- R&TTE Directive 1999/5/EC
- EN 301 908-1 V5.2.1 (2011)
- EN 301 908-2 V5.2.1 (2011)
- EN 301 511 V9.0.2 (2003)
- EN 301 489-1 V1.9.2 (2011)
- EN 301 489-7 V1.3.1 (2005)
- EN 301 489-24 V1.5.1 (2010)
- EN 55022 (2010) Class B
- EN 55024

**Transmitter Certification IDs**
- FCC: R68PWXCHSPA
- IC: 3867A-PWXCHSPA

**Carrier Certifications**
- PTCRB
- AT&T
Manufacturer's Contact:
Lantronix, Inc.
7535 Irvine Center Drive, Suite 100
Irvine, CA 92618 USA
Tel: 949-453-3990
Fax: 949-453-3995

RoHS, REACH and WEEE Compliance Statement
Appendix C: Lantronix Technical Support

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

To contact technical support or sales, look up your local office at http://www.lantronix.com/about/techsupport/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 D: 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.
4. Click **Hex**. The hexadecimal value appears.