



Installation and Management Guide

Tsunami MP-8150-CPE

Installation and Management Guide



Copyright

© 2009 Proxim Wireless Corporation, Milpitas, CA. All rights reserved. Covered by one or more of the following U.S. patents: 5,231,634; 5,875,179; 6,006,090; 5,809,060; 6,075,812; 5,077,753. This manual and the software described herein are copyrighted with all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of Proxim Wireless Corporation.

Trademarks

Tsunami, Proxim, and the Proxim logo are trademarks of Proxim Wireless Corporation. All other trademarks mentioned herein are the property of their respective owners.

Disclaimer

Proxim reserves the right to revise this publication and to make changes in content from time to time without obligation on the part of Proxim to provide notification of such revision or change. Proxim may make improvements or changes in the product(s) described in this manual at any time. When using this device, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons.

GPL License Note

Tsunami MP-8150-CPE includes software code developed by third parties, including software code subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL"). Please see the GPL and LGPL Web sites to view the terms of each license.

To access the GPL Code and LGPL Code used in Tsunami MP-8150-CPE, visit the proxim website to get a copy of the source. The GPL Code and LGPL Code used in this device are distributed WITHOUT ANY WARRANTY and are subject to the copyrights of one or more authors. For details, see the GPL Code and LGPL Code of this device and the terms of the GPL and LGPL.

IMPORTANT!

Proxim recommends you to visit the Proxim Support site at <http://support.proxim.com> for Regulatory Information and latest product updates.

Contents

Preface	8
1 Overview	10
Introduction	11
Wireless Network Topology (Point-to-Multipoint Link)	11
Multiple-Input-Multiple-Output (MIMO)	12
Management and Monitoring Capabilities	13
Web Interface	13
Command Line Interface	13
SNMP Management	13
2 Installation and Initialization	15
Hardware Overview	16
GigE Power-over-Ethernet	16
Serial Connection	17
Product Package	17
Installation Procedure	18
Initialization	26
ScanTool	26
Setting the IP Address with ScanTool	26
Modifying the IP Address	27
Logging in to the Web Interface	29
System Summary	29
COMMIT Button	30
REBOOT Button	31
Factory Default Configuration	32
3 Basic Configuration	33
Country and Related Settings	34
Dynamic Frequency Selection (DFS)	34
Transmit Power Control	34
Setting Up a Link Between BSU and SU	35
Virtual Local Area Networks (VLANs)	35
Basic Configuration Information	35
4 Advanced Configuration	40
System Configuration	40
Network Configuration	41
Configuring IP in Bridge or Router Mode	41

Ethernet Properties Configuration	43
Wireless Configuration	45
Configuring WORP Properties in SU Mode	45
Wireless Interface Properties	48
Blacklist Information	52
Sensitivity Threshold Values	53
MIMO Properties	53
Security Configuration	55
Setting Up Wireless Security	55
VLAN Configuration (Bridge Mode only)	59
Establishing a VLAN Connection	60
VLAN Modes	61
Filtering Configuration (Bridge Only)	64
Ethernet Protocol Filter	65
Static MAC Address Filter	68
Advanced Filter	71
TCP/UDP Port Filter	73
DHCP Configuration	75
DHCP server	76
DHCP Relay (Routing Mode only)	79
Routing Features Configuration	80
Static Route Table (Routing Mode Only)	80
NAT (SU, Routing Mode Only)	82
RIP (Routing Mode Only)	85
5 System Management	88
System	89
System Information	89
Identifying the Components (Inventory Management)	90
Viewing Licensed Features	91
File Management	92
Upgrade Firmware via HTTP	92
Upgrade Configuration via HTTP	93
Upgrade Firmware via TFTP	93
Upgrade Configuration via TFTP	94
Retrieve From Device	95
Services: Configuring the Passwords	96
HTTP/HTTPS	97
Telnet/SSH	98
SNMP	99
System Log Host Table	101

SNTP	103
Access Control	104
Reset to Factory	105
6 Monitoring the System.....	106
Interface Statistics	107
Ethernet Statistics	107
Wireless Statistics	108
WORP Statistics	111
General Statistics	111
BSU Statistics	112
Bridge	113
Bridge Statistics	113
Learn Table	114
Network Layer	115
Routing Table	115
IP ARP	116
ICMP Statistics	116
RIP Database	118
DHCP	118
Logs	119
Event Log	119
Syslog	121
Tools	121
Link Test	121
WORP Site Survey	123
SNMP v3 Statistics	123
7 Procedures.....	124
TFTP Server Setup	125
Web Interface Firmware Download	125
Through TFTP	125
Through HTTP	125
Configuration Backup	126
Through TFTP	126
Through HTTP	126
Configuration Restore	126
Through TFTP	126
Through HTTP	126
Soft Reset to Factory Default	127
Hard Reset to Factory Default	127

Forced Reload	127
Upgrade a New Firmware Using ScanTool in Bootloader Mode	127
Preparing to Download the Firmware	128
Download a New Firmware Using CLI from Bootloader	129
Preparing to Download the Firmware	130
8 Troubleshooting	132
Gigabit Ethernet PoE	132
The Unit Does Not Work	132
There Is No Data Link	132
“Overload” Indications	132
Connectivity Issues	133
MP-8150-CPE Does Not Boot	133
Ethernet Link Does Not Work	133
Serial Link Does Not Work	133
Cannot Use the Web Interface	133
Communication Issues	134
Two Units Are Unable to Communicate Wirelessly	134
Surge and Lightning preventive maintenance	134
Setup and Configuration Issues	134
Lost Password	134
The MP-8150-CPE Responds Slowly	134
Device Has Incorrect IP Address	135
HTTP Interface Does Not Work	135
Telnet CLI Does Not Work	135
TFTP Server Does Not Work	135
Setting IP Address using Serial Port	136
TFTP Server	137
Recovery Procedures	138
Soft Reset to Factory Defaults	138
Hard Reset to Factory Defaults	138
Forced Reload	138
VLAN Operation Issues	139
Changes Do Not Take Effect	139
Link Problems	139
General Check	140
Statistics Check	140
Analyzing the Spectrum	140
A Frequency Domains and Channels	142
B Boot Loader CLI and ScanTool	146

C	Technical Specifications	148
D	Regulatory Compliance Information	157
E	Lightning Protection	160
F	Statement of Warranty	161
G	Technical Services and Support	163

Preface

About this Manual

Congratulations on your purchase of **Tsunami MP-8150-CPE**. This manual gives you a jump-start working knowledge on the MP-8150-CPE device that can help you build a wireless network backhaul application easily! It describes the device installation and its functions, the technology used, and the recommended methods for configuring and monitoring the device.

Audience

The intended audience for this manual are the Network Administrators who are installing and/or managing this device.

Prerequisites

The reader of this document should have working knowledge of Wireless Networks, Local Area Networking (LAN) concepts, network access infrastructures, and client-server applications.

Related Documents

All other documents are included in CD ROM in both printed (PDF) and online (HTML) formats.

Products Covered in this Guide

Product	Description
Tsunami MP-8150-CPE	Wireless Outdoor Tsunami Subscriber Unit with Integrated Antenna operating in 5 GHz Band.

Organization of this Manual

This manual documents installing and managing of Tsunami MP series. Before installing and using the unit, Proxim recommends you to read the following chapters of this manual:

- **Chapter 1 Overview:** Provides an overview of Tsunami MP-8150-CPE as well as wireless network topologies and combinations that can be built with the unit.
- **Chapter 2 Installation and Initialization:** Provides detailed installation instructions and explains how to access the device for configuration and maintenance.
- **Chapter 3 Basic Configuration:** Provides a high-level overview of system features, explains how to navigate the user interface, and discusses the most common settings for managing the unit.
- **Chapter 4 Advanced Configuration:** Explains the Web Interface's "Configure" options in a hierarchical manner, so you can easily find details about each item.
- **Chapter 5 System Management:** Explains the Web Interface's "Management" options in a hierarchical manner, so you can easily find details about each item to effectively manage the device.
- **Chapter 6 Monitoring the System:** Explains the Web Interface's "Monitor" options in a hierarchical manner, so you can easily find details about each item.
- **Chapter 7 Procedures:** Provides details about the various procedures involved in the operation of the MP-8150-CPE units using the Web interface.
- **Chapter 8 Troubleshooting:** Provides instructions and solutions to solve the issues you may encounter while installing and using the MP-8150-CPE units.

The appendixes contain supplementary information, including frequency domain tables, channel frequency, and Technical Support information.

If you are already familiar with this type of product, you can use the Quick Install Guide to install the unit.

Reference Manual

As a supplement to the *Tsunami MP-8150-CPE Installation and Management Guide*, the *Tsunami MP-8150-CPE Reference Manual* provides the following information:

- **Command Line Interface:** Documents the text-based configuration utility's keyboard commands and parameters.
- **MIB Browser for SNMP Interface:** Provides information and instructions on using the MIB Browser in Snmpv1-V2c and Snmpv3.
- **Event Log Error Messages:** Documents the error messages that you may see in the Event Log.
- **System Alarm Traps:** Documents the alarm traps that you can set for alarm notification.
- **Microsoft Windows IAS Radius Server Configuration:** Provides information to assist you in setting up the IAS Radius Server.
- **Glossary:** Describes terms used in the Tsunami MP-8150-CPE documentation and in the wireless industry.

Overview

This chapter provides a description of the Tsunami MP-8150-CPE system, its functionalities, and features.

It covers the following topics:

- [Introduction](#)
- [Wireless Network Topology \(Point-to-Multipoint Link\)](#)
- [Multiple-Input-Multiple-Output \(MIMO\)](#)
- [Management and Monitoring Capabilities](#)

1.1 Introduction

The Tsunami MP-8150-CPE is a flexible wireless outdoor client that lets you design solutions for point-to-point links and point-to-multipoint networks. It is the client or satellite side in a wireless link. The product's primary components are a wireless device and a Power-over-Ethernet injector. The device has an integrated antenna enclosed in a weatherproof container, which can be mounted to the side of a building, on a pole, or on a tower structure.

The MP-8150-CPE is part of the Tsunami MP-8100 product family, which is comprised of several additional products, including the MP-8100 Base Station (BSU) and the MP-8100 Subscriber Unit (SU) for outdoor installation.

Some of the key features of the product family are:

- MIMO & Advanced Orthogonal Frequency Division Multiplexing (OFDM) enhances non-line-of-sight performance improving deployment in challenging areas
- Highly optimized WORP (Wireless Outdoor Routing Protocol) for outdoor applications
- Designed for quick and easy installation
- Management through a Web Interface, a Command Line Interface (CLI), or Simple Network Management Protocol (SNMP)
- Software and configuration upgrade through file transfer (TFTP)
- VLAN support (configured on the Base Station)

1.2 Wireless Network Topology (Point-to-Multipoint Link)

A Point-to-Multipoint link is a specific type of multipoint link which consists of a Master Wireless Unit (BSU) that is connected to multiple slave wireless units (SUs). Any transmission of data that originates from the master is received by all peripheral slaves. But during any transmission of data originating from any of the slave is received only by the Master. This allows numerous sites in a wide area to share resources, including a single high-speed connection to the Internet.

You can set up a single Point-to-Multipoint network with a single BSU and multiple SUs, as depicted in the following figure. The MP-8150-CPE device can be configured only as an SU.

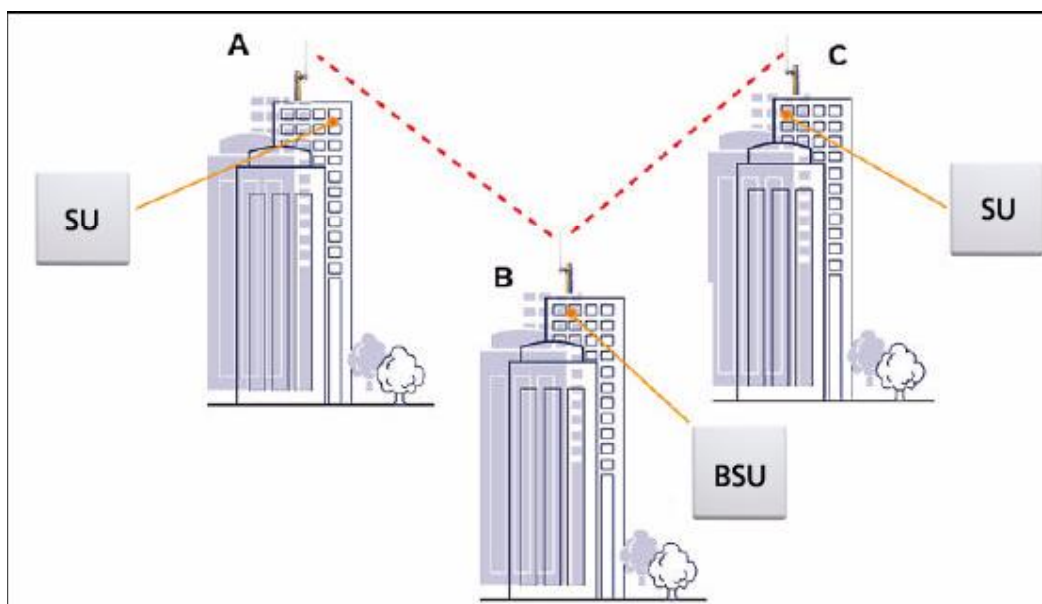


Figure 1-1 Wireless Network Topology (Point-to-Multipoint-Link)

A maximum of 250 SUs can be connected to a single BSU. Here, the BSU is equipped with either an omni-directional or a wide angle antenna, whereas the SUs are equipped with a directional antenna.

1.3 Multiple-Input-Multiple-Output (MIMO)

Multiple-Input-Multiple-Output (MIMO) is a smart antenna technology that offers tremendous performance gains for wireless devices at relatively low cost. The underlying technology of the MP-8150-CPE radios are based on a combination of MIMO and OFDM. High performance OFDM-MIMO radio combination enhances robustness using multiple transmitters and receivers, allowing the MP-8150-CPE units to completely take advantage of this antenna technology. In real-world environments, signals reflect from various objects to reach the receiving antenna, hence a signal follows different distances before being received. This phenomenon is called Multipath Propagation and causes interference and fading. On the receiver side, having multiple receivers increases the amount of received power and also reduces multipath problems by combining the received signals for each frequency component separately. Hence, MIMO significantly improves the overall gain.

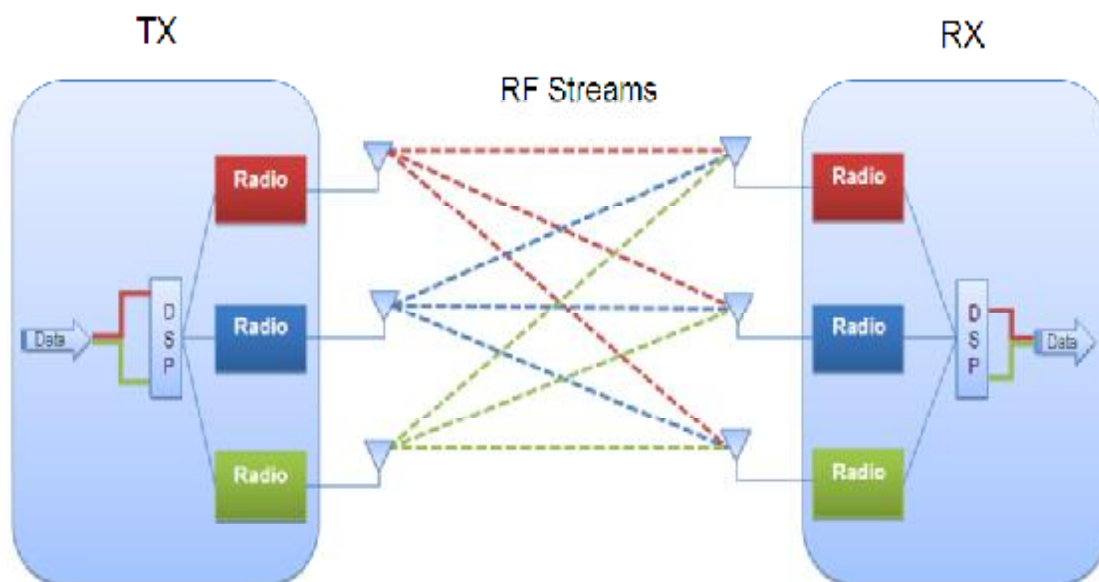


Figure 1-2 3x3 MIMO

The simplest spatially multiplexed MIMO system contains two transmit chains, two receive chains, and two data streams. When expanding such 2x2 architecture, several factors need to be considered. For example, at the device operating frequency of 2.4 GHz, the wavelength is 12 cm, the dimension of MP-8150-CPE is ~35cm, hence a 2x2-receive-chain system has sufficient antenna diversity to receive two uncorrelated signals. In a situation of not-so-perfect physical environment, a 3-receive-chain system has a much higher probability of getting two uncorrelated signals in the same environment as a 2x2 system. Also, when including the power consumption factor, 2x3 (2 transmit x 3 receive) combination MIMO works well for devices which operate on lower power consumption budgets.

A 2x2 MIMO offers better antenna gain (3 to 6dB) over a similar form factor as a 3x3. A 2x2 improves range in good conditions and is best suited for both Non-Line-of-Sight and Line-of-Sight. A 3x3 MIMO creates signal redundancy by spreading the two data streams over three RF flows. Multiple data streams across multiple RF flows improve throughput performance in difficult RF conditions and is ideal for Non-Line-of-Sight.

Theoretically, the performance of a MIMO system should improve with more transmitters and receivers. But it has been observed that the increase in performance beyond the 3x3 configuration is not substantial enough to justify the circuit complexity.

1.4 Management and Monitoring Capabilities

The network administrators can use the following management and monitoring interfaces to configure and manage the Tsunami MP-8150-CPE unit:

- Web Interface
- Command Line Interface
- SNMP Management

1.4.1 Web Interface

The Web interface (HTTP) provides easy access to configuration settings and network statistics from any computer on the network. You can access the Web interface over your network, over the Internet, or with an Ethernet cable connected directly to your computer's Ethernet port. See [Logging in to the Web Interface](#) for more information.

1.4.2 Command Line Interface

The Command Line Interface (CLI) is a text-based configuration utility that supports a set of keyboard commands and parameters to configure and manage the MP-8150-CPE devices. You can enter command statements composed of CLI commands and their associated parameters. You can enter commands from the keyboard for real-time control or from scripts that automate configuration. See the *Tsunami MP-8150-CPE Reference Manual* for more information about the Command Line Interface.

1.4.3 SNMP Management

In addition to the Web interface and the CLI, you also can use Simple Network Management Protocol (SNMP) to manage and configure the MP-8150-CPE devices. Note that this requires an SNMP manager program (sometimes called MIB browser) or a Network Manager program using SNMP. Proxim recommends NuDesign MIB Browser Pro 8.2 or iReasoning MIB browser for managing MP-8150-CPE devices. The devices support several Management Information Base (MIB) files that describe the parameters that can be viewed and configured using SNMP:

1. PXM-SNMP.mib (Enterprise MIB)
2. RFC-1213.mib (MIB-II)
3. RFC-1215.mib (Trap MIB)
4. RFC-2790.mib (HOST-RESOURCES-MIB)
5. RFC-2571.mib (SNMP-FRAMEWORK-MIB)
6. RFC-3412.mib (SNMP-MPD-MIB)
7. RFC-3414.mib (SNMP-USER-BASED-SM-MIB)

Download these MIB files from the Proxim website. You must compile one or more of these MIB files into your SNMP program's database before you manage your device using SNMP. See the documentation that came with your SNMP manager for instructions about how to compile MIBs.

NOTE: *When you update the software in the device, you must also update the MIBs to the same release. Because the parameters in the MIB may have changed, you will not otherwise have full control over the features in the new release.*

The enterprise MIB (PXM-SNMP.mib) defines the **Read and Read/Write** objects you can view or configure using SNMP. These objects correspond to most of the settings and statistics that are available with other management interfaces. See the enterprise MIB for more information. The MIB can be opened with any text editor, such as Microsoft Word, Notepad, and WordPad. See SNMP Parameters in the [Services: Configuring the Passwords](#) section.

IMPORTANT!

Using a serial connection, you can access the CLI of the device through a terminal emulation program, such as HyperTerminal. (See "HyperTerminal Connection Properties" in the *Tsunami MP-8150-CPE Reference Manual*.)

For all other modes of connection, you will need the IP address of the device to use the Web Interface, SNMP, or the CLI via telnet.

CAUTION!

For Regulatory Information and latest product updates, including firmware and the MIBs, Proxim recommends visiting the Proxim Support site at <http://support.proxim.com>.

IMPORTANT!

This user guide discusses installing the device and managing it using the Web interface only. For information on managing the device via the CLI, see the *Tsunami MP-8150-CPE Reference Manual*.

Installation and Initialization

This chapter describes the steps required to install and mount the MP-8150-CPE Series units, and to align the antenna. If you are already familiar with this type of product, refer to the *Tsunami MP-8150-CPE Quick Installation Guide* for streamlined installation procedures.

This chapter covers the following topics:

- [Hardware Overview](#)
- [Serial Connection](#)
- [Installation Procedure](#)
- [Initialization](#)
 - [ScanTool](#)
 - [Setting the IP Address with ScanTool](#)
- [Logging in to the Web Interface](#)
- [Factory Default Configuration](#)

2.1 Hardware Overview

The MP-8150-CPE is a full-featured outdoor Subscriber Unit (SU) that contains an integrated, dual polarized antenna and is fully compatible with Tsunami MP.11 Model 5054, 5054-R, and 5054-R-LR Base Station Units (BSUs) and Tsunami MP-8100 Base station Units.

The unit is designed to be mounted to a 1" - 1.5" diameter pole (not included). An optional universal pole mounting kit is also available from Proxim (P/N 1087-UMK); this kit is designed to mount directly to a flat surface such as a roof, wall, or under an eave.

The MP-8150-CPE is powered through Power-over-Ethernet via an 802.3af-compliant PoE injector such as the Proxim 1-Port Power Injector (see Power-over-Ethernet), and is equipped with the following connectors, indicators, and controls:

- Ethernet port
- RS-232 serial port
- LEDs: Ethernet, wireless, power
- Reset button: Reboots the hardware and software
- Reload button: Resets the unit to factory defaults

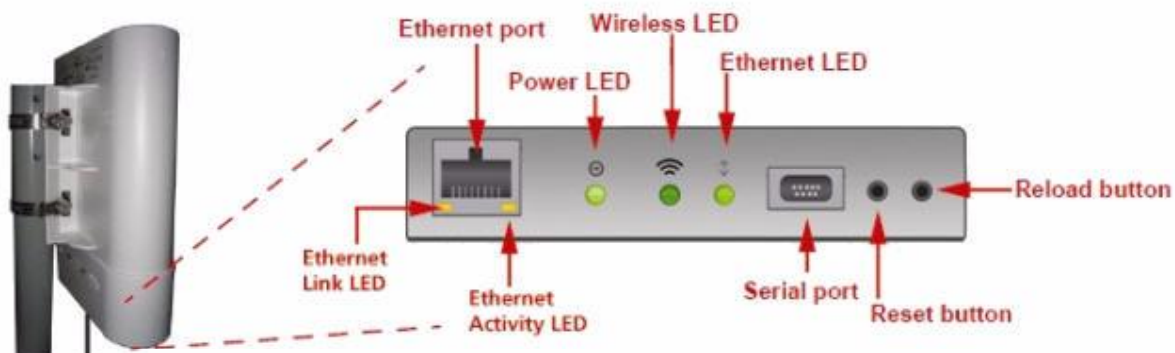


Figure 2-1 MP-8150-CPE Hardware

2.1.1 GigE Power-over-Ethernet

The unit has a built-in PoE module, which provides power and wired connectivity to the unit over a single Ethernet Port. It is always recommended to use the supplied Power Injector. The PoE integrated module provides 48 VDC over a standard Cat5e/Cat6 Ethernet cable.

Recommended Cable	
Function	Power (DC) and Ethernet connection
Type	Cat5e/Cat6, UV-shielded and outdoor-rated
Impedance	100 ohms
Recommended cables	STP, 24 AWG, UL rated
Maximum Distance	330 feet / 100 meters
Connector type, device end	Shielded RJ45 female, weatherized using weatherproof connector
Connector type, power & Ethernet adapter end	Shielded RJ45

2.1.2 Serial Connection

The serial connection is made with a straight-through RS232 cable (DB9 connectors). Connect one end of the cable to the unit and the other end to your PC to align antenna and to enter CLI commands.

2.2 Product Package

The product's shipping boxes should be left intact and sheltered until arrival at the installation site. Carefully unpack the MP-8150-CPE series shipment and check for any shipping damage or missing parts.

Each shipment includes the items listed in the following table. Verify that you have received all parts of the shipment.

NOTE: Cables are not supplied with the unit

MP-8150-CPE Unit	
Power Injector (PoE)	
Band Clamps (2)	
Installation CD and Quick Installation Guide	

2.3 Installation Procedure

This section describes the procedures to install and mount the unit and to align the antenna. The installation procedure does not include information on the mounting and connection of external antennas.

IMPORTANT

This device must be installed by a trained professional, value added reseller, or systems integrator who is familiar with RF planning issues and the regulatory limits.

CAUTION!

Pay attention to all the WARNINGS. Follow all the instructions. Only use attachments/accessories specified by the manufacturer.

CAUTION!

There are no user-serviceable parts inside. All services must be performed by qualified personnel.

CAUTION!

For Regulatory Information and latest product updates, including firmware and the MIBs, Proxim recommends visiting the Proxim Support site at <http://support.proxim.com>.

NOTE:

- The **Advanced Configuration** window provides a selectable **Frequency Domain** field that automatically provides the allowed channel bandwidth and frequencies for the selected frequency Domain/Country as well as, where applicable, Dynamic Frequency Selection (DFS) and Transmit Power Control.
- Non-US installers should not add an antenna system until the **Frequency Domain** is selected, the unit is rebooted, and the proper power level is configured. The output power level of the final channel selected by DFS scan can be found in the Event Log.
- Be sure to read the **Release Notes** file on the product CD as it contains software version and driver information.
- Equipment is to be used with, and powered by, the power injector provided with the product package or by a power injector that meets the following requirements:
 - UL-Listed/ITE (NWGQ)
 - Limited Power Source Output per UL/IEC 60950
 - CE-marked
 - Approved for Power-over-Ethernet
 - Rated output, 48 VDC/0.5 A
 - Pinout follows 802.3af standard for mid-span devices

See the following steps for installation instructions:

Step 1: Plan for Installation

There are several planning factors to be considered before installing the MP-8150-CPE system. In addition to selecting the installation site, you should do the following:

Calculate:

- Required RSL and fade margin to achieve availability objectives
- Required path availability
- Anticipated Multi-Path Reflection Points

Determine:

- System Frequency Plan
- Required Antenna Mounting Height to obtain proper Path Clearance
- Required Transmission Line Types and Lengths

Plan for:

- Device's continuous power consumption needs
- Lightning protection and system grounding
- Hardware mounting
- Cable installation including egress
- Pre-testing equipment (back-to-back test procedure)

Step 2: Choose a Location

To make optimal use of the device, you must find a suitable location to install the hardware. The range of the radio device largely depends upon the position of the antenna. Proxim recommends you do a site survey, observing the following requirements, before mounting the hardware.

- The location must allow easy disconnection of power to the radio if necessary.
- Ensure free flow of air around the hardware.
- The radio device must be kept away from vibration and excessive heat.
- The installation must conform to local regulations at all times.

The units are designed to directly mount to a pole. Using the supplied brackets and hardware, you can mount them to a 1.25 inch to 3-inch pole (outside diameter). Longer bolts (not supplied) are required for mounting the units to a larger diameter pole. Using just one of the pole mounting brackets, you can mount the units to a wall or other flat surface.

Step 3: Gather Required Tools

You should have the following tools available before installing the MP-8150-CPE units:

- Phillips (cross-tip) screwdrivers
- Small blade standard screwdriver
- Large blade standard screwdriver
- Wire crimpers (if using connectors that are not pre-made)
- Adjustable 6" wrench
- Weatherproofing material for sealing external connectors (such as butyl tape)
- Straight-through UV-protected STP-rated Cat5e/Cat6 Ethernet cable for connecting to PC, or cable for connecting to a hub or a switch.

NOTE: The total length of cabling between the PC and the MP units cannot exceed 100 meters, which includes both the cable from the PC to the power injector and the cable from the power injector to the MP unit. Due to DC power requirements, the maximum cable length between the power injector and the MP units is 75 meters.

Step 4: Unpack the Product Package

1. Unpack the device and accessories from the shipping box.
2. Note the Ethernet and MAC addresses of the unit as well as the serial number. These addresses may be used when configuring the unit.

NOTE: The serial number is required to obtain support from Proxim. Keep this information in a safe place.

Step 5: Attach Cables

NOTE: Depending on your application and location, you may find it easier to mount the unit before you attach cables to it. If this is the case, remove the cable cover (as explained in step 1 below), and then complete Step 4: Mount Unit to Pole. Return to this step for cabling instructions.

1. With the laying unit face down, depress both buttons on the back of the MP-8150-CPE unit, and pull the plastic cover downward to open. Remove cover.



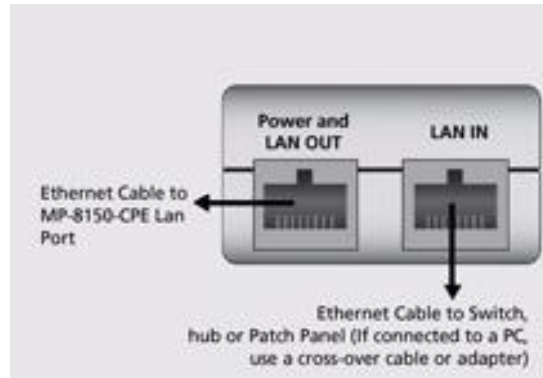
2. Connect one end of an Ethernet cable (5.5 mm/.217 in OD maximum; not supplied) to the unit's LAN port.
3. Route the Ethernet cable as shown below.



4. Connect the other end of the Ethernet cable to the **Data and Power Out** port of the DC Injector.

NOTE: You must use an 802.3af-compliant power injector, such as the Proxim Power over Ethernet Injector (P/N 76346).
5. Connect one end of a second Ethernet cable (not supplied) to the **Data In** port of the DC Injector and the other end to a switch, hub, patch panel, or single computer:

- Use a straight-through Ethernet cable if you are connecting the unit to a switch, hub, or patch panel.
- Use a cross-over Ethernet cable or adapter if you are connecting the unit to a single computer or most router ports.



Step 4: Mount Unit to Pole

Mount the MP-8150-CPE to a pole as follows:

1. Using a screwdriver, turn the screw on the band clamp counter-clockwise until the clamp opens.

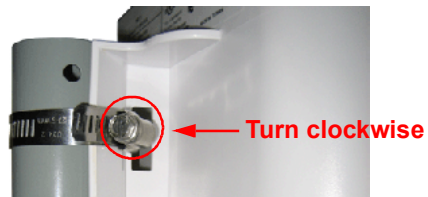


2. Place the back of the MP-8150-CPE against the pole such that the pole fits into the curved portion of the unit.



3. With the MP-8150-CPE aimed in the direction of the BSU, slide the flat end of the band clamp around the pole and through the top opening in the MP-8150-CPE unit, threading the flat end of the band clamp into the metal catch at the other end.
4. Using a 5/16" nutdriver or a screwdriver, turn the screw on the band clamp clockwise until it is tight enough to hold the unit in place

NOTE: Do not fully tighten band clamps; you must first ensure a functional link to the BSU ([Step 5: View LEDs/Adjust Mounting](#)).



5. Repeat procedure to attach other band clamp through bottom opening in the MP-8150-CPE unit.

NOTE: Do not fully tighten band clamps; you must first ensure a functional link to the BSU (Step 5: View LEDs/Adjust Mounting).

The mounted unit, using the optional Proxim universal pole mounting kit (P/N 1087-UMK), is shown below.



Step 5: View LEDs/Adjust Mounting

LEDs are located in the cable compartment.



When the unit is powered on, the MP-8150-CPE performs startup diagnostics. When startup is completed, the LEDs show the operational state of the MP-8150-CPE.

The following table shows the status of the LEDs when the MP-8150-CPE is operational.

Status	Ethernet Link	Wireless Link	Power
Power On	N/A	N/A	Permanent Solid Green
Radio Scanning	N/A	Blinking Green-Slow	N/A
No WORP Link	N/A	Blinking Green-Slow	N/A
WORP link is up	N/A	Permanent Solid Green	N/A
Ethernet Link Present	Permanent Solid Green	N/A	N/A
System failure	N/A	N/A	Off
Reload	N/A	Blinking Green-Fast	N/A
No Application	N/A	Ten Rapid Green Blinks followed by Off	N/A

NOTE:

- For Fast Blink, the LED blinks for every 2 second interval.
- For Slow Blink, the LED blinks for every 10 second interval.

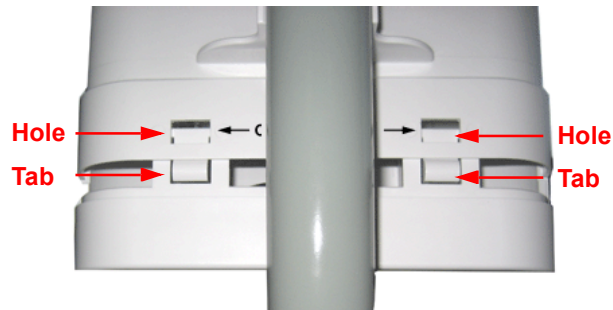
LED Display on the RJ-45 Connector for Ethernet Activity

Status	Ethernet Link LED	Ethernet Activity LED
No traffic on Ethernet interface	Solid Red: 10Mbps Solid Amber: 100Mbps Solid Green: 1000Mbps	Solid Amber: Ethernet Present
Passing traffic on Ethernet interface	Blinking Red:10Mbps Blinking Amber: 100Mbps Blinking Green: 1000Mbps	Solid Amber: Ethernet Present

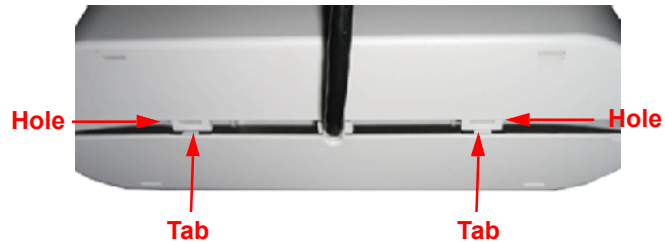
If a wireless link is not established with the BSU, adjust the direction of the unit so that the integrated antenna is more precisely aimed toward the BSU. When the Power LED is solid green or solid yellow, the link is correctly established.

Step 6: Close Cable Compartment

1. Ensure that the Ethernet cable is properly routed and exiting the unit through the notch at the bottom of the cable compartment.
2. Position the cable cover so that the notch in the cover fits over the Ethernet cable (not pictured) and the large tabs on the cover are aligned below the holes in the unit.



3. Align the small tabs in the bottom cover with the holes in the unit.



4. Slide cover upward until all tabs (large and small) on the cover snap into their respective holes on the enclosure.



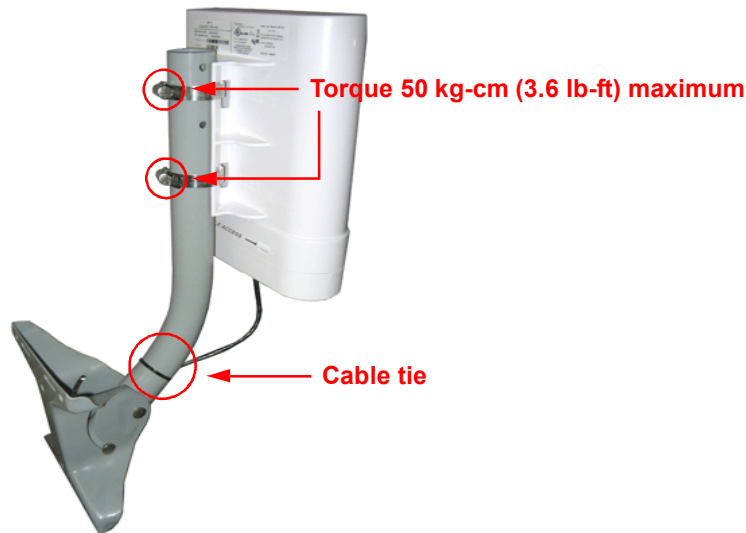
The final assembly is shown below.



Step 7: Tighten Band Clamps/Secure Ethernet Cable

1. Using a 5/16" nutdriver or a screwdriver, fully tighten both band clamps (maximum torque 50 kg-cm/3.6 lbf-ft).
2. Secure Ethernet cable to the pole with cable ties. Provide some slack between the unit and the first cable tie, which should be within 12 inches of the unit. Continue to secure cable with cable ties at 3-foot intervals.

The final assembly, using the optional Proxim universal pole mounting kit (P/N 1087-UMK), is shown below.



Step 14: Align the Antenna

Antenna alignment is the process of physically aligning the antenna of the radio receiver and transmitter to have the best possible link established between them. The antenna alignment process is usually performed during installation and after major repairs.

The antenna of the device can be aligned by entering the specified CLI command. The CLI command enables numerical feedback as the CLI shows the running Signal-to-Noise Ratio (SNR) values twice a second.

NOTES:

- The range of the average SNR has been limited to values from 5 to 43.
- The Antenna Alignment Display (AAD) CLI command is disabled automatically 30 minutes after it is enabled to remove the load of extra messages on the wireless interface. The default telnet time-out is 900 seconds (15 minutes). If AAD must run for the entire 30 minutes, change the default telnet time-out value to a value greater than 30 minutes (greater than 1800 seconds). With the serial interface, the default time out is 30 minutes.

Antenna Alignment Commands

- **aad enable local display**: Enables display of the local SNR. Local SNR is the SNR measured by the receiver at the near end.
- **aad enable remote display**: Enables display of the remote SNR. Remote SNR is the SNR as measured by the receiver at the far end.

NOTE: You must have a flat blade screw driver to disconnect and pull out the Serial cable from the enclosure after the antenna alignment is done. After withdrawing cables, seal the ethernet port carefully to avoid water seepage.

2.4 Initialization

Connecting to the device requires either:

- A direct connection with a serial RS-232 cable.
- A direct connection with an Ethernet cable or a network connection.

Connecting with the Ethernet cable allows you to use of the Web Interface and SNMP in addition to the CLI. Connecting with a serial connection allows you to configure and manage the device with the CLI.

Using a serial connection, you can access the device through a terminal emulation program, such as HyperTerminal. (See "HyperTerminal Connection Properties" in the *Tsunami MP-8150-CPE Reference Manual*.)

For all other modes of connection, you will need the IP address of the device to use the Web Interface, SNMP, or the CLI. Because each network is different, an IP address suitable for your network must be assigned to the unit. You must have this IP address to configure and manage the device through its Web Interface, SNMP, or Telnet/CLI. The device can use either a **static** or **dynamic** IP address. The device obtains its IP address automatically through DHCP (dynamic IP address); or else, you must set the IP Address manually (static IP address).

2.4.1 ScanTool

ScanTool is a software utility that runs on Microsoft Windows machines and is included in the installation CD-ROM within the device package. Using ScanTool, the IP address assigned to the device can be obtained and, if required, can be changed to the IP address that is appropriate for the network. The tool automatically detects the devices installed in the network segment, regardless of IP address, and enables the configuration of each device's IP settings.

To access the HTTP interface and configure the device, the device must be assigned an IP address, which is valid on its Ethernet network. By default, the device is configured with the IP address 169.254.128.132. Using ScanTool, you can

- Launch the Web interface
- Scan devices which can respond to the Scantool
- Modify the assigned IP address
- Switch between the network adapters, if there are multiple network adapters in the system

2.4.2 Setting the IP Address with ScanTool

To initialize the scan tool

1. Power up or reset the device.
2. Run ScanTool on a computer connected to the same LAN subnet as the device, or a computer directly connected to the device with a cross-over Ethernet cable.
3. ScanTool scans the subnet and displays a list of detected devices in the Scan List.

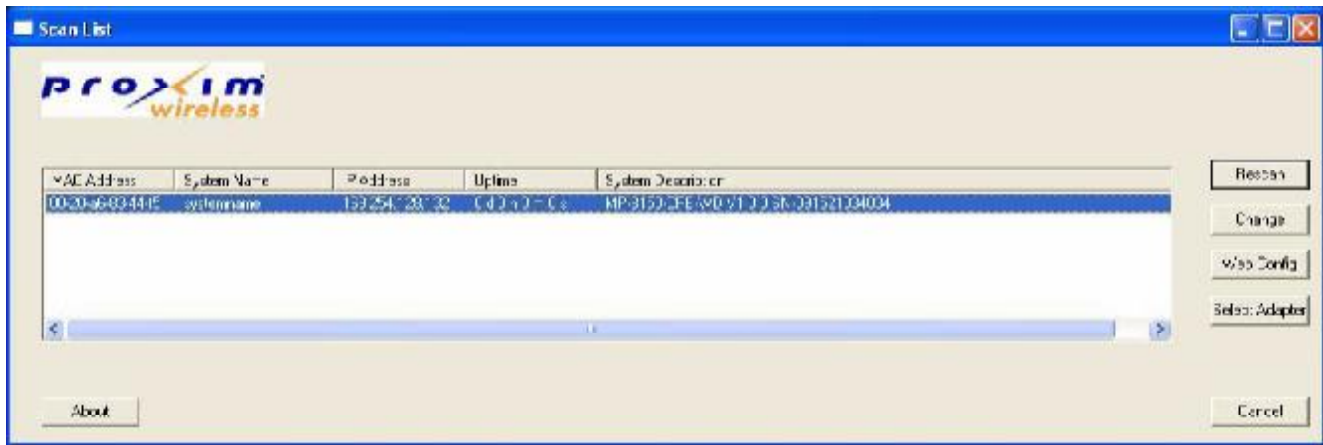



Figure 2-2 Scan List

NOTE: If your computer has more than one network adapter installed, it prompts you to select the adapter for the ScanTool before the Scan List appears. You can select either an Ethernet or wireless adaptor. If prompted, select an adapter and click **OK**. You can change your adapter setting whenever necessary by clicking **Select Adapter** on the Scan List screen.

4. If your device details do not appear in the Scan List, click **Rescan** to update the display. Note that after rebooting the device, it may take up to five minutes for the device details to appear in the Scan List. If the device details still do not appear in the list, see [Troubleshooting](#) for suggestions.

2.4.3 Modifying the IP Address

Select the device details from the scan list and click **Change**. A **Change** screen appears as shown in the following figure. The system automatically generates the **MAC address**, **System Name**, **TFTP Server IP Address** and **Image File Name** of the unit. These details can be changed only through Web Interface.



The screenshot shows a 'Change' dialog box with the following fields and values:

- MAC Address: 00-20-a6-83-44-f5
- Name: systemname
- IP Address Type: Static Dynamic
- IP Address: 169.254.128.132
- Subnet Mask: 255.255.255.0
- Gateway IP Address: 169.254.128.133
- TFTP Server IP Address: 169.254.128.133
- Image File Name: imagenam
- Read/Write Password: (empty)

Buttons at the bottom: Web Configuration, OK, Cancel.

Figure 2-3 Modifying the IP Address

2.4.3.1 Assigning the IP Address Manually

1. Select the **IP Address Type** as **Static** and then enter the appropriate **IP Address**, **Subnet Mask**, and the **Gateway IP Address** parameters.
2. Enter the SNMP Read/Write password in the **Read/Write Password** field. By default, it is **public**.
3. Click **OK** to save the details.

The device automatically reboots after clicking **OK**.

By clicking **Rescan**, verify whether the changes are applied or not. Then, click **Web Configuration** to open the web interface.

2.4.3.2 Assigning the IP Address Dynamically

NOTE: Before setting the IP Address Type as **Dynamic**, ensure there is a DHCP server in the network.

1. Select the **IP Address Type** as **Dynamic**. The **IP Address**, **Subnet Mask** and the **Gateway IP Address** fields get disabled.
2. Enter the SNMP Read/Write password in the **Read/Write Password** field. By default, it is **public**.

3. Click **OK** to save the details.

The device automatically reboots after clicking **OK**. By clicking **Rescan**, verify whether the changes are applied or not. Then, click **Web Configuration** to open the web interface.

2.5 Logging in to the Web Interface

Once the device is connected to your computer, use a web browser to configure and monitor the device. Enter <http://169.254.128.132> (the device default IP address) in the address bar.

The user is prompted to enter the username and password to access the wireless device.

The default User Name is **admin** and Password is **public**.



Figure 2-4 Login Page

NOTES:

- Depending on the settings made during the device initialization, the IP address may be either a dynamic IP address assigned by a network DHCP server or a static IP address which is manually configured. Refer to [ScanTool](#) for information on how to determine the device's IP address and manually configure a new IP address.
- If the connection is slow or unable to connect, use the Internet Explorer **Tools** option to ensure that you are not using a proxy server for the connection.
- If you are unable to log into the configuration pages by using default user name and password, please check with the administrator or follow [Forced Reload](#) procedures.
- For security purposes, it is recommended to change **Password** from the default "public" immediately to restrict unauthorized access to the device.

2.5.1 System Summary

Upon successful login, the system summary of the device is displayed on the screen. The system summary mainly displays the general information and current state of the system, such as System Name, IP Address, Interface Status, and Event Log.

System Summary

System Name	System Name
System Up-Time	00:00:00:40 (dd:hh:mm:ss)
IP Address	169.254.128.132
Remote Partners	0
Radio Mode	SU
Network Mode	Bridge

Interface	Status	Physical Address	Speed/Mode
Ethernet 1	UP	00:20:a6:00:12:12	1 Gbps / Full Duplex
Wireless	DOWN	00:03:7f:be:f0:ea	52Mbps

Event Log

```

00d:00h:00m:09s-->-----
00d:00h:00m:09s-->Device initialized with Firmware Version 1.0.1 B208143 Timest
00d:00h:00m:11s-->Device is in Bridge Mode
00d:00h:00m:39s-->Wireless: Tx Rate 52Mbps, Power Level 21.8dBm
00d:00h:00m:40s-->System Initialization Successful.

```

Clear Event Log Refresh

Figure 2-5 System Summary Page

2.5.2 COMMIT Button

Commit button is used to apply the configuration changes into the unit. When changes are made to the configuration parameters of the device, until the COMMIT button is clicked, the changes will not take effect. Some parameters may require system reboot for the changes to take effect. On clicking COMMIT, the system evaluates all the configuration dependencies and displays the configuration status.

Before applying commit, the system displays a confirmation message, as shown in the following figure:



In some cases, upon successful **COMMIT** operation, a message “**Please Reboot to take effect**” appears as follows:



2.5.3 REBOOT Button

Reboot operation is required for any change in the key parameters to take effect. For example, settings such as configuring the Radio Mode, IP Address, and Network Mode need reboot to take effect.

It is recommended that the device must be rebooted immediately after modifying a rebootable parameter. System displays a confirmation window, wherein click **OK**.



NOTES:

- It is always mandatory to commit the changes before **REBOOT**, otherwise the changes will not take effect.
- The **System Summary** can be viewed by clicking **HOME**.
- The Event Log can be cleared by clicking **Clear Event Log** and can be refreshed by clicking **Refresh**.

An error message appears when a parameter is configured with inappropriate value. This error message prompts you to verify your data or warns you to correct the pathway.

2.6 Factory Default Configuration

Parameter	Default
Network Mode	Bridge
Routing	Disabled
WORP Network Name	MY_NETWORK
Password	public
IP Address Assignment Type	Static
IP Address	169.254.128.132
Subnet Mask	255.255.255.0
Registration Timeout	5
Network Secret	Public
SNMP Management Interface	Enabled
Telnet Management Interface	Enabled
HTTP Management Interface	Enabled
MAC Authentication	Disabled
Radius Authentication	Disabled
Input Bandwidth Limit (in Kbps)	As per license
Output Bandwidth Limit (in Kbps)	As per license
QoS	Disabled
Filtering	Disabled
DHCP Server	Disabled
DHCP Relay	Disabled
RIP	Disabled
NAT	Disabled

Basic Configuration

This chapter provides an overview of the basic configuration settings of Tsunami MP-8150-CPE.

It covers the following topics:

- [Country and Related Settings](#)
- [Dynamic Frequency Selection \(DFS\)](#)
- [Transmit Power Control](#)
- [Setting Up a Link Between BSU and SU](#)
- [Virtual Local Area Networks \(VLANs\)](#)
- [Basic Configuration Information](#)

3.1 Country and Related Settings

The unit's **Advanced Configuration** window provides a frequency domain field that automatically provides the allowed bandwidth and frequencies for the selected country.

Units sold in the United States are pre-configured to scan and display only the outdoor frequencies permitted by the FCC. No other country can be configured. Units sold outside of the United States support the selection of a country by the professional installer using frequency domain.

NOTE: *Non-US installers should not add an antenna system until the Country is selected, the device is rebooted, and the proper power level is configured. The Transmit Power Control (TPC) feature should be used to reduce the power when required.*

The Dynamic Frequency Selection (DFS) feature is enabled automatically when you choose a country and band that require it. Refer to [Frequency Domains and Channels](#) for information on which bands need DFS.

3.2 Dynamic Frequency Selection (DFS)

The Tsunami MP-8150-CPE supports Dynamic Frequency Selection (DFS) for FCC, IC, and ETSI regulatory domains per FCC Part 15 Rules for U-NII devices, IC RSS-210, and ETSI EN 301-893 and 302-502 regulations, respectively. These rules and regulations require that the devices operating in the 5 GHz band must use DFS to prevent interference with radar systems.

When not connected to the BSU, the SU scans continuously for all the channels in the configured Frequency Domain for the presence of BSU. If suitable BSU is found in a channel, the SU tries to connect to it.

NOTE: *Since the device may need to scan for radar on multiple channels, you must allow a sufficient amount of time for the units to start up. This is considerably longer than when the device is not using DFS. This is expected behavior.*

The Startup time is within four minutes if no radar is detected, but up to one minute is added for every selected channel that results in radar interference.

For detailed information on DFS, refer to [Frequency Domains and Channels](#).

3.3 Transmit Power Control

Transmit Power Control is a manual configuration selection to reduce the unit's output power. The maximum output power level for the operating frequency can be found in the event log of the unit's embedded software.

ATPC (Automatic Transmit Power Control) is a feature to automatically adapt transmit power when the quality of the link is more than sufficient to maintain a good communication with reduced transmit power. This feature is required for FCC DFS. It works by monitoring the quality of the link and reducing the output power of the radio by up to 6 dB when good link quality can still be achieved. When link quality reduces, the output power is automatically increased up to the original power level to maintain a good link. For a full discussion of DFS, see [Dynamic Frequency Selection \(DFS\)](#).

By default, the device transmits at the maximum output power that the radio can sustain for data rate and frequency selected. However, with Transmit Power Control (TPC), you can adjust the output power of the device to a lower level in order to reduce interference to neighboring devices or to use a higher gain antenna without violating the maximum radiated output power allowed for your country/band. Also, some countries that require DFS also require the transmit power to be set to a 6 dB lower value than the maximum allowed EIRP when link quality permits, as part of the DFS requirements.

NOTE:

- When the system is set to transmit at the maximum power, professional installers must ensure that the maximum EIRP limit is not exceeded. To achieve this, they may have to add attenuation between the device and the antenna when a high gain antenna is used.
- You can see your unit's current output power for the selected frequency in the event log. The event log shows the selected power for all data rates, so you must look up the relevant data rate to determine the actual power level.
- This feature lets you only to decrease your the output power of the device; you cannot increase the output power of your device beyond the maximum the radio allows for your frequency and data rate.
- If TPC is used or activated, ATPC will be deactivated.

3.4 Setting Up a Link Between BSU and SU

The following parameters have to be configured with the same values on both BSU and SU or forming a link.

- Network Name
- Network Secret
- Encryption (when used)
- Frequency Channel (when available)
- Channel Bandwidth
- Data Rate

See the description of these parameters and how to configure them in [Advanced Configuration](#).

3.5 Virtual Local Area Networks (VLANs)

Virtual Local Area Networks (VLANs) are logical groupings of network hosts. Defined by software settings, other VLAN members or resources appear (to connected hosts) to be on the same physical segment, no matter where they are attached on the logical LAN or WAN segment. They simplify allowing traffic to flow between hosts and their frequently- used or restricted resources according to the VLAN configuration.

MP-8150-CPE devices are fully VLAN-ready; however, by default, VLAN support is disabled. Before enabling VLAN support, certain network settings should be configured and network resources such as VLAN-aware switches should be available, based on the type of configuration.

For details on how to configure VLAN parameters, refer to [VLAN Configuration \(Bridge Mode only\)](#).

3.6 Basic Configuration Information

The BASIC CONFIGURATION Page in the Web-based Configuration Interface provides a one-place access to a minimum set of configuration parameters to quickly set up a point-to-multipoint network.

Basic Configuration

System Name	System Name	(0-64) characters
Frequency Domain	United States 5GHz	*
Radio Mode	SU	*
Channel Bandwidth	20	MHz *
Auto Channel Selection	Enable	
Active Channel	104 (5.52 GHZ)	
Tx Rate	52Mbps	
Network Name	MY_NETWORK	
BSU Name	<input style="width: 100%;" type="text"/>	
Legacy Mode	Disable	

IP Configuration*

Interface	IP Address	Subnet Mask	Address Type
Ethernet 1	189.254.128.132	255.255.255.0	Static

Default Gateway IP Address

IP Address	189.254.128.132
------------	-----------------

Notes: 1. Channel Bandwidth change will reset the Tx Rate to default value.
 2. Change in the Radio Mode reset Wireless and WORP parameters to default values after reboot.
 * Reboot is required

Figure 3-1: Basic Configuration

See the following table for Basic Configuration parameters and their descriptions:

Parameter	Description
System Name	This is the system name for easy identification of the SU. The System Name field is limited to a length of 64 characters.

Parameter	Description
Frequency Domain	<p>It specifies the country of operation, permitted frequency bands and regulatory rules for that country/domain. Upon choosing a frequency domain, the Dynamic Frequency Selection (DFS) and Automatic Transmit Power Control (ATPC) features are enabled automatically if the selected country and band has a regulatory domain that requires it. The Frequency domain selection pre-selects and displays only the allowed frequencies for the selected country/domain.</p> <p>NOTE: Units sold only in the United States are pre-configured to scan and display only the outdoor frequencies permitted by the FCC. No other country selections, channels, or frequencies can be configured. Units sold outside of the United States support the selection of a Country by the professional installer. If you change the Frequency Domain, a reboot of the unit is necessary for the upgrade to take place.</p> <p>NOTE: On units, if World 5 GHz is selected from the Frequency Domain drop-down menu, any Channel in the 5 GHz range are displayed for manual selection.</p> <p>For a non US device, the default Frequency Domain selected is World 5GHz. For more information on frequency domains, refer to Frequency Domains and Channels</p>
Radio Mode	It specifies the mode of operation of the Unit. The Radio Mode is SU.
Channel Bandwidth	Selects the channel bandwidth. By default, it is set to 20 MHz. 40 MHz can be selected for higher throughputs depending on the distance and signal quality.
Auto Channel Selection	<p>Enable or disable the auto channel selection for wireless interface. If ACS is enabled on the BSU, it scans all the channels and selects the best channel at the start up. If ACS is enabled on the SU, SU continuously scans all the channels till it connects to an BSU.</p> <p>NOTE: ACS is enabled by default on SU.</p>
Preferred Channel	<p>It displays a list of available channels in the specified frequency domain. Configure this if you want to operate the device in a specific channel.</p> <p>NOTE: When DFS is active, the Device will automatically pick a new channel when RADAR interference is detected. Preferred channel is applicable only when Automatic Channel Selection is disabled.</p>

Parameter	Description
Active Channel	This will display the current active channel on which wireless interface is operating. If you have enabled the auto channel selection option or if the device moves to a different channel because of radar detection, then this field displays the current operating channel.
Tx Rate	This parameter represents the transmission data rate of the device. Desired rate can be selected from the list of available Tx rates. NOTE: Configure the appropriate data rate based on the signal level.
Network Name	It is the name given to a network so that an BSU and an SU can mutually authenticate. SU can register to BSU, only if it has the same Network Name. The Network Name can be 2 to 32 characters in length.
Legacy Mode	Select Enable or Disable . When Legacy Mode is enabled, it helps the device to interoperate with the legacy products of the Tsunami MP.11 family: MP.11 5054 series, 5012 series, 2454 series, etc.
Ethernet IP Configuration	
By default, the device is configured to operate in Bridge Mode. The parameters in this section vary depending on the device's operating mode, i.e., Bridge or Router.	
IP Address Type	<ul style="list-style-type: none"> • Select Static if you want to assign a static IP address to the unit. Use this setting if you do not have a DHCP server or if you want to manually configure the IP settings. • Select Dynamic to have the device run in DHCP client mode, which gets an IP address automatically from a DHCP server over the network. <p>NOTE: The default Address Type is Static.</p> <p>When the unit is in Bridge mode, only one IP address is required. This IP address also can be changed with ScanTool (See Setting the IP Address with ScanTool).</p>
IP Address	This parameter is configurable only if the IP Address Assignment Type is set to Static. The default IP Address for device is 169.254.128.132.
Subnet Mask	The mask of the subnet to which the unit is connected (the default subnet mask is 255.255.255.0). This parameter is configurable only if the IP Address Assignment Type is set to Static.

Parameter	Description
Gateway IP Address	The IP address of the default gateway. This parameter is configurable only if the IP Address Assignment Type is set to Static. The default gateway IP Address is 169.254.128.132.

4

Advanced Configuration

This chapter provides details about the Tsunami MP-8150-CPE parameters and describes the procedures to configure them using Web-based management interface. These parameters can also be configured using other management interfaces like SNMP and CLI.

The following topics are covered in this chapter:

- [System Configuration](#)
- [Network Configuration](#)
- [Ethernet Properties Configuration](#)
- [Wireless Configuration](#)
- [Security Configuration](#)
- [VLAN Configuration \(Bridge Mode only\)](#)
- [Filtering Configuration \(Bridge Only\)](#)
- [DHCP Configuration](#)
- [Routing Features Configuration](#)

4.1 System Configuration

The System screen allows you to configure the MP-8150-CPE device as an SU, the frequency domain, and the network mode as Bridge or Routing.

To configure the System

1. Click **ADVANCED CONFIGURATION > System**. The System screen is displayed as shown below.

System	
Radio Mode	SU *
Frequency Domain	United States 5GHz *
Network Mode	Bridge *
* Reboot is required	
<input type="button" value="OK"/>	

Figure 4-1 System screen

2. The **Radio Mode** for the MP-8150-CPE device is **SU**.
3. The **Frequency Domain** for the MP-8150-CPE device is 5 GHz.
4. From the **Network Mode** drop-down menu, select either **Bridge** or **Routing**.
5. Click **OK**.

The following table lists the System parameters and their descriptions:

Parameter	Description
Radio Mode	Radio mode specifies the mode of operation and MP-8150-CPE supports SU mode.
Network Mode	The device can be configured in two network modes: Bridge Mode and Routing Mode. The default network mode is Bridge Mode. Refer to Configuring IP in Bridge or Router Mode for more information.
Frequency Domain	A valid frequency domain must be set before the device can be configured with any other parameters. Selecting a frequency domain makes the device compliant with the allowed frequency bands and channels for that regulatory domain.
Active Network Mode	This is a read-only parameter which shows current operating network mode of the device. It is displayed only when the newly configured Network mode differs from the current Active Network mode.

NOTE: Click **COMMIT** and **REBOOT** after changing any system parameter.

4.2 Network Configuration

Based on the selected mode of operation, the IP settings vary. When the device is in Bridge mode, only a single IP address is required; but for Routing mode, individual IP address are needed for each of the Ethernet and Wireless interfaces. In Bridge mode, the IP address can be statically assigned or dynamically obtained through DHCP; whereas in Routing mode, only static assignment is supported.

4.2.1 Configuring IP in Bridge or Router Mode

To configure the Network IP properties

1. Click **ADVANCED CONFIGURATION > Network > IP Configuration**.

If the device is configured in Bridge mode, the following screen appears:

The screenshot shows a configuration window titled "Network CFG". Inside the window, there is a label "Network Mode" followed by a dropdown menu. The dropdown menu is open, and the option "Bridge" is selected and highlighted in blue.

Figure 4-2 IP Configuration in Bridge Mode

If the device is configured in Router mode, the following screen appears:

The screenshot shows a window titled "Network CFG". Inside, there are two buttons: "Network Mode" and "Routing". The "Routing" button is highlighted in blue, indicating it is the selected option.

Figure 4-3 IP configuration in Router mode

2. Enter the appropriate parameters in the IP Configuration screen. See the following table that lists and describes the parameters.
3. Click **OK**. The IP configuration takes effect only after Reboot.

The screenshot shows the "IP Configuration" screen. It contains the following sections:

- Ethernet***: A table with columns S.No., IP Address, Subnet Mask, and Address Type.

S.No.	IP Address	Subnet Mask	Address Type
1	169.254.128.132	255.255.255.0	Static
- Default Gateway IP Address***: A field for IP Address with the value 169.254.128.132.
- DNS**: Fields for Primary IP Address (0.0.0.0) and Secondary IP Address (0.0.0.0).

Below the fields, there is a note: *** Reboot is required**. A further note states: **Notes: 1. DHCP Server must be disabled before changing the network configurations like IPAddress, Subnet Mask, Address Type.** At the bottom, there is an "OK" button.

Figure 4-4 IP Configuration

Parameter	Description
Ethernet	
Address Type	This field is applicable only if the Network mode on the System screen is configured in Bridge mode. This parameter specifies whether the device network parameters are to be configured through DHCP or to be assigned statically. Select Dynamic to configure the device as a Dynamic Host Configuration Protocol (DHCP) client. If Dynamic is selected, the device obtains the IP settings from a network DHCP server automatically during the bootup. If you do not have a DHCP server or if you want to manually configure the device's IP settings, select Static for the Address Type .
IP Address	Enter the IP Address of the interface. In Bridge Mode: When the Address Type is selected as Dynamic , this field becomes read-only and displays the current IP address of the device. If the device cannot obtain an address from a DHCP server, it displays the default IP Address as 169.254.128.132.
Subnet Mask	This parameter represents the subnet mask of the interface. In Bridge Mode: When the Address Type is selected as Dynamic , this field becomes read-only and displays the current subnet mask of the device. If the device cannot obtain an address from a DHCP server, it displays the default subnet mask as 255.255.255.0.
Default Gateway IP Address	This parameter represents the gateway IP Address of the device. In Bridge Mode: When the Address Type is selected as Dynamic , this parameter becomes read-only and displays the device's current gateway IP Address that is obtained through DHCP. If the device cannot obtain an address from a DHCP server, the default gateway IP Address is 169.254.128.132. When Static IP assignment is used, subnet of the default gateway should match with the subnet of any one of the interfaces.
Primary DNS	Specifies the IP Address of the Primary DNS Server.
Secondary DNS	Specifies the IP Address of the Secondary DNS Server.

NOTE: Click **COMMIT** and then **REBOOT** for the changes to take effect.

4.3 Ethernet Properties Configuration

In the Ethernet Interface Properties screen, you can configure the Ethernet transmission properties. The recommended settings are **Auto** for **TxMode And Speed**. The device supports the ethernet interface **Ethernet 1**.

To configure the Ethernet Interface,

1. Click **ADVANCED CONFIGURATION > Ethernet**. The Ethernet Interface Properties screen is displayed as shown below.

S.No.	MACAddress	Operational Speed	Operational TxMode	TxMode And Speed
1	00:20:a6:00:12:12	1 Gbps	Full Duplex	Auto

Figure 4-5 Wireless Ethernet Properties

2. Enter the appropriate parameters in the Ethernet Interface Properties screen. See the following table that lists the parameters and their descriptions.
3. Click **OK** and then click **COMMIT**.

Parameter	Description
MAC Address	Displays the MAC address of the Ethernet interface.
Operational Speed	Displays the current operational speed of the Ethernet interface. The speed can be 1Gbps, 100 Mbps, or 10Mbps.
Operational Tx Mode	Displays the current operational transmit mode of the Ethernet interface. There are 2 types of transmission modes: <ul style="list-style-type: none"> • Half Duplex: Allows one-way transmission at a time. Only receive or transmit operations can be performed at once. • Full Duplex: Allows two-way transmissions simultaneously.

Parameter	Description
TxMode And Speed	<p>This parameter allows the user to select the speed and mode based on the requirement for the corresponding interface.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • <i>Auto: Selects the best transmission mode available when both sides are set to Auto.</i> • <i>The recommended setting is Auto.</i> • <i>In order to allow communication, the transmitter and receiver should be configured in same transmission modes.</i> • <i>The maximum speed is measured as 1 gigabit per second.</i>

4.4 Wireless Configuration

The MP-8150-CPE series of devices use a proprietary Wireless Outdoor Router Protocol (WORP). WORP offers services based on a polling algorithm, specially designed for wireless outdoor networks. WORP is designed to minimize the number of packets being sent over the air by incorporating several mechanisms, like super-packeting and piggy-back acknowledgment in order to achieve maximum throughput possible in the outdoor conditions.

A WORP-based device provides SU mode of operation for establishing a wireless link. The following section describes the configurations for SU.

4.4.1 Configuring WORP Properties in SU Mode

To set the WORP properties

1. Click **Advanced Configuration > Wireless > Interface1 > WORP**. The WORP Configuration screen appears.

WORP Configuration			
Mode	SU		
BSU Name	<input type="text" value="MY_BSU"/>		
Network Name	<input type="text" value="MY_NETWORK"/>	(2-32) characters	
WORP MTU	<input type="text" value="3808"/>	(350-3808) Bytes	
Super Framing	<input type="text" value="Enable"/>	▼	
Registration Timeout	<input type="text" value="10"/>	(1-10) Seconds	
Retry Count	<input type="text" value="3"/>	(0-10)	
Tx Rate	<input type="text" value="52"/>	Mbps ▼	
Input Bandwidth Limit	<input type="text" value="307200"/>	300Mbps	(64 - 307200) Kbps
Output Bandwidth Limit	<input type="text" value="307200"/>	300Mbps	(64 - 307200) Kbps
Bandwidth Limit Type	<input type="text" value="Shaping"/> ▼		
Security Profile Name	<input type="text" value="WORP Security"/> ▼		
<p>Notes: 1. When Channel Bandwidth/Guard Interval/Data Streams are modified, Tx Rate is reset to default automatically</p>			
<input type="button" value="OK"/>			

Figure 4-6 Wireless Interface WORP

2. Enter the appropriate parameters in the WORP Configuration screen. See the following table for the descriptions of the parameters.
3. Click **OK**.

Parameter	Description
Mode	It specifies the radio mode in which the device is configured. MP-8150-CPE supports SU mode.
BSU Name	System Name given to the BSU (Refer to Basic Configuration Information). If the BSU Name is specified, it forces the SU to register to the BSU with the given Network Name and System Name. If the BSU Name is left blank, it allows the SU to register to any BSU with the given Network Name
Network Name	It is the name given to a network so that the BSU and SU can mutually authenticate. The SU can register to the BSU only if it has the same Network Name. The Network Name can be 1 to 32 characters in length.
WORP MTU	WORP MTU (Maximum Transfer Unit) is the largest size of the data payload in wireless frame that may be transmitted. The MTU size can range from 350 to 3808 for High Throughput modes. The default and maximum value of the WORP MTU is 3808.
Super Framing	Super Framing refers to the mechanism that enables multiple Ethernet/802.3 frames to be packed in a single WORP data frame. When the WORP MTU size is configured larger than the Ethernet frame size, then WORP constructs a super frame with size of the WORP MTU configured and pack multiple Ethernet frames. It results in reducing the number of frames transmitted over wireless medium thereby conserving wireless medium and increasing the overall throughput.
Registration Time-out	It specifies the maximum duration for the registration process to complete once the SU starts registering with the BSU. Default time is 10 seconds.
Retries	This parameter specifies the maximum number of times a data message is retransmitted, over the wireless medium, if acknowledgement is not received. By default, this parameter is set to 3.

Parameter	Description
Tx Rate	This parameter represents the modulation rate at which the packet will be transmitted from the wireless device. NOTE: <i>The supported transmission rates vary based on the Channel Bandwidth, Guard Interval, and Number of Data Streams parameters.</i>
Input/Output Bandwidth Limit	This parameter limits the data received on the wireless interface and transmitted to the wireless interface. Minimum of 64 Kbps to the maximum value specified in the License File.
Bandwidth Limit Type	This parameter specifies the action performed when the traffic utilization exceeds the configured input/output limits. Policing: When the traffic utilization reaches the configured limit, the excess traffic will be discarded. Shaping: When the traffic utilization reaches the configured limit, the excess traffic will be buffered and sent at the rate specified in the Output Bandwidth Limit.
Security Profile Name	This parameter represents the security profile currently used. The default Security Profile Name is WORP Security. The Security Profile contains the authentication and encryption methods used to secure the connection between the BSU and SU. Refer to Security Configuration .

To apply the configured properties to the device, click **COMMIT**.

NOTE:

- *Modifying the WORP parameters of SU may result in temporary loss of the link.*
- *When you modify WORP parameters and click **COMMIT**, it may result in brief interruption of service.*

4.4.2 Wireless Interface Properties

In the Wireless Interface Properties screen, you can configure the properties of wireless interface.

To configure the wireless interface properties

1. Click **ADVANCED CONFIGURATION > Wireless > Interface 1 > Properties**. The Wireless Interface Properties screen is displayed as shown below.

Wireless Interface Properties	
Status	<input type="checkbox"/>
Channel Bandwidth	20 MHz *
Auto Channel Selection	Disable
Preferred Channel	160 5.8 GHZ
Active Channel	160 (5.8 GHZ)
Channel Wait Time	60 (0-120) Seconds
Satellite Density	Disable
Cell Size	Large
TPC	0 (0-18) dBm
Antenna Gain	0 (0-40) dBi
Wireless Inactivity Timer	1 (0-600) Minutes
Legacy Mode	Disable

**Note: Channel Bandwidth change will reset the Tx Rate to default value.
* Reboot is required**

OK

Blacklist Information

Channel Number	Reason	Time Elapsed
Refresh		

Figure 4-7 Wireless interface properties

2. Enter the appropriate parameters. See the following table that lists the parameters and their descriptions.
3. Click **OK**.

NOTE: If ACS is enabled and World/Russia frequency domain is selected, establishing WOPR link might take longer time because the device has to scan relatively more number of channels.

NOTE: When you modify wireless parameters and click **COMMIT**, it may result in brief interruption of service.

Parameter	Descriptions
Channel Bandwidth	This parameter specifies the channel bandwidth. By default, it is set to 20 MHz. 40 MHz can be selected for higher throughput.
Auto Channel Selection (ACS)	Enable or disable the Auto Channel Selection for wireless interface. If ACS is enabled on the SU, the SU continuously scans all the channels till it connects to a BSU. By default, ACS is enabled on SU.
Preferred Channel	Select a channel from the drop-down menu if you want to operate the device in that specific channel. NOTE: Preferred channel cannot be configured when ACS is enabled. If DFS is active, the device will automatically pick a new channel when radar interference is detected.
Active Channel	This displays the current operating channel on which wireless interface is operating. NOTE: Active Channel can be different from Preferred Channel if radar interface is detected.
Channel Wait Time	Specifies the maximum time the device waits to begin operation on the selected channel. By default, this value is 60 seconds and ranges from 0 to 120 second.

Parameter	Descriptions
Satellite Density	<p>Satellite Density setting helps achieve maximum bandwidth in a wireless network. It influences the receive sensitivity of the radio interface and improves operation in environments with high noise level.</p> <p>Reducing the sensitivity of the device enables unwanted “noise” to be filtered out (it disappears under the threshold).</p> <p>You can configure the Satellite Density to be Disable, Large, Medium, Small, Mini, or Micro. By default, Satellite Density is disabled. The Medium, Small, Mini, and Micro settings are appropriate for high noise environments; whereas, Large is appropriate for a low noise environment. A long distance link may have difficulty maintaining a connection with a small density setting because the wanted signal can disappear under the threshold. Consider both noise level and distance between the peers in a link when configuring this setting. The threshold should be chosen higher than the noise level, but sufficiently below the signal level. A safe value is 10dB below the present signal strength.</p> <p>If the Signal-to-Noise Ratio (SNR) is not sufficient, you may need to set a lower data rate or use antennas with higher gain to increase the margin between wanted and unwanted signals. In a point-to-multipoint configuration, the BSU should have a density setting suitable for SU, especially the ones with the lowest signal levels (longest links). Take care when configuring a remote interface; check the available signal level first, using Remote Link Test.</p> <p>See Sensitivity Threshold Values for more information on Sensitivity threshold values corresponding to various Satellite Density values.</p> <p>NOTE: <i>When the remote interface is accidentally set to small and communication is lost, it cannot be reconfigured remotely and a local action is required to bring the communication back. Therefore, the best place to experiment with the level is at the device that can be managed without going through the link. If the link is lost, the setting can be adjusted to the correct level to bring the link back.</i></p>
Cell Size	<p>This parameter specifies the cell size for the TPC setting on the wireless medium. By default, the cell size is configured to Large. You can configure the cell size as Large, Medium or Small. The TPC range is controlled by this parameter.</p>

Parameter	Descriptions
TPC	<p>With Transmit Power Control (TPC), you can adjust the output power of the device to a lower level. This is performed to reduce interference with the neighboring devices. It can be helpful when higher gain antenna is used without violating the maximum radiated output power for a country or regulatory domain. This value can be configured in 1 dB increments.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • This feature only lets you decrease the output power; it does not let you increase the output power beyond the maximum allowed defaults for the selected frequency and country. • The range of values depend on the Cell Size.
Antenna Gain	<p>The sensitivity of the radio card can be modified when detecting radar signals in accordance with ETSI, FCC, and IC Dynamic Frequency Selection (DFS) requirements. As the radar detection threshold is fixed by ETSI, the FCC, and IC and a variety of antennas with different gains may be attached to the device, you must adjust this threshold to account for higher than expected antenna gains. This can avoid false radar detection events which can result in frequent change in the Frequency channels.</p> <p>Configure the threshold for radar detection at the radio card to compensate for increased external antenna gains. The Antenna Gain value ranges from 0 to 40. The default value is 0.</p> <p>NOTE: Modifying any of the wireless parameters results in temporary loss of connectivity between the BSU and SU.</p>
Wireless Inactivity Timer	<p>Resets the wireless interface if there is no change in the Tx and Rx Packet Count in the specified interval of time. The default value is set to 1 min. and can be configured between 0 to 600 min.</p>
Legacy Mode	<p>Select Enable or Disable. When Legacy Mode is enabled, it helps the device to interoperate with the legacy products of the Tsunami MP.11 family: MP.11 5054 series, 5012 series, 2454 series, etc.</p>

4.4.3 Blacklist Information

This section displays information regarding various blacklisted channels. It consists of the following parameters.

NOTE: Click **COMMIT** for the changes to take effect.

Parameter	Description
Channel Number	The channel number indicates the channel that is blacklisted.
Reason	The reason for which that particular channel is blacklisted. The most common reason for blacklisting a channel is the presence of a radar in that channel.
Time Elapsed	The time elapsed since the channel was blacklisted. When the channel is black listed due to the presence of a radar, it will be de-blacklisted after 30min.

4.4.4 Sensitivity Threshold Values

Sensitivity threshold values corresponding to various Satellite Density values are given in the table below:

Satellite Density	Receive Sensitivity Threshold	Defer Threshold
Large	-96 dbm	-62 dbm
Medium	-86 dbm	-62 dbm
Small	-78 dbm	-52 dbm
Mini	-70 dbm	-42 dbm
Micro	-62 dbm	-36 dbm

4.4.5 MIMO Properties

The MIMO Properties screen allows you to configure the Multiple-Input-Multiple-Output radio to achieve maximum performance and high throughput.

To configure MIMO properties

1. Click **ADVANCED CONFIGURATION > Wireless > Interface1 > MIMO Properties**. The MIMO Properties screen opens as shown below.

MIMO Properties

Guard Interval	Full GI-800nSec
Data Streams	2-Higher Throughput ▼

Note: 1. Data Streams/Guard Interval change will reset the TX Rate to default value.

Antenna Status

	A1	A2	A3	
Tx Antenna Status	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="OK"/>
Rx Antenna Status	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="OK"/>

Figure 4-8 MIMO Properties

2. Enter the appropriate parameters on the MIMO Properties screen. See the following table that lists the parameters and their descriptions.
3. Click **OK**.

NOTE: When you modify MIMO parameters and click **COMMIT**, it may result in brief interruption of service.

Parameter	Description
Frequency Extension	<p>Configuration of this parameter is valid only if the channel bandwidth is 40 MHz. If Upper Extension Channel is selected, the radio automatically uses the current channel (20MHz) as well as next upper adjacent channel (20 MHz) for data transmission. If Lower extension channel is selected, the radio automatically uses the current channel (20MHz) as well as lower adjacent channel (20 MHz) for data transmission.</p> <p>For example, if channel 36 is selected in 40+ mode, the radio uses 36 as well as next upper adjacent channel 40 also for data transmission, similarly if channel 40 is used in 40- mode, the radio uses 40 as well as the next lower adjacent channel 36 for data transmission.</p>

Parameter	Description
Guard Interval	Possible values for Guard interval are 800 nSec and 400 nSec. 400 nSec is valid only for 40 MHz channel bandwidth.
Data Streams	MIMO radio uses multiple antennas for transmitting and receiving the data. These data streams specify the number of data streams over the air transmitted or received in parallel. <ul style="list-style-type: none"> Data streams "1-Longer Range" uses a single flow of the signals on the antennas. Data streams "2-Higher Throughput" uses double flow of the signals on the antennas in parallel.
Tx Antenna Status	This parameter allows the user to specify the antenna to be used for data transmission. Selecting the respective antenna number checkbox specifies radio to use that specific antenna for data transmission.
Rx Antennas Status	This parameter allows the user to specify the antenna to be used for data reception. Selecting the respective antenna number checkbox specifies radio to use that specific antenna for data reception.

Modifying the Guard Interval, Data Streams, Tx Antenna Status and Rx Antenna Status will reset the Tx Rate to default.

4.5 Security Configuration

4.5.1 Setting Up Wireless Security

In Wireless Security page, you can configure security mechanisms used to secure the communication link between the BSU and SU. By default, a security profile (**WORP Security**) is preconfigured with the default configuration for WORP security. However, more profiles can be created as required. Even though multiple security profiles can be created, only one security profile can be active at a time. The active security profile is configured as part of the WORP property **Security Profile Name**. For a security profile to be active, it must be enabled.

NOTE: The active security profile parameters on the BSU and SU should match for the connection to work as desired.

To configure the Wireless security properties

1. Click **ADVANCED CONFIGURATION > Security > Wireless Security**. The Wireless Security Configuration screen is displayed as shown below.

S.No.	Profile Name	Entry Status	Edit
1	WORP Security	Enable	

OK Add

Figure 4-9 Wireless Security Configuration

2. Select the appropriate parameters. See the following table that lists the parameters and their descriptions.
3. Click **OK**.

Field	Description
Profile Name	Specifies the security profile name.
Entry status	Used to enable or disable the security profile.
Edit	Click Edit to modify the Profile parameters.

- By default, **WORP Security** is added to the wireless security configuration.
- Default authentication mode is **WORP**.

4.5.1.1 Creating a New Security Profile

To create a new security profile

1. Click **ADVANCED CONFIGURATION > Security > Wireless Security**.
2. Click **Add** in the Wireless Security Configuration screen to create a new entry. The **Wireless Security Add Row** screen is displayed as shown below.

Wireless Security Add Row

Profile Name	Security
Encryption Type	AES-CCM
Key 1
Key 2
Key 3
Key 4
Transmit Key	1
Entry Status	Enable
Network Secret (6-32)

Note:

1. For WEP Encryption type the keys length should be (Ascii 5/13/16) (Hex 10/26/32)
2. For TKIP/AES-CCM Encryption types the keys length should be (Ascii 16) or (Hex 32)
3. For 11NA/11NG modes, only AES-CCM Encryption is supported
4. For setting the password characters - = " ' ? \ / space are not allowed.

Add Back

Figure 4-10 Creating a New Security Profile

3. Enter the appropriate parameters in the Wireless Security Add Row screen. See the following table for information on the parameters and their descriptions.
4. Click **Add**.

Field	Description
Profile Name	Enter the security profile name.
Encryption Type	Select an option from None , WEP , TKIP or AES-CCM for the Encryption Type .

Field	Description
	<p>1. None - If this option is selected, no encryption will be applied to the wireless link frames.</p> <p>2. AES-CCM - This option represents CCM Protocol with AES Cipher restricted to 128 bits.</p> <ul style="list-style-type: none"> • Key 1/Key 2/Key 3/Key 4: Enter 16 ASCII Characters or 32 Hex Digits. • Transmit Key: Select one out of the four keys described above as the default transmit key with which the frames are encrypted. <p>3. WEP - This option represents the WEP Encryption type, which uses RC4 stream cipher for confidentiality and CRC-32 for integrity. The supported key lengths for WEP are 5/13/16 ASCII Characters or 10/26/32 Hexadecimal digits.</p> <ul style="list-style-type: none"> • Key1 / Key 2 / Key 3 / key 4: Enter 5/13/16 ASCII Characters or 10/26/32 Hexadecimal digits. • Transmit Key: Select one out of the four keys described above as the default transmit key with which the frames are encrypted. <p>4. TKIP - This option represents the TKIP Encryption type, which uses RC4 stream cipher for confidentiality. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism. It uses 128-bit keys for encryption. The key length for TKIP is 16 ASCII characters or 32 Hexadecimal digits.</p> <ul style="list-style-type: none"> • Key1 / Key 2 / Key 3 / key 4: Enter 16 ASCII Characters or 32 Hexadecimal digits. • Transmit Key: Select one out of the four keys described above as the default transmit key with which the frames are encrypted. <p>NOTE:</p> <ul style="list-style-type: none"> • All four Keys (Key1, Key2, Key3, Key4) have to be of same length and same type i.e., all four Keys should be either ASCII Characters or Hexadecimal digits. • Transmit Key can be any one of the four keys, provided all the four keys in BSU and SU are the same. • WEP/TKIP Encryption Types are supported only in legacy Modes. • The encryption mode should not be selected as AES-CCM while the device is interoperating with legacy Tsunami MP.11 family devices which include 954-R, 2454-R, 4954-R, 5054-Series, and 5012-Series.
Entry status	Select Enable/Disable to enable or disable the status of the security profile.
Network Secret	<p>Enter the WOPR Protocol Secret Key used for authenticating the SU with the BSU.</p> <p>NOTE: The BSU and SU should have same Network Secret.</p>

Sample Security Profile Configuration

	SU
Profile Name	WORP Security
Encryption Type	AES-CCM
Key 1	1234567890abcdef
Key 2	1asdf67890abcdef
Key 3	abcde7890abcdefg
Key 4	pjhohm7890abcdef
Transmit Key	2
Network Secret	public
Entry status	Enable
<p>NOTE:</p> <ul style="list-style-type: none"> • <i>By using the preceding security configuration, Wireless link data follows these constraints:</i> <ul style="list-style-type: none"> – <i>At SU, frames going out from the SU are encrypted using Key 2 and decrypted using Key 1.</i> 	

4.5.1.2 Modifying a Security Profile

To edit the parameters of the existing security profiles

1. Click **ADVANCED CONFIGURATION > Security > Wireless Security**.
2. Click **Edit**. The Wireless Security Edit Row page appears.
3. Edit the parameters and click **OK**.
4. To apply the configured properties to the device, click **COMMIT**.

4.6 VLAN Configuration (Bridge Mode only)

Virtual Local Area Networks (VLANs) are logical groupings of network hosts. Defined by software settings, other VLAN members or resources appear (to connected hosts) to be on the same physical segment, no matter where they are attached on the logical LAN or WAN segment. They simplify traffic flow between clients and their frequently-used or restricted resources.

A device can communicate across a VLAN-capable switch that analyses VLAN tagged frames and directs traffic to the appropriate units. The purpose of this network is to provide an easy way of modifying logical groups in the dynamic environment. VLAN is supported only in **Bridge** mode.

VLANs are used to conveniently, efficiently, and easily manage your network in the following ways:

- Define groups
- Reduce broadcast and multicast traffic to unnecessary destinations
 - Improve network performance and reduce latency

- Increase security
 - Secure network restricts members to resources on their own VLAN

VLAN features can be managed via:

- The device's Web interface
- The Command Line Interface (see "Command Line Interface" section in the Reference Manual)
- SNMP (Log on to Proxim support site <http://support.proxim.com> for MIBs)

4.6.1 Establishing a VLAN Connection

For enabling the VLAN support, certain network settings should be configured and certain network resources, such as VLAN aware switches should be available, depending upon the type of configuration.

VLAN support also provides the capability to specify a separate VLAN ID and priority for management frames (SNMP, ICMP, Telnet, DHCP, and TFTP).

To configure VLAN

- Click **ADVANCED CONFIGURATION > VLAN**.

VLAN	
VLAN Status	<input type="checkbox"/>
Management VLAN ID	-1 (-1, 1-4094)
Management VLAN Priority	5 (0 - 7)
<input type="button" value="OK"/>	

Figure 4-11 Configuring VLAN

VLAN parameters can be classified into two types: System-related VLAN parameters and Interface-related VLAN parameters.

1. **System-related parameters:** These parameters are applicable to the whole device. The following parameters are the System-related VLAN parameters.
 - a. **VLAN Status:** Selecting the **VLAN Status** checkbox enables the VLAN Status on the device. To update all VLAN related parameters, VLAN status should be enabled.

NOTE: By default, the VLAN status is disabled.

- b. **Management VLAN ID:** This parameter is used to configure the Management VLAN ID. This option is available when Management VLAN ID is configured. The management stations must tag the management frames sent to the device with the management VLAN ID specified in the device. The device will tag all the management frames from the device with the specified management VLAN and priority.

NOTE:

- If the Management VLAN ID is -1, only untagged frames can access the device.
 - Before setting the Management VLAN ID from 1 to 4094, make sure that the management platform or host is a member of the same VLAN; or else, your access to the device will be lost.
- c. **Management VLAN Priority:** This parameter is used to set IEEE 802.1p priority for the frames. The priority value ranges from 0 to 7. By default, it is set to 0 (zero).
2. **Interface-related VLAN parameters:** The device supports configuring VLAN modes for Ethernet interface. The wireless interface is always in **Transparent Mode**.

4.6.2 VLAN Modes

4.6.2.1 Transparent Mode

Transparent Mode is available for the Ethernet and Wireless interfaces. It is equivalent to **NO VLAN** support and is the default mode. It is used to connect VLAN aware/unaware networks. An interface in transparent mode forwards both tagged and untagged frames.

To configure the VLAN Transparent Mode

1. Click **ADVANCED CONFIGURATION > VLAN > Ethernet**. The VLAN Ethernet Configuration window appears as shown below.

Figure 4-12 VLAN Operation in Transparent Mode

2. Enter the parameters listed in the following table.
3. Click **OK**.

Parameters	Description
Interface	Displays the name of the interface.
VLAN Mode	Select the VLAN mode as Transparent .

Click **COMMIT** for the changes to take effect. Once the transparent mode is set, both tagged and untagged frames are received on the interface.

NOTE: Wireless Interface of the device will always be in transparent mode. There is no support provided to edit the wireless interface VLAN parameters.

4.6.2.2 Trunk Mode

Trunk mode is configurable on the ethernet interface of the SU. It is mainly used to connect VLAN Aware networks with VLAN Aware networks. When an interface is in **Trunk** mode, it forwards only those tagged frames whose VLAN ID matches with a VLAN ID present in trunk table. All other frames will be dropped.

VLAN Ethernet Configuration

Ethernet 1

Interface: eth1

VLAN Mode: Trunk

Allow untagged Frames: Disable

S.No.	Trunk Id	Entry Status
1.1	15	Enable
1.2	42	Enable

OK Add

Figure 4-13 VLAN operation in Trunk Mode

To enable Trunk mode, click **ADVANCED CONFIGURATION > VLAN > Ethernet** and enter the settings as described in the following table:

Parameter	Description	
Interface	Displays the name of the interface.	
VLAN Mode	Select the VLAN Mode as Trunk .	
Allow Untagged Frames	Select Enable or Disable for this option.	
	Enable	If this option is selected, an interface in trunk mode forwards both tagged frames whose VLAN ID matches with one of the VLAN IDs of the trunk table and untagged frames.

Parameter	Description	
	Disable	If this option is selected, an interface in trunk mode forwards only tagged frames and drops untagged frames.

Adding New Trunk Table Entries

To add new table entries

1. Click **Add** in the VLAN Ethernet Configuration screen. The **VLAN Trunk Table Add Row** page appears.

Figure 4-14 VLAN Trunk Table Add Row

2. Enter the parameters as described in the following table.
3. Click **Add**.

Field	Description
Trunk Id	Enter the value of the trunk VLAN Id.
Entry Status	Enable or disable the status of the trunk table entry.

4. Click **COMMIT** for the changes to take effect.

NOTE: Up to 16 VLAN IDs can be configured on the Ethernet interface of SU.

4.6.2.3 Access Mode

Access mode is available only on the Ethernet interface of SU. This mode is used to connect VLAN aware networks with VLAN unaware networks. In access mode, Tagged frames with specified Access Vlan ID going out of the device through the Ethernet interface are untagged and forwarded. The untagged frames coming into the device through the Ethernet interface are tagged with specified Access Vlan ID and Access Vlan priority and forwarded.

To configure the Access Mode in the VLAN network

1. Click **ADVANCED CONFIGURATION > VLAN > Ethernet**. The VLAN Ethernet Configuration screen appears.

Figure 4-15 VLAN Ethernet Configuration

- Enter the parameters as described in the following table.

Parameter	Description
Interface	Displays the name of the interface.
VLAN Mode	Select the VLAN mode as Access .
Access VLAN Id	The Access VLAN Id values range from 1 to 4094. The default value is -1.
Access VLAN Priority	The Access VLAN priority values range from 0 to 7. The default priority is 0.

- Click **OK**.
- Click **COMMIT** for the changes to take effect.

4.7 Filtering Configuration (Bridge Only)

Filters are useful for preventing bridging of selected protocol traffic from one segment of a network to other segments (or subnets). This feature can be used both to increase the amount of bandwidth available on the network and to increase network security.

The Packet Filtering features help in controlling the amount of traffic exchanged between the wired and wireless networks. Filtering features are available only in bridge mode operations. Using the filtering processes, you can restrict any unauthorized packets from accessing the network.

Following are various filtering types supported by MP-8150-CPE:

- [Ethernet Protocol Filter](#)
- [Static MAC Address Filter](#)
- [Advanced Filter](#)
- [TCP/UDP Port Filter](#)

To configure the filtering mechanism

1. Click **ADVANCED CONFIGURATION > Filtering**. The Filtering screen appears.



Figure 4-16 Filtering

2. Enter the appropriate parameters in the **Filtering** screen. See the following table that lists all the parameters and their descriptions.

Parameter	Description
Global Filter Flag	This parameter is used to enable or disable complete filtering operations.
STP Frame Forward Status	By accepting the STP frames, any loops that occurs within a network can be avoided. Enable: When this option is selected, the STP frames in the system are bridged. Disable: When this option is selected, the STP frames encountered in a network are terminated at bridge.

3. Click **OK**.

NOTE:

- The filtering process is activated only when the **Global Filter Flag** is selected as **Enable**.
- Click **COMMIT** for the changes to take effect in the device.

4.7.1 Ethernet Protocol Filter

The Ethernet Protocol Filter blocks or forwards packets based on the Ethernet protocols supported on the device. The filtering takes effect only when the **Global Flag** is enabled.

The packets are forwarded or dropped depending on their **Entry status**, **Filter status** and **Filtering Type**.

To configure **Ethernet Protocol Filtering**,

1. Click **ADVANCED CONFIGURATION > Filtering > Ethernet Protocol Filtering**. The Protocol Filter screen is displayed as shown below.

Protocol Filter

Filtering Control	Disable ▼
Filtering Type	Passthru ▼

S.No.	Protocol Name	Protocol Number	Filter Status	Entry Status
1	Apollo Domain	80:19	Block ▼	Disable ▼
2	Apple Talk 1 and 2	80:9b	Block ▼	Disable ▼
3	Apple Talk ARP 1 and 2	80:f3	Block ▼	Disable ▼
4	Banyan VINES	0b:ad	Block ▼	Disable ▼
5	Banyan VINES Echo	0b:af	Block ▼	Disable ▼
6	Decnet Phase IV	60:03	Block ▼	Disable ▼
7	DEC Diagnostic	60:05	Block ▼	Disable ▼
8	DEC LAT	60:04	Block ▼	Disable ▼
9	DEC MOP Dump/Load	60:01	Block ▼	Disable ▼
10	DEC MOP Rem Cons	60:02	Block ▼	Disable ▼

Figure 4-17 Protocol Filter

2. Enter the appropriate parameters in the **Protocol Filter** screen. See the following table that lists the parameters and their descriptions.

Parameter	Description
Filtering Control	This parameter is used to configure the interface on which filtering has to be applied. By default, it is disabled. It can be configured as: <ul style="list-style-type: none"> • Ethernet: Packets are examined on the receive path of the Ethernet interface. • Wireless: Packets are examined at the Wireless interface. • All Interfaces: Packets are examined at both Ethernet and wireless interfaces. • Disable: The protocol filtering process is disabled.
Filtering Type	The Filtering Type specifies the action to be taken on the packet whose protocol/ether type is not registered in the protocol filter table or whose Entry Status is in Disable state. By default, it is set to Passthru . <p>Block: The protocols with entry status Disable or the protocols which do not exist in the protocol filtering table are blocked.</p> <p>Passthru: The protocols with entry status Disable or the protocols which do not exist in the protocol filtering table are allowed through the interface.</p>
NOTE: Click COMMIT for the changes to take effect in the device.	
Ethernet Protocol Filter Table	
Protocol Name	Specifies the name of the Ethernet Protocol.
Protocol Number	Specifies the value of the Ethernet packet. The value is of 4 digit Hex format.
Filter Status	This parameter allows configuring the Filter Status as either Block or Passthru . The default is Block . Selection of the Filter Status takes effect only if the Entry Status is Enabled . <p>When this filter status is set to Passthru and entry status is Enable, all packets whose protocol matches with the given protocol number are forwarded on the selected interface.</p> <p>When this filter status is set to Block and entry status is Enable, all packets whose protocol matches with the given protocol number are dropped on selected interface.</p>
Entry Status	Set the Entry Status as Enable/Disable/Delete .
NOTE: Click COMMIT for the changes to take effect in the device.	

3. A few frequently used filters are listed in the **Ethernet Protocol Filter Table**.
4. For adding new entries to the **Protocol filter Table**:
 - a. Click **Add** to display the **Protocol Filters Add Row** page as shown in the following figure.

- b. Enter the details as described in the preceding table and click **Add**.

Protocol Filter Add Row	
Protocol Name	TEST_CASE
Protocol Number	10:20
Filter Status	Block
Entry Status	Enable
<input type="button" value="Add"/> <input type="button" value="Back"/>	

Figure 4-18 Protocol Filter Add Row

NOTE:

- By default, the system generates 19 entries. You can **Enable** or **Disable** the default entries, but the **Delete** option is not applicable for all the default 19 entries.
- The added entry in the table can be enabled, disabled, or deleted based on user requirement.
- Max Entries supported in **Ethernet Protocol Filter Table** are 64.

4.7.2 Static MAC Address Filter

4.7.2.1 Overview

The Static MAC Address filter optimizes the performance of a wireless and wired network. When this feature is configured, the device can block traffic between wired and wireless network based on MAC address.

The filter limits the data traffic between two specific devices (or between groups of devices based on MAC addresses and masks) through the unit's wireless interface. For example, a server on the network, which should not allow wireless clients to communicate, can be set up with a static MAC filter to block traffic between these devices. The **Static MAC Filter Table** performs bi-directional filtering.

Each MAC address or mask consists of 12 hexadecimal digits (0-9 and A-F) that correspond to a 48-bit identifier. Each hexadecimal digit represents 4 bits (0 or 1).

Taken together, a MAC address/mask pair specifies an address or a range of MAC addresses that the device looks for when examining packets. The device performs bitwise "AND" operation between the MAC address and the mask at the bit level. A mask of 00:00:00:00:00:00 corresponds to all MAC addresses, and a mask of FF:FF:FF:FF:FF:FF applies only to the specified MAC address.

For example, if the MAC address is 00:20:A6:12:54:C3 and the mask is FF:FF:FF:00:00:00, the device examines the source and destination addresses of each packet looking for any MAC address starting with 00:20:A6. If the mask is FF:FF:FF:FF:FF:FF, the device looks only for the specific MAC address (in this case, 00:20:A6:12:54:C3).

When creating a filter, the user can configure the Wired parameters only, the Wireless parameters only, or both sets of parameters.

- To prevent all traffic from a specific wired MAC address from being forwarded to the wireless network, configure only the Wired MAC address and Wired mask (leave the Wireless MAC and Wireless mask set to all zeros).

- To prevent all traffic from a specific wireless MAC address from being forwarded to the wired network, configure only the Wireless MAC and Wireless mask (leave the Wired MAC address and Wired mask set to all zeros).
- To block traffic between a specific wired MAC address and a specific wireless MAC address, configure all four parameters.

4.7.2.2 Static MAC Filter Examples

Consider a network that contains a wired server and three wireless clients. The MAC addresses for each unit are as follows:

- **Wired Server:** 00:40:F4:1C:DB:6A
- **Wireless Client 1:** 00:02:2D:51:94:E4
- **Wireless Client 2:** 00:02:2D:51:32:12
- **Wireless Client 3:** 00:20:A6:12:4E:38

Prevent Two Specific Devices from Communicating

Configure the following settings to prevent the Wired Server and Wireless Client 1 from communicating:

- **Wired MAC Address:** 00:40:F4:1C:DB:6A
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:02:2D:51:94:E4
- **Wireless Mask:** FF:FF:FF:FF:FF:FF

Result: Traffic between the Wired Server and Wireless Client 1 is blocked. Wireless Clients 2 and 3 still can communicate with the Wired Server.

Prevent Multiple Wireless Devices From Communicating With a Single Wired Device

Configure the following settings to prevent Wireless Clients 1 and 2 from communicating with the Wired Server:

- **Wired MAC Address:** 00:40:F4:1C:DB:6A
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:02:2D:51:94:E4
- **Wireless Mask:** FF:FF:FF:00:00:00

Result: When a logical "AND" is performed on the Wireless MAC Address and Wireless Mask, the result corresponds to any MAC address beginning with the 00:20:2D prefix. Since Wireless Client 1 and Wireless Client 2 share the same prefix (00:02:2D), traffic between the Wired Server and Wireless Clients 1 and 2 is blocked. Wireless Client 3 can still communicate with the Wired Server since it has a different prefix (00:20:A6).

4.7.2.3 Prevent All Wireless Devices From Communicating With a Single Wired Device

Configure the following settings to prevent Wired Server from communicating with all three Wireless Clients:

- **Wired MAC Address:** 00:40:F4:1C:DB:6A
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:00:00:00:00:00
- **Wireless Mask:** 00:00:00:00:00:00

Result: The unit blocks all traffic between the Wired Server and all wireless clients.

4.7.2.4 Prevent a Wireless Device from Communicating with the Wired Network

Configure the following settings to prevent Wireless Client 3 from communicating with any device on the Ethernet:

- **Wired MAC Address:** 00:00:00:00:00:00

- **Wired Mask:** 00:00:00:00:00:00
- **Wireless MAC Address:** 00:20:A6:12:4E:38
- **Wireless Mask:** FF:FF:FF:FF:FF:FF

Result: The unit blocks all traffic between Wireless Client 3 and the Ethernet network.

4.7.2.5 Static MAC Address Filter Configuration

To configuring Static MAC Filter

1. Click **ADVANCED CONFIGURATION > Filtering > Static Mac Address Filter**. The **Static MAC Address Filter** screen is displayed as shown below.

S.No.	Wired MAC Address	Wired MAC Mask	Wireless MAC Addr	Wireless MAC Mask	Comment	Entry Status
1	10:20:30:40:50:60	10:20:30:40:50:60	10:25:35:45:55:65	10:25:35:45:55:65	TEST_CASE	Enable <input type="button" value="v"/>

OK Add

Figure 4-19 Static MAC Address Filter

2. Click **Add**. The **Static MAC Address Filter Add Row** screen appears.

Wired MAC Address	<input type="text" value="10:20:30:40:50:60"/>
Wired MAC Mask	<input type="text" value="10:20:30:40:50:60"/>
Wireless MAC Address	<input type="text" value="10:25:35:45:55:65"/>
Wireless MAC Mask	<input type="text" value="10:25:35:45:55:65"/>
Comment	<input type="text" value="TEST_CASE"/>
Status	Enable <input type="button" value="v"/>

Add Back

Figure 4-20 Creating a new Static MAC Address Filter

3. Enter the parameters listed in the following table.

Parameter	Description
Wired MAC Address	Specifies the MAC address of the device on the wired network that is restricted from communicating with a device in the wireless network.
Wired MAC Mask	Specifies the range of MAC address to which this filter is to be applied.
Wireless MAC address	Specifies the MAC address of the device on the wireless network that is restricted from communicating with a device in the wired network.
Wireless MAC Mask	Specifies the range of MAC address to which this filter is to be applied.
Comment	Specifies the comment associated with Static MAC Filter table entry.
Status	Specifies the status of the newly created filter.

NOTE: The **Static MAC Address Filter** table supports up to 200 entries.

4. Click **Add** to add a new entry to the Static MAC Address Filter table.
5. Click **Commit** so that the filter gets applied on the network.

NOTE:

- The Wired MAC address and the Wireless MAC address should be a unicast MAC address.
- MAC Address/Mask includes 12 hexadecimal digits (each hexadecimal equals to 4 bits containing 0 or 1) which are equivalent to 48 bit identifier.

4.7.3 Advanced Filter

In Advanced Filtering, IP protocols which are frequently used or transmitted through the network are filtered.

To view the advanced filtering

1. Click **ADVANCED CONFIGURATION > Filtering > Advanced Filtering**. The Advanced Filtering screen is displayed as shown below.

Advanced Filtering			
S.No.	Protocol Name	Direction	Entry Status
1	Deny IPX RIP	Both	Disable
2	Deny IPX SAP	Both	Disable
3	Deny IPX LSP	Both	Disable
4	Deny IP Broadcasts	Both	Disable
5	Deny IP Multicasts	Both	Disable

Figure 4-21 Advanced Filtering

2. The following table describes the parameters present in the **Advanced Filtering** table.

Parameter	Description
Name	This parameter specifies the protocol name. The following filters are supported in Advanced Filtering: <ul style="list-style-type: none"> Deny IPX RIP Deny IPX SAP Deny IPX LSP Deny IP Broadcasts Deny IP Multicasts
Direction	This parameter specifies the direction of an individual entry in the Advanced Filter table. The direction can be Ethernet to Wireless, Wireless to Ethernet, or both.
Entry Status	This parameter specifies the status of the individual entry.

NOTE:

- The Advanced Filtering table contains maximum 5 entries.
- New entries cannot be added and existing entries cannot be deleted from the **Advanced Filtering** table.

4.7.3.1 Editing Table Entries

- Click **Edit** to modify the existing table details. The **Advanced Filtering - Edit Entries** page appears.

Advance Filtering - Edit Entries	
Name	Deny IPX RIP
Direction	Both
Status	Disable
Name	Deny IPX SAP
Direction	Both
Status	Disable
Name	Deny IPX LSP
Direction	Both
Status	Disable
Name	Deny IP Broadcasts
Direction	Both
Status	Disable
Name	Deny IP Multicasts
Direction	Both
Status	Disable
<input type="button" value="BACK"/> <input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Figure 4-22 Advance Filtering- Edit Entries

1. After making the desired modifications, click **OK** to update the table.
2. Click **Back** to navigate to the previous page. Click **Cancel** to retain the previous entries.

NOTE: Click **COMMIT** for the changes to take effect in the device.

4.7.4 TCP/UDP Port Filter

Port-based filtering controls the user access to network services by selectively blocking TCP/UDP protocols through the device. A user can specify a Protocol Name, Port Number, Port Type (TCP, UDP, or Both), and filtering interfaces (only Wireless, only Ethernet or all Interfaces). These parameters can be used to block access to services, such as Telnet and FTP and the traffic, such as NETBIOS and HTTP.

To configure the TCP/UDP Port filtering technique

1. Click **ADVANCED CONFIGURATION > Filtering > TCP/UDP Port Filter**. The TCP/UDP Port Filter screen is displayed as shown below. Create a new protocol by clicking **Add** or make use of the existing protocols.

TCP / UDP Port Filter

Filter Control: ▼

S.No.	Protocol Name	Port Number	Port Type	Filter Interface	Entry Status
1	NetBios Name S	137	Both ▼	All Interface ▼	Disable ▼
2	NetBios Datagra	138	Both ▼	All Interface ▼	Disable ▼
3	NetBios Session	139	Both ▼	All Interface ▼	Disable ▼
4	SNMP service	161	Both ▼	All Interface ▼	Disable ▼
5	IPSEC/ISAKMP	500	Both ▼	All Interface ▼	Disable ▼
6	L2TP	1701	Both ▼	All Interface ▼	Disable ▼
7	PPTP	1723	Both ▼	All Interface ▼	Disable ▼

Figure 4-23 TCP/UDP Port Filter

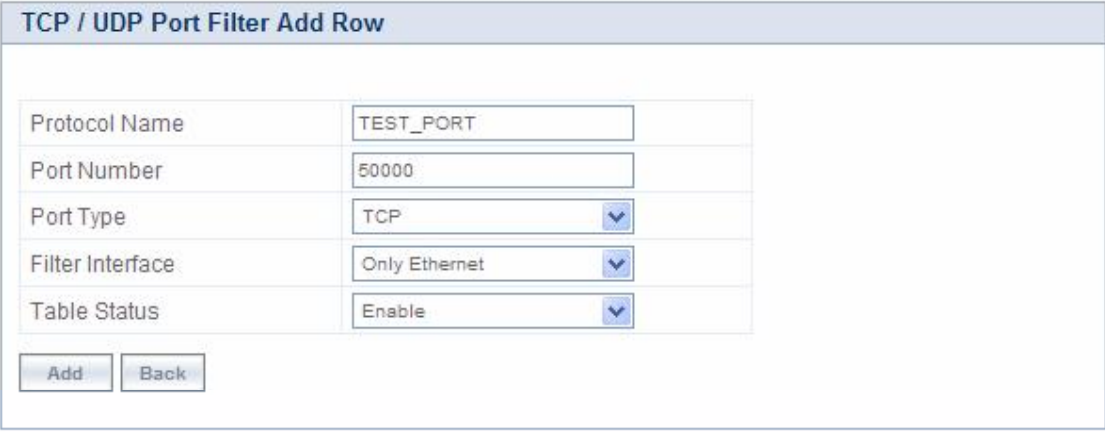
2. Enter the appropriate parameters. See the following table that lists the parameters and their descriptions.

Parameter	Description
Filter Control	This parameter is used to enable the TCP/UDP filter. By default, Disable is selected.
Protocol Name	This parameter specifies the TCP/UDP protocol filter name.
Port Number	This parameter specifies the TCP/UDP port number. It accepts the values within the range 0-65535.
Port Type	This parameter specifies the type of the port. The various options for the Port Type are TCP , UDP and Both . By default, Port Type is Both for the default entries and TCP for the newly added entries.
Filter Interface	This parameter is used to configure the interface type. Options for filter interface are Ethernet, Wireless, and All Interfaces.
Entry Status	This parameter indicates the status of TCP/UDP filter entry. Enable : The device filters the TCP/UDP protocols Disable : The device allows all the TCP/UDP protocols.

4.7.4.1 Adding TCP/UDP Port Table Entries

To add TCP/UDP Port Table entries

1. Click **Add** to create a new TCP/UDP port filter. The **TCP/UDP Port Filter Add Row** page is displayed as shown below.



TCP / UDP Port Filter Add Row	
Protocol Name	TEST_PORT
Port Number	50000
Port Type	TCP
Filter Interface	Only Ethernet
Table Status	Enable
<input type="button" value="Add"/> <input type="button" value="Back"/>	

Figure 4-24 TCPUDP Port Filter Add Row

2. Enter the details and click **Add** to update the entry in the TCP/UDP table.

NOTE:

- The TCP/UDP filtering operation is allowed only when the **Global flag** and **Filter Control** options are selected as **Enable**.
- Maximum 64 entries can be added to the table.
- Click **COMMIT** for the changes to take effect in the device.

4.8 DHCP Configuration

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to assign an IP address to a device from a defined range of IP addresses configured for a given network. It allows you to distribute IP addresses from a central point to various hosts and simplifies the process of configuring the IP addresses to individual hosts.

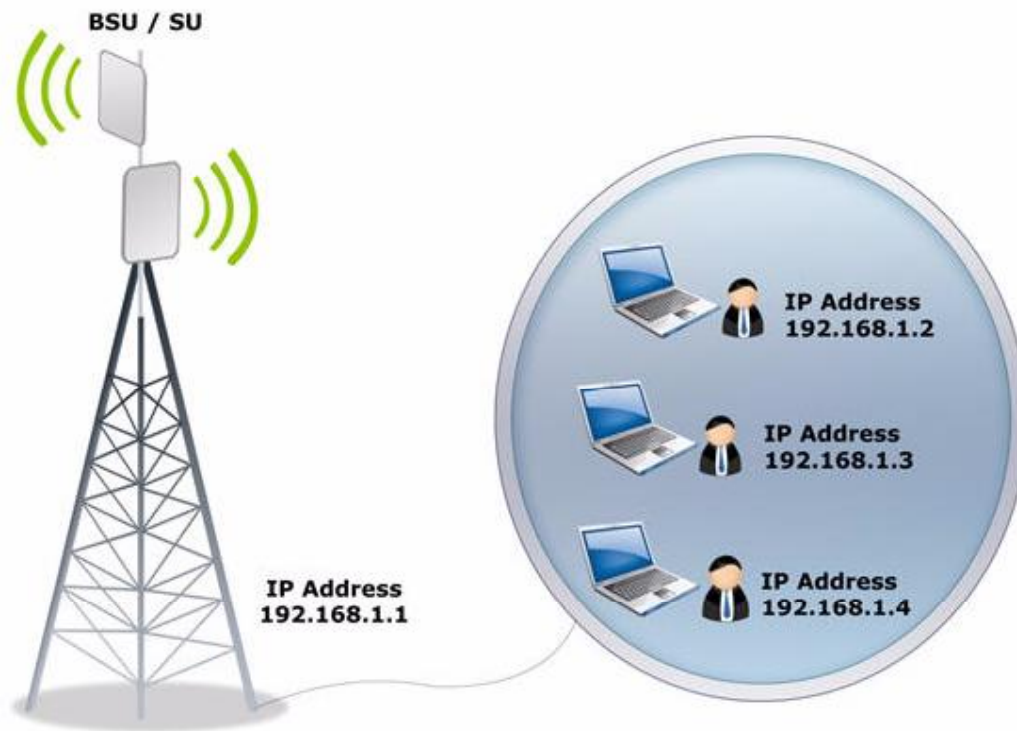


Figure 4-25 DHCP

4.8.1 DHCP server

DHCP automatically allocates network addresses and also delivers configuration parameters dynamically to the clients from the DHCP server. When DHCP server is enabled, it allows allocation of IP addresses to clients connected to the SU.

The DHCP Server lets the SU respond to DHCP requests with the following information:

- Host IP address
- Gateway IP address
- Subnet Mask
- Lease Time
- DNS Primary Server IP address
- DNS Secondary Server IP address

In Routing mode, DHCP Server can be configured for each interface separately. Unless the DHCP Server functionality is enabled for an interface, the DHCP Server does not respond to the DHCP requests received on that interface.

NOTE: The DHCP Server functionality is available in both **Routing** and **Bridge Modes**.

To configure the DHCP server and DHCP Interface table

1. Click **ADVANCED Configuration > DHCP > DHCP Server > Interfaces**. The **DHCP** screen appears as shown below.

DHCP Server

DHCP Server Status: Disable Enable

Max Lease Time: 86400 (in Secs)

DHCP Interface Table

S.No.	Interface	Net Mask	Default Gateway	Primary DNS	Secondary DNS	Default Lease Time	Comment	Entry Status
1	Bridge	255.255.255.0	169.254.128.1	0.0.0.0	0.0.0.0	86400		Disable ▼

Notes :

1. To enable DHCP Server on the device, at least one interface must be enabled in the DHCP Interface Table.
2. To enable DHCP Server on an interface at least one pool must be configured for it.
3. When DHCP Server is enabled DHCP Relay is disabled automatically.
4. Default Lease time must be with in the range 3600 Seconds(Min) - 172800 Seconds(Max).

OK

Figure 4-26 DHCP

2. Enter the appropriate parameters in the DHCP Interface Table. See the following table that lists the parameters and their descriptions.

NOTE: To enable the DHCP Server Interface, the DHCP server pool table should have at least one range configured for that interface.

Parameter	Description
Interface Type	Specifies the interface for which the DHCP Server functionality shall be configured.
Net Mask	Specifies the subnet mask to be sent to the client along with the assigned IP address. The netmask configured here should be greater than or equal to the netmask configured on the interface.
Default Gateway	Specifies the default gateway to be sent to the client along with assigned IP Address. Default Gateway is a node that serves as an accessing point to another network.
Primary DNS	Specifies the primary DNS (Domain Name Server) IP address to be sent to the client.
Secondary DNS	Specifies the secondary DNS IP address to be sent to the client.
Default Lease Time	DHCP Server uses this option to specify the lease time it is willing to offer to the client over that interface.
Comment	Specifies a note for the device administrator.

Parameter	Description
Entry Status	Used to enable or disable the DHCP server functionality over the interface.

- To enable DHCP Server, select **Enable** for DHCP Server Status. Before enabling, in interface table there should be at least one interface enabled on which the DHCP Server has to run and the DHCP server pool table should have at least one entry configured for that interface.
- In the **Max Lease Time** field, enter the maximum lease time.

Parameter	Description
DHCP Status	This parameter is used to enable DHCP Server or disable the DHCP functionality on the device.
Max Lease Time	Specifies the maximum lease time for which the DHCP client can have the IP address provided by the Server. The value ranges from 3600-86400 seconds.

- Click **OK**.
- To apply the configured properties of the device, click **COMMIT**.

NOTE: For DHCP Server to be enabled on an interface, at least one address pool must be configured for that interface.

4.8.1.1 DHCP Pool

To configure DHCP Pool

- Click **ADVANCED CONFIGURATION > DHCP > DHCP Server > Pool**. The DHCP Pool screen appears as shown below.

S.No.	Interface	Start IP Address	End IP Address	Delete
1	Bridge	10.0.0.1	10.0.0.10	Delete

OK Add

Figure 4-27 DHCP Pool

Parameter	Description
Interface	Specifies the interface to which the pool belongs.
Start IP Address/End IP Address	Specifies the start and end IP Address of the pool.
Delete	Allows the user to delete the added pool entry.

NOTE: Up to 5 entries per interface can be added in the IP Pool Table. A pool entry can be deleted but cannot be edited.

4.8.1.2 Adding a New Pool Entry

To add a new Pool entry to the DHCP server

1. Click **Add** in the DHCP Pool screen. The **DHCP Pool Table Add Row** screen is displayed as shown below.

DHCP Pool Table Add Row	
Pool Interface	Bridge
Start IP Address	10.0.0.1
End IP Address	10.0.0.10
Entry Status	Enable
<input type="button" value="Add"/> <input type="button" value="Back"/>	

Figure 4-28 DHCP Pool Table Add Row

2. After entering the details, click **Add**. The entry will be updated in the DHCP pool table.
3. To apply the changes, click **COMMIT**.

4.8.2 DHCP Relay (Routing Mode only)

The DHCP relay agent forwards DHCP requests to the given DHCP server. There must be at least one entry in the corresponding Server IP Address table to enable the DHCP Relay Agent. A maximum of 5 servers can be configured. To enable the DHCP Relay functionality, set the **DHCP Mode** to **DHCP Relay**.

NOTE: DHCP Relay Agent parameters are configurable only in Routing mode. It cannot be enabled when NAT or DHCP Server are enabled.

To view entries in DHCP Relay Server

- Click **ADVANCED CONFIGURATION > DHCP > DHCP Relay > Relay Server**.

DHCP Relay

DHCP Relay Status Disable Enable

DHCP Relay Server Table

S.No.	IP Address	Delete
1	10.0.0.100	Delete

Notes : 1. To enable DHCP Relay on the device, at least one IP Address must be configured in the DHCP Relay Server Table.
2. When DHCP Relay is enabled DHCP Server is disabled automatically.

OK Add

Figure 4-29 DHCP Relay

To add Relay Server Table entry,

1. Click **ADVANCED CONFIGURATION > DHCP > DHCP Relay > Relay Server**.
2. Click **Add** in the DHCP Relay Server screen. The **DHCP Relay Server Add Row** screen is displayed as shown below.

DHCP Relay Server Add Row

Server IP Address 10.0.0.100

Entry Status Enable

Add Back

Figure 4-30 DHCP Relay Server Add Row

3. Enter the Server IP Address and then click **Add**.
4. To enable DHCP Relay, click **Enable** for DHCP Relay Status. Before enabling, there must be at least one IP address configured in the DHCP Relay Server Table.
5. Click **OK**. To apply the changes, click **COMMIT**.

NOTE: To enable the DHCP Relay, the NAT functionality must be disabled.

4.9 Routing Features Configuration

4.9.1 Static Route Table (Routing Mode Only)

The static routing table mechanism is available for the SU in routing mode only. It stores the route to various destinations on the network. When packets are to be routed, the routing table is referred to for the destination address.

S.No.	Destination Address	Subnet Mask	Route Next Hop	Admin Metric	Entry Status
1	10.0.0.5	255.255.255.255	169.254.130.12	5	Enable
2	10.0.0.2	255.255.255.255	169.254.130.12	5	Enable

Figure 4-31 NetIp Static Route Table

To set the static routing table

1. Click **ADVANCED CONFIGURATION > Network > Static Route Table**.
2. Enter the appropriate parameters. See the following table that lists the parameters and their descriptions.
3. Click **Add** to add a new entry in the table.

Parameter	Description
Route Status	This parameter is used to enable or disable the static Route Status . This parameter is applicable to all static routes.
Destination Address	Specifies the destination IP address for which the static route is to be made.
Route Mask	Specifies the subnet mask of the destination IP address.
Route Next Hop	Specifies the next hop IP Address through which route is available to the destination IP address. Next hop IP should belong to at least one of the subnets connected to the device.
Metric	It is a metric that specifies the distance to the target usually counted in hops. The priority is given to this route relative to others. It can range from 0 – 16.
Entry Status	This parameter is used to configure the status of the static route. Only enabled routes are considered for routing the packets.

4.9.1.1 Adding Static Route Entries

To add Static Route entries,

1. Click **Add** in the Static Route Table screen. The **Static Route Table Add Row** screen is displayed as shown below.

Static Route Table Add Row	
Destination Address	<input type="text" value="10.0.0.2"/>
Subnet Mask	<input type="text" value="255.255.255.255"/>
Route Next Hop	<input type="text" value="189.254.130.12"/>
Metric	<input type="text" value="5"/>
Entry Status	<input type="text" value="Enable"/> <input type="button" value="v"/>
<input type="button" value="Add"/> <input type="button" value="Back"/>	

Figure 4-32 Static Route Table Add Row

2. After adding the entry into the Static Route table, click **Add**.
3. Click **COMMIT** for the changes to take effect.

NOTE:

- Maximum 256 entries can be added to the static route table.
- While adding a new entry, the IP address of the Next Hop must be on the subnet of one of the device's network interfaces.

4.9.2 NAT (SU, Routing Mode Only)

The NAT (Network Address Translation) feature allows hosts on the Ethernet side of the SU to transparently access the public network through the BSU. All the hosts in the private network can have simultaneous access to the public network.

The SU supports NAPT (Network Address Port Translation) where all private IP addresses are mapped to a single public IP address and does not support Basic NAT (where private IP addresses are mapped to a pool of public IP addresses).

Both **dynamic mapping** (allowing private hosts to access hosts in the public network) and **static mapping** (allowing public hosts to access hosts in the private network) are supported.

1. **Static NAT:** Static mapping is used to provide inbound access. The SU maps the public IP address and its transport identifiers to the private IP address (local host address) in the local network. This is used to provide inbound access to a local server for hosts in the public network. Static port mapping allows only one server of a particular type. Up to 100 entries are supported in the static port bind table.
2. **Dynamic NAT:** In dynamic mapping, the SU maps the private IP addresses and its transport identifiers to transport identifiers of a single Public IP address as they originate sessions to the public network. This is used only for outbound access.

NOTE:

- When NAT is enabled, the network on the wireless side of the device is considered Public and the network on the Ethernet side are considered Private.

- When NAT functionality is enabled, the DHCP Relay and RIP features are not supported. The **DHCP Relay Agent** and **RIP** must be disabled before enabling NAT.

To set the NAT parameters,

1. Click **ADVANCED CONFIGURATION > Network > NAT**. The NAT screen appears as shown below.

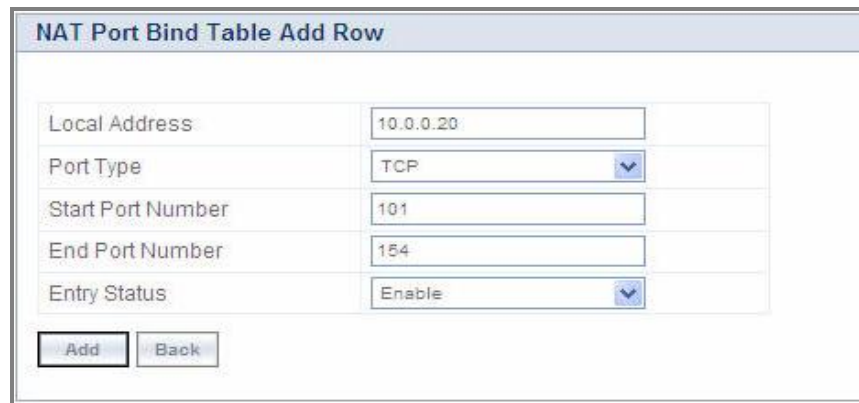
Figure 4-33 NAT

2. Enter the appropriate parameters. See the following table that lists the parameters and their descriptions.
3. Click **OK**.

Field	Description
Status	This parameter is used to enable or disable NAT feature.
Port Binding status	This parameter is used to enable or disable the Static NAT feature within different networks. It allows public hosts to access hosts in a private network. By default, it is disabled.

NOTE:

- To enable **Dynamic NAT**, set the **NAT Status** to **Enable**. To enable **Static NAT**, set the **NAT Status** to **Enable** and the **Port Binding Status** to **Enable**.
- NAT feature is available for SU in the routing mode only.
- Any change in the parameters requires a reboot.
- The NAT feature uses the IP address of the wireless interface as the Public IP address.



NAT Port Bind Table Add Row	
Local Address	10.0.0.20
Port Type	TCP
Start Port Number	101
End Port Number	154
Entry Status	Enable

Figure 4-34 NAT Port Bind Table Add Row

To add entries in the NAT static port bind table

1. Enter the Local IP Address of the host on the Ethernet (private) side of the SU.
2. Select the Port Type as: TCP, UDP, or Both.
3. Enter the Start Port, End Port and enable the Entry Status.
4. Click **Add**.
5. After adding the entry into the Static Port Bind Table, click **COMMIT** and then click **REBOOT** for the changes to take effect.

4.9.2.1 Supported Session Protocols

Certain applications require an Application Level Gateway (ALG) to provide the required transparency for an application running on a host in a private network to connect to its counterpart running on a host in the public network. An ALG may interact with NAT to set up state information, use NAT state information, modify application-specific payload, and perform the tasks necessary to get the application running across address realms.

No more than one server of a particular type is supported within the private network behind the SU. Following is the list of supported protocols with their corresponding default ALG's:

S.No.	Protocol	Support	Applications
1	H.323	H.323 ALG	Multimedia Conferencing
2	HTTP	Port Mapping for inbound connection	Web Browser
3	TFTP	Port Mapping for inbound connection	Trivial file transfer
4	Telnet	Port Mapping for inbound connection	Remote login
5	IRC	Port Mapping for inbound connection	Chat and file transfer
6	AMANDA	Port Mapping for inbound connection	Backup and archiving
7	FTP	FTP ALG	File Transfer
8	PPTP	PPTP ALG	VPN related
9	NETBIOS	Port Mapping for inbound connection	Applications on different computers can communicate within a LAN
10	SNMP	SNMP ALG	Network Management
11	DNS	Port Mapping for inbound connection	Domain Name Service

4.9.3 RIP (Routing Mode Only)

Routing Information Protocol (RIP) is a dynamic routing protocol, which can be used to automatically propagate routing table information between routers. The unit can be configured in RIPv1, RIPv2, or both while operating in Routing mode.

When a router receives a routing update including changes to an entry, it updates its routing table to reflect the new route. RIP maintains only the best route to a destination. Therefore, whenever new information provides a better route, the old route information is replaced.

NOTE: RIP is configurable only when the unit is in Routing Mode and Network Address Translation (**NAT**) is disabled.

To enable RIP functionality

- Enable RIP status from the drop-down menu. RIP runs on per interface basis.

To configure RIP parameters

1. Click **ADVANCED CONFIGURATION > Network > RIP**. The RIP screen is displayed as shown below.

RIP

RIP Status:

S.No.	Name	Status	Authorization Type	Authorization Key	Version Number	Direction
1	Ethernet 1	Enable	Simple	Both	Rx only
2	Wireless 1	Disable	md5	V2	Rx and Tx

Notes:

- To enable RIP, NAT must be disabled.
- Auth. Type & Key are valid for V2 version only
- If Auth. Type is "None" Auth. Key is ignored.

OK

Figure 4-35 Configuring RIP

- Enter the appropriate parameters. See the following table that lists the parameters and their descriptions.
- Click **OK**.
- Click **COMMIT** for the changes to take effect.

Parameter	Description
Name	Displays the name of the interface as Ethernet1 or Wireless.
Status	This parameter is used to enable or disable RIP for that particular network interface.
Authorization Type	Select the appropriate authorization type. This parameter is not applicable if RIP v1 is selected as the Version number .
Authorization Key	Enter the authorization key. This parameter is not applicable if RIP v1 is selected as the Version number .
Version Number	Select RIP Version number from the Version Number list. Available options are V1 , V2 and both . The default is V2 .
Direction	Specifies whether RIP is enabled for Receive only or for both Receive and Transmit.

NOTE:

- Authorization Type** and **Authorization Key** are valid only for RIPV2 and both versions.

- *The maximum metric of a RIP network is 15 hops, i.e., a maximum of 15 routers can be traversed between a source and destination network before a network is considered unreachable.*
- *By default, a RIP router will broadcast/multicast its complete routing table for every 30 seconds, regardless of whether anything has changed.*
- *RIP supports the split horizon, poison reverse and triggered update mechanisms to prevent incorrect routing updates being propagated.*

System Management

This chapter provides details about the Management screen of the Web interface and describes the procedures to effectively manage the Tsunami MP-8150-CPE device.

It covers the following topics:

- [System](#)
- [File Management](#)
- [Services: Configuring the Passwords](#)
- [SNTP](#)
- [Access Control](#)
- [Reset to Factory](#)

5.1 System

5.1.1 System Information

This section displays the basic system information. This information further helps in viewing the device details during troubleshooting. For configuring the system information, click **MANAGEMENT > System > Information**.

System Information	
System Up-Time	00:00:09:17 (dd:hh:mm:ss)
System Description	MP-8150-CPE-WD-v1.0.1(208143)
System Name	System Name (0-64) characters
Email	name@Organization.com
Phone Number	Contact Phone Number
Location	System Location
GPS Longitude	-121.8893
GPS Latitude	37.3321
GPS Altitude	10

OK

Figure 5-1 System Information

Parameter	Description
System Up-Time	Specifies the duration of the device running time, since its last reboot.
System Description	Specifies the description of the system. It reports the device name, current firmware and build number.
System Name	Specifies the system name for easy identification of the SU. The System Name parameter is limited to a length of 64 characters. Use the System Name of an BSU to configure the BSU Name parameter on an SU if you want the SU to register only with this BSU. If the BSU Name is left blank on the SU, it can register with any BSU that has a matching Network Name and Network Secret.

Parameter	Description
Email	Specifies the Email address of the concerned person responsible for the device. The Email parameter is limited to a length of 32 characters.
Phone Number	Specifies the Phone number of the concerned person responsible for the device. The Phone Number parameter is limited to a length of 32 characters.
Location	Specifies the location of the device. This parameter is limited to a length of 64 characters.
GPS Longitude, GPS Latitude and GPS Altitude	Specifies the GPS longitude, latitude and altitude at which the device is installed. These parameters are limited to a length of 64 characters.

After setting the system information, click **COMMIT** for the changes to take effect in the device.

5.1.2 Identifying the Components (Inventory Management)

Inventory management provides complete component information of the device. This section describes the version history of each component.

To view the details of inventory components, click **MANAGEMENT > System > Inventory Management**.

System Inventory Management Table							
S.No.	Number	Name	Comp ID	Variant ID	Release Version	Major Version	Minor Version
1	BUILD-360	Wireless Card 1 -NIC (0x60)	2300	1	7	0	0
2	207200	Application Software Image	2103	1	1	0	0
3	SN000	Hardware Inventory	2001	1	1	0	0
4	-NA-	BSP-Bootloader	2107	1	1	0	0
5	-NA-	Enterprise MIB	2200	1	2	0	0
6	-NA-	Config File	2201	1	2	0	0
7	-NA-	License File	2203	2	2	0	0
8	-NA-	Daughter Card	2011	1	1	0	0

Refresh

Figure 5-2 Inventory Management

By default, the components information is auto-generated by the device. This information is standard and is used only for reference purpose.

5.1.3 Viewing Licensed Features

Licensing is considered to be the most important component of an enterprise class device which typically has a feature-based pricing model. It is also required to prevent the misuse and tampering by a wide variety of audience whose motives may be intentional or accidental.

Licensed Features are, by default, set by the company. To view the licensed features, click **MANAGEMENT > System > Licensed Features**. Refer to the parameter description given in the following table:

Licensed Features	
Product Description	= MP-8150-CPE-WD
Number of Radios	= 1
Number of Ethernet Interfaces	= 1
Radio 1 Allowed Frequency Band	= 5 GHz
Maximum Output Bandwidth	= 2 Mbps
Maximum Input Bandwidth	= 23 Mbps
Maximum Aggregate Bandwidth	= 25 Mbps
Product Family	= Tsunami MP-8100
Product Class	= Outdoor
Maximum SUs Allowed	= 100
Allowed Operations Modes of Radio 1	= SU

Figure 5-3 Licensed features

Parameter	Description
Product Description	Specifies the product description.
Number of Radios	Specifies the number of radios that the device is licensed to operate.
Number of Ethernet Interfaces	Specifies the number of Ethernet interfaces that the device is licensed to operate.
Radio 1 Allowed Frequency Band	Specifies the wireless operational frequency band supported by the device.
Maximum Output Bandwidth	Specifies the Maximum output bandwidth limit in multiples of 1Mbps (Refer to Note below).
Maximum Input Bandwidth	Specifies the Maximum output bandwidth limit in multiples of 1Mbps (Refer to Note below).
Maximum Aggregate Bandwidth	Specifies the Max cumulative bandwidth of the device which is the sum of configured output and input.

Parameter	Description
Product Family	Specifies the Product Family of the device.
Product Class	Specifies the Product Class of the device. It can be indoor or outdoor product based on this parameter.
Maximum SUs Allowed	Specifies the maximum number subscriber units allowed.
Allowed Operational Modes of Radio1	Specifies the device operational mode as SU.

NOTE: The Input and Output Bandwidth features are referred with respect to the wireless interface. That is, input bandwidth refers to the data received on the wireless interface and output bandwidth refers to the data sent out of the wireless interface.

5.2 File Management

Using this section, you can upgrade the firmware or configuration of the device and also retrieve the log/configuration files from the device. File Management can be done using TFTP (by using an external TFTP Server) using Web, CLI or SNMP. It can also be done using the HTTP using Web Interface.

5.2.1 Upgrade Firmware via HTTP

For upgrading the firmware via HTTP web interface, click **MANAGEMENT > File Management > Upgrade Firmware > HTTP**.

Figure 5-4 HTTP Upgrade Firmware

Steps to upgrade the firmware via HTTP

1. Click **Browse** and locate the firmware file.
2. Click **Update** to initiate the HTTP Update operation.

A confirmation message prompts you that a reboot of the device is required for changes to take effect. Click **OK**.

NOTE:

- After upgrading new firmware, the device must be rebooted. Until a reboot occurs, the device will continue to run the firmware it was using before the upgrade started.
- If the user navigates to another page before upgradation is complete, the user may not be able to use the eventlog/syslog to confirm the status of update.

5.2.2 Upgrade Configuration via HTTP

For updating the configuration via HTTP web interface, click **MANAGEMENT > File Management > Upgrade Configuration > HTTP**.

Figure 5-5 HTTP Update-Configuration

To upgrade the configuration via HTTP

1. Click **Browse** and locate the configuration file.
2. Click **Update** to initiate the HTTP Update operation.

NOTE: After upgrading new configuration, the device must be rebooted.

5.2.3 Upgrade Firmware via TFTP

Using TFTP, the device can be upgraded with new firmware or configuration file. Also it can be used to retrieve the configuration or log files from the device.

To upgrade the firmware via TFTP Server, click **MANAGEMENT > File Management > Upgrade Firmware > TFTP**.

Upgrade Firmware

HTTP **TFTP**

Server IP Address: 169.254.128.133

File Name: image.bin

Notes: Please don't navigate away from this page when the update in progress.

Update

Update & Reboot

Figure 5-6 Upgrade Firmware-TFTP To upgrade the firmware via TFTP server:

1. Enter the TFTP Server IP Address.
2. Enter the name of the firmware file to update to the device.
3. Click **Update** to initiate the new firmware updation or click **Update and Reboot** to update and reboot with new firmware immediately.

5.2.4 Upgrade Configuration via TFTP

For upgrading the configuration via TFTP Server, click **MANAGEMENT > File Management > Upgrade Configuration > TFTP**.

Upgrade Configuration

HTTP **TFTP**

Server IP Address: 169.254.128.133

File Name: image.bin

Notes : 1. After Upgrading the configuration, Reboot is required to work with new upgraded configuration.
2. Please don't Navigate away from this page when the update in progress.

Update

Update & Reboot

Figure 5-7 Upgrade Configuration via TFTP

To upgrade the configuration via TFTP server,

1. Enter the TFTP Server IP Address.
2. Enter the name of the configuration file to be updated to the device.
3. Click **Update** to initiate the TFTP update operation or click **Update and Reboot** to update and reboot with new configuration immediately.

5.2.5 Retrieve From Device

5.2.5.1 HTTP Retrieve

For retrieving a configuration file or Event log file via HTTP web interface, click **MANAGEMENT > File Management > Retrieve From Device > HTTP**.

To retrieve files from the device via HTTP

1. From the **File Type** list, select the type of file to retrieve.
 - a. **Config**: To retrieve the configuration file from the device.
 - b. **Event Log**: To retrieve the event log file from the device.
2. Click **Retrieve** to initiate the operation and retrieve the file to the local system.

The screenshot shows a web interface titled "Retrieve from Device". At the top, there are two tabs: "HTTP" (which is selected) and "TFTP". Below the tabs, there is a "File Type" label followed by a dropdown menu currently set to "Config". Below this, there is a red note with two points: "1. When the device is running with factory default settings there is no config file present and hence the config file cannot be retrieved." and "2. If the eventlog is not created or has been cleared, it cannot be retrieved." At the bottom left of the main content area, there is a "Retrieve" button.

Figure 5-8 HTTP Retrieve

5.2.5.2 TFTP Retrieve

This option is used to retrieve files from the device to the TFTP server. The TFTP server must be running and configured in the desired directory path to copy the retrieved file. Assign a proper name to the file which may include version or location information.

Retrieve from Device

HTTP

TFTP

Server IP Address	<input type="text" value="169.254.128.133"/>
File Name	<input type="text" value="image.bin"/>
File Type	<input style="border: none; border-bottom: 1px solid #ccc; background-color: #e0e0e0; width: 100%;" type="text" value="Event Log"/>

Note: 1. When the device is running with factory default settings there is no config file present and hence the config file cannot be retrieved.
2. If the eventlog is not created or has been cleared, it cannot be retrieved.

Figure 5-9 TFTP Retrieve

For retrieving a configuration file or Event log file via TFTP web interface, click **MANAGEMENT > File Management > Retrieve From Device > TFTP**.

To retrieve files from the device via TFTP Server

1. Enter the TFTP Server IP address.
2. Enter the name of the file to be downloaded to the device.
3. Select the type of file to upgrade from the **File Type** list:
 - a. **Config**: To retrieve the configuration file from the device.
 - b. **Event Log**: To retrieve the event log file from the device.
4. Click **Retrieve** to initiate the operation and retrieve the file to the TFTP Server.

NOTE: If the device is in default configuration, there will be no config file to upload. Similarly, Event Log cannot be uploaded if there is no Event Log created on the device.

5.3 Services: Configuring the Passwords

SNMP version, SNMP passwords, and SNMP Trap Host Table parameters can be configured to prevent unauthorized access. Each management interface can be configured with its own password. Each of the three management interfaces (HTTP/HTTPS, Telnet/SSH, and SNMP) is arranged in tabs under the **Services** link of **MANAGEMENT** tab in the Main Left Panel.

The following special characters are not allowed for setting passwords for Telnet/SSH, HTTP/HTTPS, and SNMP v2/v3: **& / \ ' " =? &** and blank space.

NOTE: The passwords in the Services screen are configurable.

5.3.1 HTTP/HTTPS

The screenshot shows a configuration window titled "Services" with four tabs: "HTTP / HTTPS", "Telnet / SSH", "SNMP", and "SYSLOG Host Table". The "HTTP / HTTPS" tab is selected. It contains the following fields:

- Password:** A text input field with masked characters (dots) and a range indicator "(6-32) *".
- HTTP:** A dropdown menu set to "Enable" with a red asterisk.
- HTTP Port:** A text input field containing "80" with a red asterisk.
- HTTPS:** A dropdown menu set to "Enable" with a red asterisk.

Below the fields, a note reads: "Notes: 1. For setting the password characters - = \ ' ' ? / space are not allowed. * Reboot is required". An "OK" button is located at the bottom left of the window.

Figure 5-10 HTTP/HTTPS

The parameters for HTTP/HTTPS are described in the following table.

Parameter	Description
Password	Set a new password for the interface or interfaces (Ethernet/Wireless) to manage the device through the Web interface. Enter a password between 6 and 32 characters in the Password field. The default password is " public ".
HTTP	Select Enable to allow HTTP access to the device from any host. You can also select Disable to prevent access to the device from Web interface. Similar settings are applicable for Hypertext Transfer Protocol over Secure Socket Layer or HTTPS.
HTTP Port	Specifies the port number for HTTP interface. By default, the port number is 80.
HTTPS	Similar settings as mentioned for HTTP. The password configuration for HTTPS is same as configured for HTTP.

5.3.2 Telnet/SSH

Services

HTTP / HTTPS
Telnet / SSH
SNMP
SYSLOG Host Table

Password	<input type="password" value="....."/>	(6-32) *
Telnet	<input type="button" value="Enable"/>	*
Telnet Port	<input type="text" value="23"/>	*
Telnet Sessions	<input type="text" value="1"/>	(0-3) *
SSH	<input type="button" value="Enable"/>	*
SSH Port	<input type="text" value="22"/>	*
SSH Sessions	<input type="text" value="2"/>	(0-3) *

Notes: 1. For setting the password characters - = \ " ' ? / space are not allowed.
 2. The sum of Telnet and SSH sessions cannot be more than 3.

* Reboot is required

Figure 5-11 Telnet/SSH

The parameters for Telnet/SSH are described in the following table.

Telnet/SSH Parameter settings	
Password	Set a new password for the interface or interfaces to manage the device through the CLI. The same password is used for serial CLI also.
Telnet	Select Enable to allow the Telnet access to the device from any host. You can also select Disable to prevent a user from accessing the device from the CLI. Similar settings are applicable for Secure Shell or SSH.
Telnet Port	Specifies the port number for Telnet interface. By default, the port number is 23.
Telnet Sessions	Specifies the number of Telnet sessions which controls the number of active Telnet connections. By default, the number of telnet sessions allowed is 1.
SSH	Select Enable to enable SSH access to the device from any host or select Disable to prevent a user from accessing the device.
SSH Port	Enter the port number for Secure Shell port for CLI interface. By default, the port number is 22.

SSH Sessions	<p>Enter the number of SSH sessions. By default, it is 2 sessions.</p> <p>NOTE: Total number of CLI sessions allowed is 3, so the sum of Telnet and SSH sessions cannot be more than 3. For example, if you configure the number of Telnet sessions as 2, then the number of SSH sessions can only be a value from 0 to 1.</p>
---------------------	---

5.3.3 SNMP

Services

HTTP / HTTPS
Telnet / SSH
SNMP
SYSLOG Host Table

SNMP	Enable <input type="button" value="v"/>	(Ref Note) *
Version	SNMPv1-v2c <input type="button" value="v"/>	*
Read Password	(6-32) *
Read/Write Password	(6-32) *
Security Level	None <input type="button" value="v"/>	*
Priv Protocol	None <input type="button" value="v"/>	*
Priv Password	(8-32) *	
Auth Protocol	None <input type="button" value="v"/>	*
Auth Password	(8-32) *

SNMP Trap Host Table *

S.No.	IP Address	Password	Comment	Entry Status
1	169.254.128.13	Default	Enable <input type="button" value="v"/>

Notes: 1. Change in SNMP Status will effect the NMS Access
 2. For setting the password characters - = \ " ' ? / space are not allowed.
 * Reboot is required

Figure 5-12 SNMP

The parameters for SNMP are described in the following table.

SNMP Parameter settings	
SNMP	This parameter provides the access control for the SNMP interface. Select Enable/Disable to enable or disable the SNMP access to the device from any host. Disabling the SNMP will affect the NMS/PVES access to the device.
Version	This parameter configures the SNMP version. The available versions are v1-v2 and v3. By default, the SNMP starts in version v2c. On selecting SNMP v1-v2c, the following parameters need to be configured. Please refer to the <i>Tsunami MP-8150-CPE Reference Manual</i> for SNMPv1-v2c Configuration.
Read Password	This parameter represents the read only community name used in SNMP Protocol. It is sent along with each SNMP GET / WALK / GETNEXT / GETBULK request to allow or deny access to the device. This password should be same as read password set at the NMS or MIB browser. The default password is "public" and range of this parameter must be between 6-32 characters.
Read/Write Password	This parameter represents the read-write community name used in SNMP Protocol. It is sent along with each SNMP GET / WALK / GETNEXT / SET request to allow or deny access to the device. This password should be same as read-write password set at the NMS or MIB browser. The default password is "public" and range of this parameter must be between 6-32 characters.

5.3.3.1 SNMPv3 Configuration

On selecting SNMP V3, the following parameters need to be configured:

SNMP V3 Parameter settings	
Security level	The supported security levels for MP-8150-CPE is AuthNoPriv and AuthPriv . Select AuthNoPriv for Extensible Authentication or AuthPriv for both Authentication and Privacy (Encryption).
Priv Protocol	This field configures the type of privacy (or encryption) protocol. This parameter is available only when the security level is AuthPriv . Select the encryption standard either AES-128 (Advanced Encryption Standard) or DES (Data Encryption Standard) from the list. The default Priv Protocol is AES-128.
Priv Password	This field configures the pass key for Privacy protocol selected. This parameter is available only when the security level is AuthPriv . The default password is public123 and range of this field must be between 8-32 characters.
Auth Protocol	This field configures the type of Authentication protocol. Select the encryption standard either SHA (Secure Hash Algorithm) or MD5 (Message-Digest algorithm) from the list. The default Auth Protocol is DES .

Auth Password	<p>This configures the pass key for Privacy protocol selected. The default password is public123 and range of this field must be between 8-32 characters.</p> <p>The default user in SNMPv3 is "admin" has all read-write privileges and only one user is supported.</p> <p>If SNMPv3 is enabled, the v3 stats can be seen in the MONITOR > SNMPv3 stats page.</p> <p>The option "None" in Security Level, Auth Protocol and Priv Protocol is present to support the parameters in lower versions and is not allowed to configure by the user.</p>
---------------	--

5.3.3.2 SNMP Trap Host Table

This table contains the list of IP addresses where the SNMP traps will be delivered. It supports maximum 5 rows.

Adding Entries to the Trap Host Table

To add entries to the Trap Host Table

1. Click **Add** to add Table Entries to the Trap Host Table.

Figure 5-13 SNMP Host Table Add Row

2. Enter the IP Address, Password, and Comment.
3. Select the entry status as **Enable** or **Disable** and click **Add**.

All traps will be delivered to the host port number 162. The community string/ password field is not valid if the device is configured in SNMPv3 mode.

NOTE: Changes to SNMP parameters require a Reboot to take effect.

5.3.4 System Log Host Table

System log messages are generated by the system by sending requests at various instances to the system log server. The priority with which the messages are to be logged from the configured instance can be reconfigured by selecting a desired priority from the **Log Priority** drop-down menu. These system log details are lost on system reboot. System message logging can be disabled if needed.

NOTE: When a particular priority is selected, the messages with a priority higher than the value selected will also be logged. Change of priority does not change the priority of the messages already logged but only specifies the priority of future messages to be logged.

To configure the System Log settings

1. Select a **Log Status** from the drop-down list.
2. Select a required Log Priority from the drop-down list: **Emergency, Alert, Critical, Error, Warning, Notice, Info or Debug.**
3. Click **OK.**

The screenshot shows the 'Services' configuration page with the 'SYSLOG Host Table' tab selected. The 'Log Status' is set to 'Enable' and 'Log Priority' is set to 'Critical'. Below this, a table lists the configured host entries:

S.No.	IP Address	Port	Host Comment	Entry Status
1	10.0.0.5	50000	TEST_CASE	Enable

Buttons for 'OK' and 'Add' are located at the bottom left of the configuration area.

Figure 5-14 Syslog Host Table

To add entries to the System Log Host Table

1. Click **Add** to display **SYSLOG Host Table Add Row** page.
2. Enter the parameters listed in the following table.
3. Click **Add.**

The screenshot shows the 'SYSLOG Host Table Add Row' page with the following input fields:

IP Address	10.0.0.5
Host Port	50000 (0-65535)
Comment	TEST_CASE

Buttons for 'Add' and 'Back' are located at the bottom left of the form.

Figure 5-15 SYSLOG Host Table Add Row

Parameter	Description
IP Address	Represents the IP address of the SYSLOG server.
Port	Represents the host port number. Default port is 514.
Host Comment	Used to provide a note for the device administrator.
Entry Status	Used to configure the status of the Syslog host entry table.

5.4 SNTP

SNTP allows a network entity to communicate with time servers in the network/Internet to retrieve and synchronize the time of day information. When this feature is enabled, the system attempts to retrieve the time of day information from the configured time servers (primary or secondary); and when successful, it updates the relevant time objects in the system.

Figure 5-16 SNTP

To configure and view parameters within the SNTP screen

1. Click **MANAGEMENT > SNTP**.
2. Select the **Enable SNTP Status** checkbox. The selected status determines which of the parameters on the SNTP page are configurable.
3. Enter the parameters listed the following table.
4. Click **OK**.
5. Click **COMMIT** for the changes to take effect.

Parameter	Description
Primary Server IP Address/Domain Name	Specifies the host name or the IP address of the primary SNTP server. Either a domain name or an IP address can be provided.

Parameter	Description
Secondary Server IP Address/Domain Name	This optional parameter specifies the host name or an IP address of the secondary SNTP server.
Time Zone	This parameter specifies the time zone set for the SNTP.
Day Light Saving Time	Specifies the number of hours adjusted for Daylight Saving Time.
Current Date/Time	Displays current date and time. If SNTP is not enabled, the current date and time are automatically generated from the local system. If SNTP is enabled, it displays the time the device has got from the SNTP server.

NOTE:

- Provide the Primary and Secondary Server details only if the SNTP status is enabled.
- For any reason, if the servers configured are not responding, the SNTP client retries every minute.

5.5 Access Control

The Management Access Control feature provides the option of controlling the management interfaces only from the specified hosts. The user needs to update the table with an IP address, which provides access to management interfaces, such as SNMP, HTTP, HTTPS, TELNET, and SSH.

To view and configure the **Access Table Status** and **Management Access Control Table**, click **MANAGEMENT > Access Control**.

Management Access Control Table

Access Table Status: Enable

S.No.	IP Address	Entry Status
1	10.0.0.5	Enable

Note : Changes to these parameters will require a reboot to take effect.

OK Add

Figure 5-17 Management Access Control Table

Parameter	Description
Access Table Status	Enable or disable the Management Access Control Table status. By default, it is disabled.
IP Address	Specifies the IP Address of the machine to which the management traffic needs to be allowed.
Entry Status	Used to enable/disable a particular entry in the Management Access Table.

To add a new IP Address, follow these steps

1. Select **Enable** for the **Access Table Status**.
2. Click **Add** to display the **Management Access Table Add Row** page.

Figure 5-18 Management Access Table Add Row

3. Enter the IP Address of the device.
4. Select **Enable** or **Disable** for the Entry status of the device.
5. Click **Add**.

Ensure that the IP address of the management PC that is used to manage the device is present in the table. Otherwise, you will not be able to manage the device. If this case occurs, try to give the PC correct IP address for management; or else, the device can be configured via the CLI over the serial port.

5.6 Reset to Factory

Click **Reset to Factory** to reset the device to its factory default state. This resets the network configuration values, including the password, IP address, and subnet mask.

- Device will reboot automatically after clicking on the **Reset To Factory Defaults**. The device comes up with default configurations after reboot.

Figure 5-19

Monitoring the System

This chapter describes the procedures to monitor the Tsunami MP-8150-CPE using the **MONITOR** screen of the Web interface.

It covers the following topics:

- [Interface Statistics](#)
- [WORP Statistics](#)
- [Bridge](#)
- [Network Layer](#)
- [DHCP](#)
- [Logs](#)
- [Tools](#)
- [SNMP v3 Statistics](#)

NOTE: The MONITOR screen has **Refresh** and **Clear** buttons. Click **Refresh** to refresh the current page with the latest statistics. Click **Clear** to clear the current statistics.

6.1 Interface Statistics

Interface Statistics provides detailed information about the data exchanged in both directions through the device interface. The statistical information include the type of interface, operational status, MAC address of the protocol, number of packets transmitted, signal information, number of collisions and errors occurred while transmitting the data.

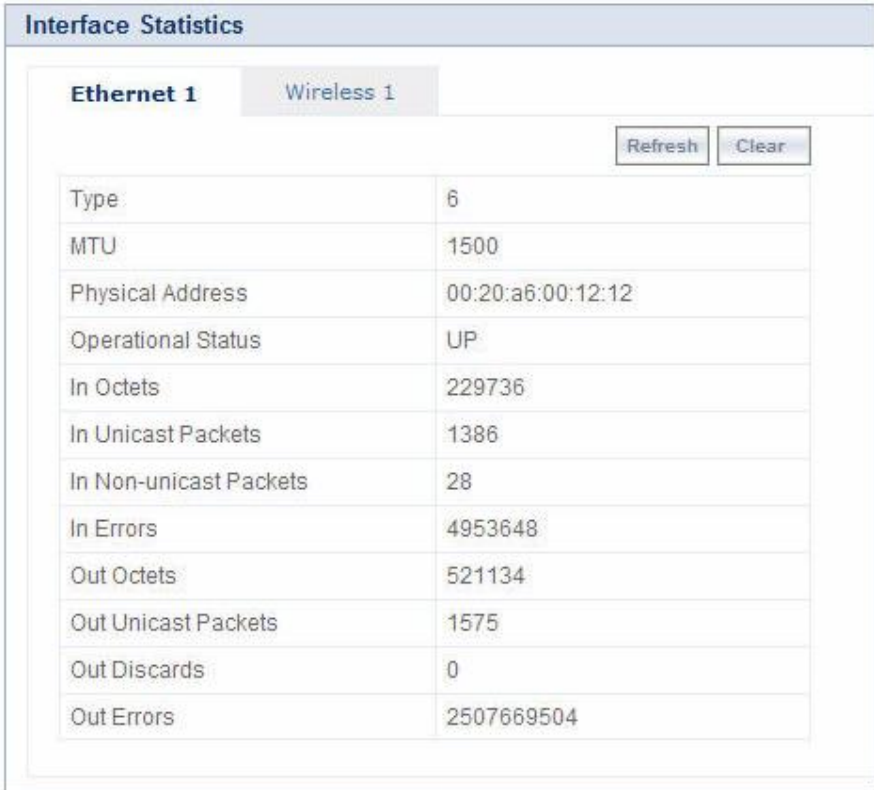
The main function of interface statistics is to monitor and record the status and performance of the ethernet and the wireless interfaces.

NOTE: For every 4 seconds, statistics pages get refreshed.

6.1.1 Ethernet Statistics

Ethernet Statistics provides you a collection of statistics generated by gathering the network traffic details. Using the statistics, you can track the number of transactions occurred through this interface.

To view the Ethernet Interface Statistics, click **MONITOR > Interface Statistics** and click Ethernet 1.



The screenshot shows the 'Interface Statistics' window with two tabs: 'Ethernet 1' (selected) and 'Wireless 1'. There are 'Refresh' and 'Clear' buttons in the top right. Below the tabs is a table of statistics for Ethernet 1.

Interface Statistics	
Ethernet 1	
Type	6
MTU	1500
Physical Address	00:20:a6:00:12:12
Operational Status	UP
In Octets	229736
In Unicast Packets	1386
In Non-unicast Packets	28
In Errors	4953648
Out Octets	521134
Out Unicast Packets	1575
Out Discards	0
Out Errors	2507669504

Figure 6-1 Ethernet Statistics

The parameters displayed in this page are explained in the following table.

Field	Description
Type	This parameter displays the type of interface. The interface type is differentiated based on the network layers.
MTU	This parameter displays to the largest size of the data packet received/sent on the interface.
Physical Address	This parameter displays the MAC address at the Ethernet protocol layer.
Operational Status	This parameter displays the current operational state of the interface.
In Octets	This parameter displays the total number of the octets received on the interface.
In Ucast Packets	It displays the number of subnetwork- unicast packets delivered to the higher level protocol.
In NUcast Packets	This parameter displays the number of non-unicast subnetwork packets delivered to the higher level protocol.
In Errors	This parameter displays the number of inbound packets that contained errors and restricted them from being delivered.
Out Octets	This parameter displays the total number of octets transmitted out of the interface.
Out Ucast Packets	It displays the total number of packets requested by the higher level protocol and then, transmitted to the non-unicast address.
Out Discards	This parameter displays the number of error-free outbound packets chosen to be discarded to prevent them from being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Out Errors	It displays the number of outbound packets that could not be transmitted because of errors.

6.1.2 Wireless Statistics

Wireless Statistics screen displays the details of the wireless interface.

To view the Wireless Statistics, click **MONITOR > Interface Statistics > Wireless1**.

In addition to the parameters displayed for Ethernet interface, the following parameters are displayed for the wireless interface.

Parameter	Description
RSSI Statistics	
RSSI stands for Received Signal Strength Indicator. For receiving strong signal, the RSSI should be high. This section displays the Receiver statistics. It indicates the power viewed across the receiver input.	
Antenna	Specifies all the antenna ports available for the product. This is based on the product option.
Status	Specifies the configuration status of the antenna ports. ON indicates that antenna port is enable for that chain. OFF means antenna port is disabled for that chain.
Control	Specifies the RSSI value of the packet received on the selected channel.
Extension	Specifies RSSI value of the packets received on the adjacent channel (20MHz). This parameter is applicable only for the 40 MHz modes, i.e., 40 PLUS and 40 Minus modes.
Rx Error Details	
Decrypt Errors	This parameter is applicable if the Security is enabled. It indicates the number of received packets that failed to decrypt.
CRC Errors	Specifies the number of received packets with invalid CRC.



Figure 6-2 Wireless Statistics

6.2 WORP Statistics

6.2.1 General Statistics

WORP General Statistics screen displays the signal information, WORP data messages, Data transmission statistics, and Registration details of all the data transmitted through the interface.

To view the General Statistics, click **MONITOR > WORP Statistics > Interface 1 > General Statistics**.

WORP General Statistics																																	
Interface Type	SU																																
<input type="button" value="Refresh"/> <input type="button" value="Clear"/>																																	
<table border="0" style="width: 100%;"> <tr> <td style="width: 50%; vertical-align: top;"> Signal Information <table border="1" style="width: 100%;"> <tr><td>Avg Local Signal</td><td>-10 dBm</td></tr> <tr><td>Avg Local Noise</td><td>-94 dBm</td></tr> <tr><td>Avg Remote Signal</td><td>-20 dBm</td></tr> <tr><td>Avg Remote Noise</td><td>-94 dBm</td></tr> </table> </td> <td style="width: 50%; vertical-align: top;"> Registration details <table border="1" style="width: 100%;"> <tr><td>Remote Partners</td><td>1</td></tr> <tr><td>Announcements</td><td>5</td></tr> <tr><td>Request For Service</td><td>3</td></tr> <tr><td>Registration Requests</td><td>5</td></tr> <tr><td>Registration Rejects</td><td>0</td></tr> <tr><td>Authentication Requests</td><td>5</td></tr> <tr><td>Authentication Confirms</td><td>5</td></tr> <tr><td>Registration Attempts</td><td>1</td></tr> <tr><td>Registration Incompletes</td><td>0</td></tr> <tr><td>Registration Timeouts</td><td>0</td></tr> <tr><td>Registration Last Reason</td><td>None</td></tr> </table> </td> </tr> </table>		Signal Information <table border="1" style="width: 100%;"> <tr><td>Avg Local Signal</td><td>-10 dBm</td></tr> <tr><td>Avg Local Noise</td><td>-94 dBm</td></tr> <tr><td>Avg Remote Signal</td><td>-20 dBm</td></tr> <tr><td>Avg Remote Noise</td><td>-94 dBm</td></tr> </table>	Avg Local Signal	-10 dBm	Avg Local Noise	-94 dBm	Avg Remote Signal	-20 dBm	Avg Remote Noise	-94 dBm	Registration details <table border="1" style="width: 100%;"> <tr><td>Remote Partners</td><td>1</td></tr> <tr><td>Announcements</td><td>5</td></tr> <tr><td>Request For Service</td><td>3</td></tr> <tr><td>Registration Requests</td><td>5</td></tr> <tr><td>Registration Rejects</td><td>0</td></tr> <tr><td>Authentication Requests</td><td>5</td></tr> <tr><td>Authentication Confirms</td><td>5</td></tr> <tr><td>Registration Attempts</td><td>1</td></tr> <tr><td>Registration Incompletes</td><td>0</td></tr> <tr><td>Registration Timeouts</td><td>0</td></tr> <tr><td>Registration Last Reason</td><td>None</td></tr> </table>	Remote Partners	1	Announcements	5	Request For Service	3	Registration Requests	5	Registration Rejects	0	Authentication Requests	5	Authentication Confirms	5	Registration Attempts	1	Registration Incompletes	0	Registration Timeouts	0	Registration Last Reason	None
Signal Information <table border="1" style="width: 100%;"> <tr><td>Avg Local Signal</td><td>-10 dBm</td></tr> <tr><td>Avg Local Noise</td><td>-94 dBm</td></tr> <tr><td>Avg Remote Signal</td><td>-20 dBm</td></tr> <tr><td>Avg Remote Noise</td><td>-94 dBm</td></tr> </table>	Avg Local Signal	-10 dBm	Avg Local Noise	-94 dBm	Avg Remote Signal	-20 dBm	Avg Remote Noise	-94 dBm	Registration details <table border="1" style="width: 100%;"> <tr><td>Remote Partners</td><td>1</td></tr> <tr><td>Announcements</td><td>5</td></tr> <tr><td>Request For Service</td><td>3</td></tr> <tr><td>Registration Requests</td><td>5</td></tr> <tr><td>Registration Rejects</td><td>0</td></tr> <tr><td>Authentication Requests</td><td>5</td></tr> <tr><td>Authentication Confirms</td><td>5</td></tr> <tr><td>Registration Attempts</td><td>1</td></tr> <tr><td>Registration Incompletes</td><td>0</td></tr> <tr><td>Registration Timeouts</td><td>0</td></tr> <tr><td>Registration Last Reason</td><td>None</td></tr> </table>	Remote Partners	1	Announcements	5	Request For Service	3	Registration Requests	5	Registration Rejects	0	Authentication Requests	5	Authentication Confirms	5	Registration Attempts	1	Registration Incompletes	0	Registration Timeouts	0	Registration Last Reason	None		
Avg Local Signal	-10 dBm																																
Avg Local Noise	-94 dBm																																
Avg Remote Signal	-20 dBm																																
Avg Remote Noise	-94 dBm																																
Remote Partners	1																																
Announcements	5																																
Request For Service	3																																
Registration Requests	5																																
Registration Rejects	0																																
Authentication Requests	5																																
Authentication Confirms	5																																
Registration Attempts	1																																
Registration Incompletes	0																																
Registration Timeouts	0																																
Registration Last Reason	None																																
WORP Data Messages <table border="1" style="width: 100%;"> <tr><td>Poll Data</td><td>9726</td></tr> <tr><td>Poll No Data</td><td>9541</td></tr> <tr><td>Reply Data</td><td>9724</td></tr> <tr><td>Reply More Data</td><td>0</td></tr> <tr><td>Reply No Data</td><td>9514</td></tr> <tr><td>Poll No Replies</td><td>0</td></tr> </table>		Poll Data	9726	Poll No Data	9541	Reply Data	9724	Reply More Data	0	Reply No Data	9514	Poll No Replies	0																				
Poll Data	9726																																
Poll No Data	9541																																
Reply Data	9724																																
Reply More Data	0																																
Reply No Data	9514																																
Poll No Replies	0																																
Data Transmission Statistics <table border="1" style="width: 100%;"> <tr><td>Send Success</td><td>214</td></tr> <tr><td>Send Retries</td><td>2</td></tr> <tr><td>Send Failures</td><td>0</td></tr> <tr><td>Receive Success</td><td>185</td></tr> <tr><td>Receive Retries</td><td>0</td></tr> <tr><td>Receive Failures</td><td>0</td></tr> </table>		Send Success	214	Send Retries	2	Send Failures	0	Receive Success	185	Receive Retries	0	Receive Failures	0																				
Send Success	214																																
Send Retries	2																																
Send Failures	0																																
Receive Success	185																																
Receive Retries	0																																
Receive Failures	0																																

Figure 6-3 WORP General Statistics

The parameters displayed in this page are described in the following table.

Field	Description
Interface Type	Specifies the type of radio interface.
Signal Information	Specifies the SNR details of local and remote devices. These details are measured in dBm.
WORP Data Messages	Specifies the sent or received data frames through wireless interface.

Field	Description
Data Transmission Statistics	Specifies the number of transmissions occurred through the interface.
Registration details	Specifies the status of the entire registration process.

NOTE: For better results, the Send Failure/Send Retrieve must be low in comparison to Send Success. The same applies for Receive Retries/Receive Failure. Click **Refresh** to update the details in this page.

6.2.2 BSU Statistics

WORP BSU Statistics provides the information related to the BSU currently connected to the SU.

To view the Interface Statistics, click **MONITOR > WORP Statistics > Interface 1 > BSU Statistics**.

WORP BSU Statistics										
BSU Name	MAC Address	Bridge Port	Local Tx Rate (Kbps)	Remote Tx Rate (Kbps)	Local Signal (dBm)	Local Noise (dBm)	Local SNR	Remote Signal (dBm)	Remote Noise (dBm)	Remote SNR
BSU	00:02:6f:5b:6b:28	3	52000	52000	-10	-96	86	-10	-96	86

Figure 6-4 WORP BSU Statistics

Click **Refresh** to get the latest updates in this page.

The following table lists the parameters and their descriptions:

Field	Description
BSU Name	System name of the BSU connected.
Mac Address	MAC address of the BSU connected.
Local Tx Rate (Kbps)	SU Tx Rate.
Remote Tx Rate (Kbps)	BSU Tx Rate.
Local Signal (dBm)	Refers to the signal level with which the SU received wireless frames from the BSU.
Local Noise (dBm)	Refers to the noise level with which the SU received wireless frames from the BSU.
Remote Signal (dBm)	Signal level with which the BSU receives wireless frames from the SU.

Field	Description
Remote Noise (dBm)	Refers to the noise level with which the BSU receives wireless frames from the SU.

6.3 Bridge

6.3.1 Bridge Statistics

To view the Bridge Statistics, click **MONITOR > Bridge > Bridge Statistics**.

Description	Bridge
Type	6
MTU	1500
Physical Address	00:20:a6:00:12:12
Operational Status	UP
In Octets	100584
In Unicast Packets	692
In Non-unicast Packets	66
In Errors	0
Out Octets	370472
Out Unicast Packets	830
Out Discards	0
Out Errors	0

Figure 6-5 Bridge Statistics

The following table lists the parameters and their descriptions:

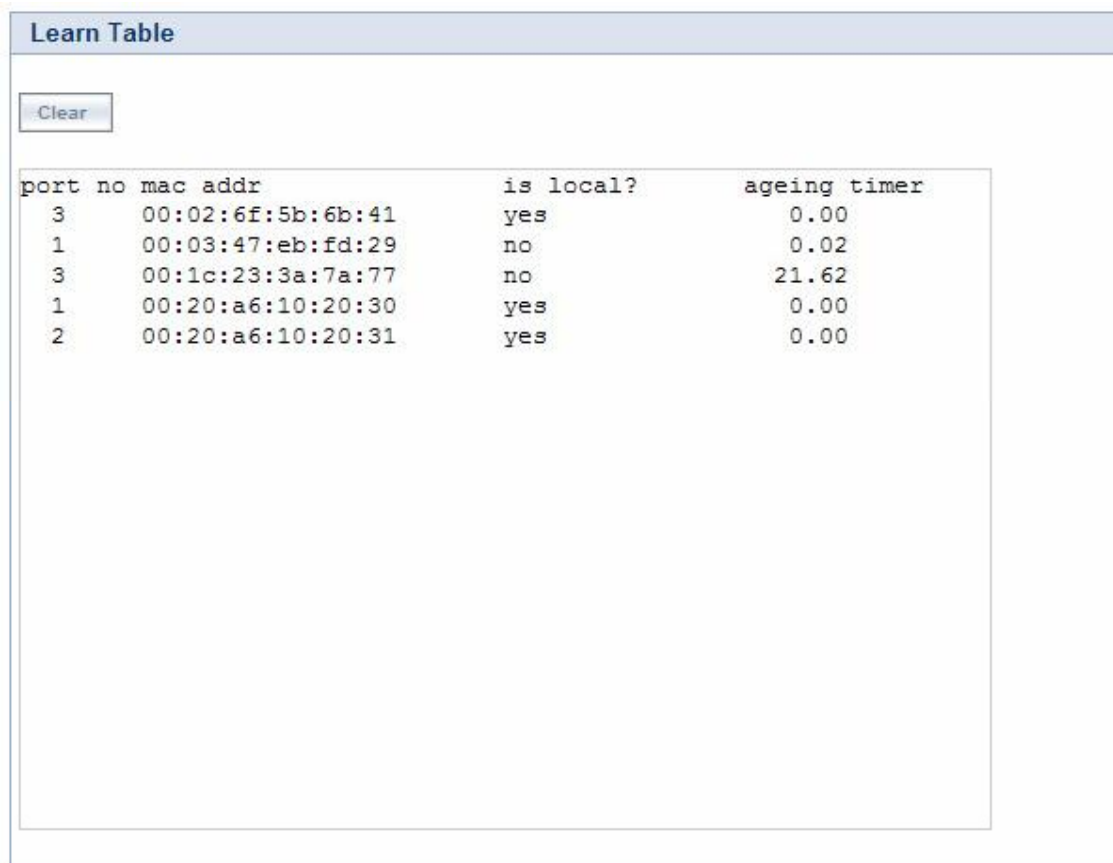
Parameter	Description
Description	Displays the textual string containing information about the interface.
Type	Displays the type of interface.

Parameter	Description
MTU	Displays the MTU value.
Physical Address	Displays the bridge MAC Address.
Operational Status	Displays the current state of the interface: Up (ready to pass packets) or Down (not ready to pass packets).
In Octets	Displays the total number of octets received on the interface, including the framing characters.
In Unicast Packets	Displays the number of subnetwork unicast packets received at the bridge interface.
In Non-Unicast Packets	Displays the number of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets received at the bridge interface.
In Errors	Displays the number of inbound packets that contained errors and are restricted for delivering them to a higher-layer protocol at the bridge interface.
Out Octets	Displays the total number of octets transmitted out of the interface, including the framing characters.
Out Unicast Packets	Displays the total number of packets requested by higher-level protocols to be transmitted out of the interface to a subnetwork-unicast address, including those that were discarded or not sent.
Out Discards	Displays the number of error-free outbound packets chosen to be discarded to prevent them being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Out Errors	Displays the number of outbound packets that could not be transmitted because of errors.

6.3.2 Learn Table

Learn Table is used to view all MAC addresses the device has learnt on an interface. The Learn Table displays the information of learnt MAC addresses, the interface on which it learnt the MAC address, aging timer corresponding to the MAC add entry, and the type of interface as local interface or attached interface to the device. It reports the MAC address for each node that the device has learnt on the network and the interface on which the node was detected. There can be up to 10,000 entries in the Learn Table.

To view the **Learn Table** entries, click **MONITOR > Bridge > Learn Table**.



port no	mac addr	is local?	ageing timer
3	00:02:6f:5b:6b:41	yes	0.00
1	00:03:47:eb:fd:29	no	0.02
3	00:1c:23:3a:7a:77	no	21.62
1	00:20:a6:10:20:30	yes	0.00
2	00:20:a6:10:20:31	yes	0.00

Figure 6-6 Learn Table

6.4 Network Layer

6.4.1 Routing Table

Routing table displays all the active routes of the network. These can be either static or dynamic (obtained through RIP). For every route created in the network, the details of that particular link or route will get updated in this table.

To view the Routing Table, click **MONITOR > Network Layer > Routing Table**.

NOTE: This feature is available only in Routing mode.

Routing Table						
Destination	Gateway	Genmask	Flags	Metric	Ref	Use Iface
169.254.128.0	0.0.0.0	255.255.255.0	U	0	0	0 br0
0.0.0.0	169.254.128.132	0.0.0.0	UG	0	0	0 br0

Figure 6-7 Routing Table

6.4.2 IP ARP

This section displays the mapping of the IP and MAC addresses of all nodes in the network. This information is based upon the Address Resolution Protocol (ARP). ARP is a L2 neighboring protocol which converts the IP address into a physical address on the Ethernet network.

To view the current ARP table

1. Click **MONITOR > Network Layer > IP ARP**.

IP ARP Table			
Note : On clicking CLEAR button it will take upto 10 seconds to update.			
<input type="button" value="Clear"/>			
If Index	Physical Address	Net Address	Type
2	00:03:47:eb:fd:29	10.0.0.100	Dynamic
<input type="button" value="Refresh"/> <input type="button" value="OK"/>			

Figure 6-8 IP ARP Table

2. Click **Refresh** to get the updated or latest ARP Table.
3. Click **Clear** to delete all entries of the ARP Table.

6.4.3 ICMP Statistics

This page provides the statistical information for both received and transmitted messages by the device. The ICMP Statistics attributes can be used to monitor message traffic.

To view the ICMP Statistics, click **MONITOR > Network Layer > ICMP Statistics**.

ICMP Statistics			
<input type="button" value="Refresh"/>			
In Msgs	34	Out Msgs	34
In Errors	0	Out Errors	0
In Dest Unreachs	34	Out Dest Unreachs	34
In Time Excds	0	Out Time Excds	0
In Parm Probs	0	Out Parm Probs	0
In Src Quenchs	0	Out Src Quenchs	0
In Redirects	0	Out Redirects	0
In Echos	0	Out EchoReps	0
In EchoReps	0	Out Timestamps	0
InTimestamps	0	Out Timestamp Reps	0
In Timestamp Reps	0	Out Addr Masks	0
In Addr Masks	0	Out Addr Mask Reps	0
In Addr Mask Reps	0		

Figure 6-9 ICMP Statistics

The following table lists the parameters and their descriptions:

Field	Description
In Msgs	The number of ICMP messages that are received by the device.
In Errors	The number of ICMP messages that the entity received but determined as having errors.
In Dest Unreachs	The number of ICMP Destination Unreachable messages received.
In Time Excds	The number of ICMP Time Exceeded messages received.
In Parm Probs	The number of ICMP Parameter Problem messages received.
In Srec Quenchs	The number of ICMP Source Quench messages received.
In Redirects	The rate of ICMP Redirect messages received.
In Echos	The rate of ICMP Echo messages received.
In EchoReps	The rate of ICMP Echo Reply messages received.
In Timestamps	The rate of ICMP Timestamp (request) messages received.
In Timestamps Reps	The rate of ICMP Timestamp Reply messages received.
In Addr Masks	The number of ICMP Address Mask Request messages received.

Field	Description
In Addr Mask Reps	The number of ICMP Address Mask Reply messages received.

6.4.4 RIP Database

This section shows the information about the RIP database. It contains routes learnt from other routers.

RIP Database					
RIP DATABASE					
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP					
Sub-codes:					
(n) - normal, (s) - static, (d) - default, (r) - redistribute,					
(i) - interface					
Network	Next Hop	Metric	From	Iag	Time

Figure 6-10 RIP Database

6.5 DHCP

DHCP Leases file stores the DHCP client database of the DHCP clients that the DHCP Server has served. The information stored includes the duration of the lease, for which the IP address has been assigned, the start and end dates for the lease, and the MAC address of the network interface card of the DHCP client.

To view DHCP Leases, click **MONITOR > DHCP Leases**.

```
DHCP Leases

lease 169.254.128.1 {
  starts 6 2000/01/01 00:10:06;
  ends 0 2000/01/02 00:10:06;
  cltt 6 2000/01/01 00:10:06;
  binding state active;
  next binding state free;
  hardware ethernet 00:19:5b:7e:e1:57;
  uid "\001\000\031[~\341W";
  client-hostname "my pc";
}
```

Figure 6-11 DHCP Leases

6.6 Logs

6.6.1 Event Log

The Event Log keeps track of events that occur during the operation of the device. It displays the event occurring time, event type, and the name of the error or the error message. Based on the priority, the event details are logged and can be used for any reference or troubleshooting.

To view the Event Log

1. Click **MONITOR > Logs > Event Log**. The Event Log screen appears as shown below.

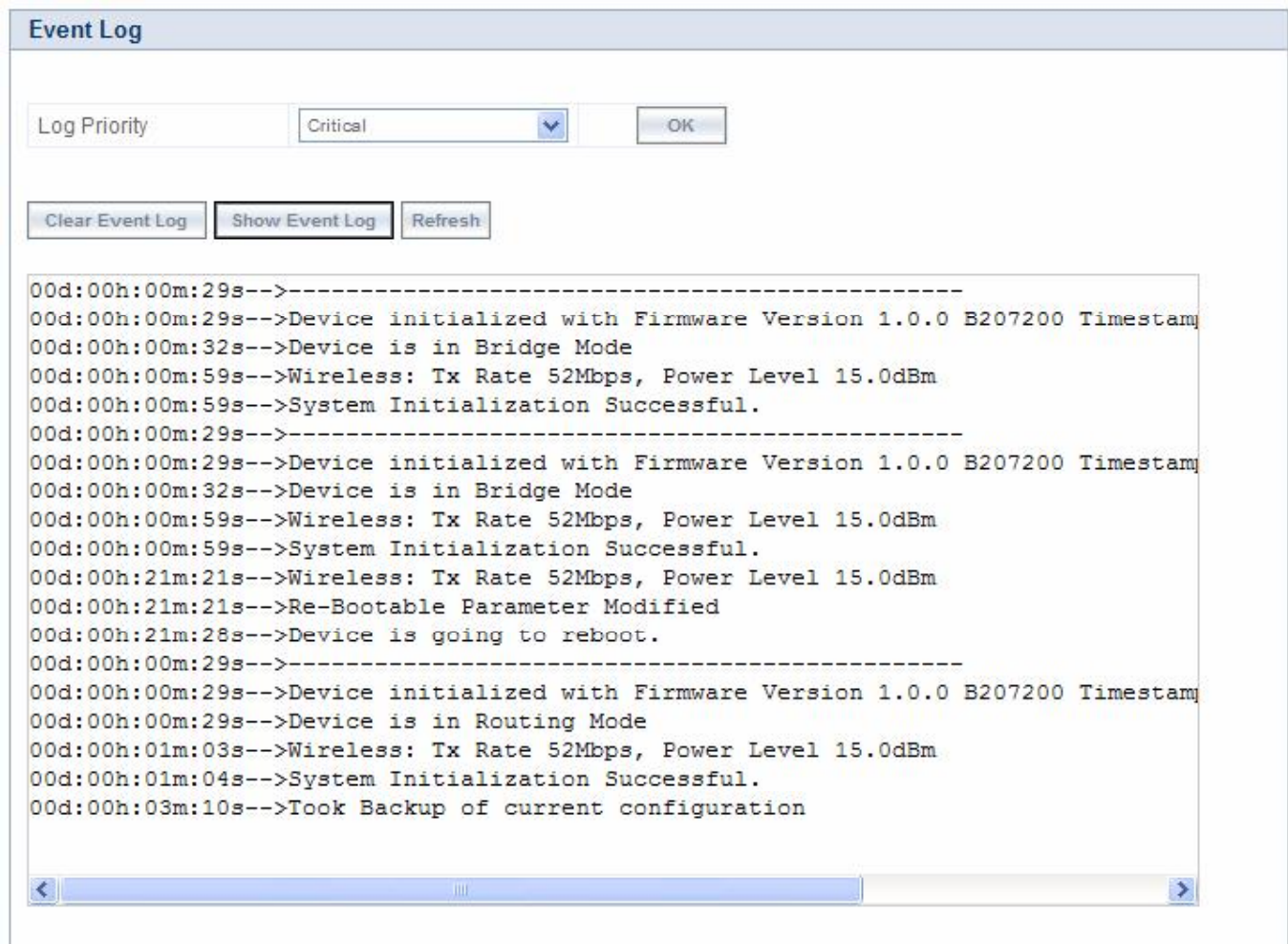


Figure 6-12 Event Log

2. Select the appropriate log priority from the Log Priority drop-down list that has the following options: **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Info**, and **Debug**.

NOTE: When **Critical** is selected, the system logs only critical messages and the messages with higher priority (i.e., **Emergency** and **Alert**) will be logged from the instance the priority is selected.

3. After setting the event log priority option, click **Show Event Log** to display the event logs.
 - To delete the Event Log, click **Clear Event Log**.

NOTE: The recent eventlogs are stored in the flash memory.

6.6.2 Syslog

System log messages are generated by the system by sending requests at various instances to the system log server.

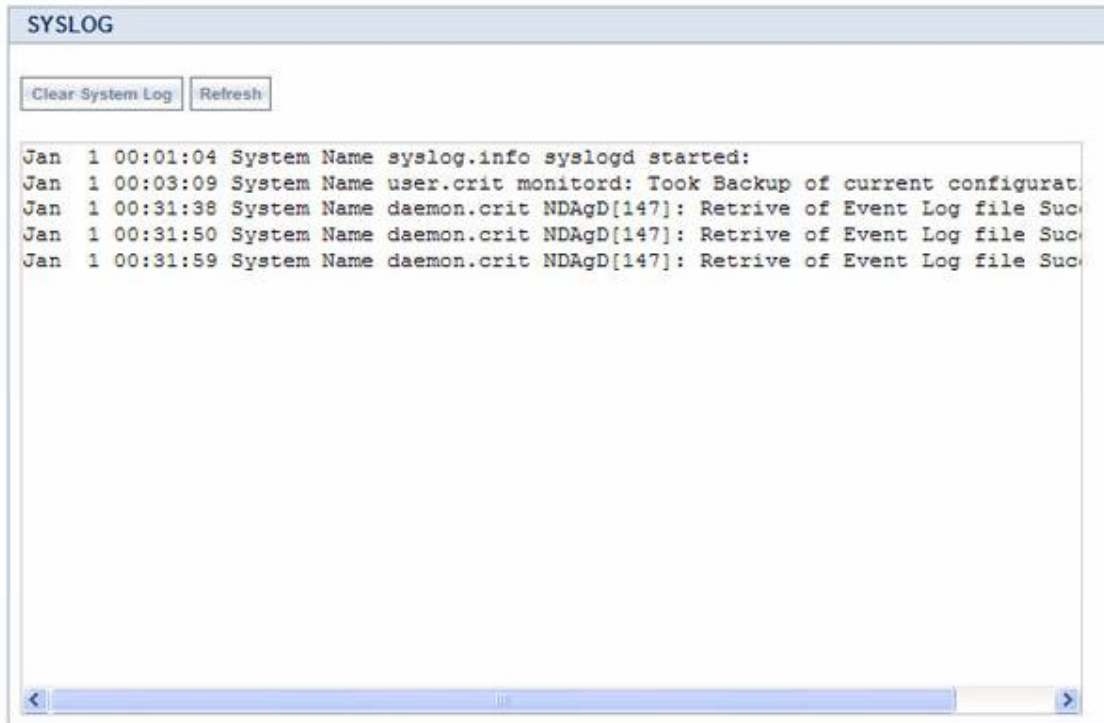


Figure 6-13 System Log

- Click **Show System Log** to display SYSLOG information.
- Click **Clear System Log** to clear the SYSLOG information.

6.7 Tools

6.7.1 Link Test

WORP Link Test shows, in graphical form, Signal and Noise levels at which packets are received at local and remote unit. WORP link test feature is used to monitor the local/remote signal/noise/SNR details of the connected WORP link. During antenna alignment, this feature can be enabled to monitor the min/cur/max signal details.

NOTE: Internet Explorer 6.0 and its above versions support the link tests.

To view the Interface Statistics, click **MONITOR > Tools > Link Test**.



Figure 6-14 WORP Link Test

Click **Explore Start** to explore the established WORP links. This process lists the details of the registered SUs. Clicking the **Graph** icon provides the local/remote station information. After starting the link test explore, if the user moves out of this page before stopping, exploration is automatically stopped after Link Test Idle Timeout.

When you set the **Link Test Idle Timeout** value, the exploring process automatically stops on the given timeout value if you navigate out of the web page. The default Link Test Idle Timeout is 300 seconds.

The following figure displays the graph for Local/Remote Station information, such as **Station Name** and **MAC address** of both BSU and SU.

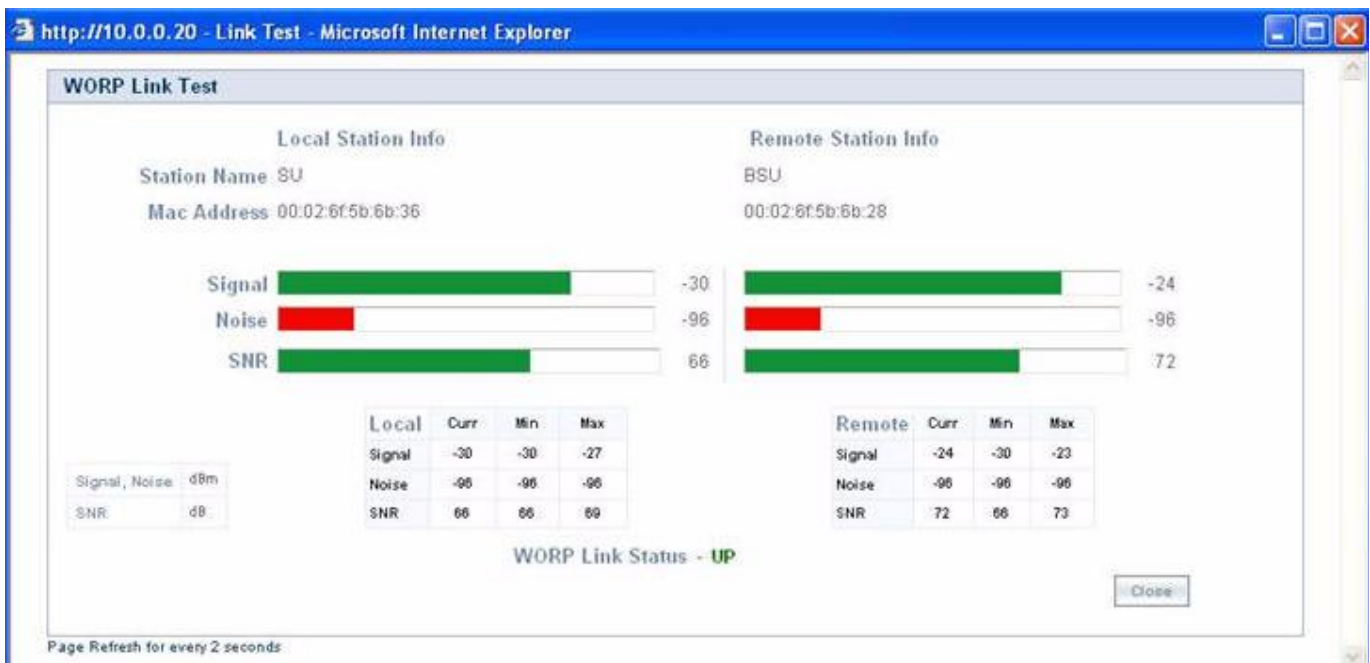


Figure 6-15 WORP Link Status Graph

To stop the link test, click **Close**.

NOTE: Link tests are performed for maximum 3 times. By default, the **Link Test Status** is disabled.

6.7.2 WORP Site Survey

WORP Site Survey is done by the SU. The SU scans all the available channels and channel bandwidths, and collects information about all the BSUs on those channels/bandwidths with the given Network Name. Referring to the displayed list, the user can see which is the best BSU.

WORP Site Survey Table								
BSU Name	MAC Address	Channel Number	Channel Bandwidth (MHz)	Rx Rate (Kbps)	Local Signal (dBm)	Local Noise (dBm)	Local SNR	Registration Status
BSU	00:02:6f:5b:6b:28	160	20	52000	-26	-96	70	Registered

Stop

Figure 6-16 WORP Site Survey Table

To initialize the survey process, click **Start** button. This process lists all the available BSU details. If you want to stop the site survey process, click the **Stop** button.

6.8 SNMP v3 Statistics

This tab is displayed only when SNMP v3 is configured. It displays the SNMP v3 statistics.

SNMP V3 Statistics	
Unsupported Sec Levels	0
NotIn Time Windows	2
Unknown User Names	0
Unknown Engine IDs	2
Wrong Digests	0
Decryption Errors	0

Refresh

Figure 6-17 SNMP v3 Statistics

Procedures

This chapter provides details about the various procedures involved in the operation of the MP-8150-CPE units through the Web, CLI, and SNMP interface.

The following topics are covered in this chapter:

- [TFTP Server Setup](#)
- [Web Interface Firmware Download](#)
- [Configuration Backup](#)
- [Configuration Restore](#)
- [Soft Reset to Factory Default](#)
- [Hard Reset to Factory Default](#)
- [Forced Reload](#)
- [Upgrade a New Firmware Using ScanTool in Bootloader Mode](#)
- [Download a New Firmware Using CLI from Bootloader](#)

7.1 TFTP Server Setup

A Trivial File Transfer Protocol (TFTP) server lets you transfer files across a network. You can retrieve files from the device for backup or copying, and you can upgrade the firmware or the configuration file. You can download the SolarWinds TFTP server software from the product installation CD or from <http://support.proxim.com>. You can also download the latest TFTP software from SolarWind's Web site at <http://www.solarwinds.net>. The following instructions are prepared with an assumption that you are using the SolarWinds TFTP server software; other TFTP servers may require different configurations.

NOTE: *If a TFTP server is not available in the network, you can perform similar file transfer operations using the HTTP interface.*

Ensure the following:

1. The upload or download directory is correctly set (the default directory is **C:\TFTP-Root**).
2. The required firmware file is present in the directory.
3. The TFTP server is running. The TFTP server must be running only during file upload and download. You can check the connectivity between the MP-8150-CPE and the TFTP server by pinging the MP-8150-CPE from the computer that hosts the TFTP server. The ping program should show replies from MP-8150-CPE.
4. The TFTP server is configured to both Transmit and Receive files (on the Security tab under **File > Configure**), with no automatic shutdown or time-out (on the **Auto-Close** tab).

7.2 Web Interface Firmware Download

In some cases, it may be necessary to upgrade the embedded software of the unit by downloading the firmware. You can download the firmware through TFTP or HTTP.

7.2.1 Through TFTP

1. Set up the TFTP server as described in TFTP Server Setup.
2. Access the unit as described in [Logging in to the Web Interface](#).
3. Click **Management > File Management > Upgrade Firmware > TFTP** tab.
4. Fill in the following details:
 - Server IP Address <IP address TFTP server>
 - File Name <image file name>
5. Click **Update/Update-Reboot** to start the file transfer.

The unit downloads the firmware. The TFTP server program should show download activity after a few seconds. When the download is complete, the unit is ready to start the embedded software upon reboot.

7.2.2 Through HTTP

1. Access the unit as described in [Logging in to the Web Interface](#).
2. Click **Management > File Management > Upgrade Firmware > HTTP** tab.
3. Fill in the following details:
 - File Name <firmware file name>. Using the browse button, select the firmware form the host to be uploaded.
4. Click **Update** to start the file transfer.

The unit downloads the firmware. When the download is complete, the unit is ready to start the embedded software upon reboot.

7.3 Configuration Backup

You can back up the unit's configuration by retrieving the configuration file. You can use this file to restore the configuration or to configure another similar unit (see [Configuration Restore](#)). You can update a configuration file through TFTP or HTTP.

7.3.1 Through TFTP

1. Set up the TFTP server as described in TFTP Server Setup.
2. Access the unit as described in [Logging in to the Web Interface](#).
3. Click **Management > File Management > Retrieve From Device > TFTP** tab.
4. Fill in the following details:
 - Server IP Address <IP address TFTP server>
 - File Name <configuration file name>
 - File Type <configuration file type>
5. Click **Retrieve** to start the file transfer.

The unit uploads the configuration file. The TFTP server program should show upload activity after a few seconds. When the upload is complete, the configuration is backed up.

7.3.2 Through HTTP

1. Access the unit as described in [Logging in to the Web Interface](#).
2. Click **Management > File Management > Retrieve From Device > HTTP** tab.
3. Fill in the following details:
 - File Type <configuration file type>
4. Click **Retrieve** to start the file transfer.

The unit uploads the configuration file. When the upload is complete, the configuration is backed up.

7.4 Configuration Restore

You can restore the configuration of the unit by downloading a configuration file. The configuration file contains the configuration information of a unit. You can download a configuration file through TFTP or HTTP.

7.4.1 Through TFTP

1. Set up the TFTP server as described in TFTP Server Setup.
2. Access the unit as described in [Logging in to the Web Interface](#).
3. Click **Management > File Management > Upgrade Configuration > TFTP** tab.
4. Fill in the following details:
 - Server IP Address <IP address TFTP server>
 - File Name <configuration file name>
5. Click **Update/Update-Reboot** to start the file transfer.

The unit downloads the configuration file. The TFTP server program should show download activity after a few seconds. In case of **Update** and **Reboot**, when the upgrade is complete and the system rebooted, the configuration is restored.

7.4.2 Through HTTP

1. Access the unit as described in [Logging in to the Web Interface](#).
2. Click **Management > File Management > Upgrade Configuration > HTTP** tab.

3. Fill in the following details:
 - File Name <configuration file name>
4. Click **Update** to start the file transfer.

A reboot is required for the new configuration to be restored into the device.

7.5 Soft Reset to Factory Default

The unit can be reset to the factory default settings. Resetting to default settings leads to configuring the unit anew.

To reset to factory default settings using the Web Interface

1. Click **Management > Reset for Factory**.
2. Click the **Reset to Factory Default** button.

The device configuration parameter values are reset to their factory default values. If you do not have access to the unit, you can use the procedure described in Hard Reset to Factory Default as an alternative.

7.6 Hard Reset to Factory Default

If you cannot access the unit or you have lost its password, you can reset the unit to the factory default settings. Resetting to default settings leads to configuring the unit anew.

To reset to factory default settings, press and hold the RELOAD button on the side of the unit's power supply or **RELOAD** button on the unit for 5 seconds. The current configuration is deleted from the unit and the unit reboots with factory defaults.

CAUTION: *If you hold the RELOAD button for longer than 10 seconds, you may go into Forced Reload mode, which erases the unit's embedded software.*

7.7 Forced Reload

With Forced Reload, you can erase the embedded software. Use this procedure only as a last resort if the unit does not boot and the "Reset to Factory Defaults" procedure does not help. If you perform a Forced Reload, you must download a new firmware with the Bootloader (see "Firmware Download with the Bootloader" below).

CAUTION: *The following procedure erases the embedded software of the unit. This software image must be reloaded through an Ethernet connection with a TFTP server. The image filename to be downloaded can be configured with ScanTool through the Ethernet interface to make the unit functional again.*

To do a forced reload

1. Disconnect and reconnect power to the unit; the unit resets and the LEDs flash.
2. Immediately press and hold the RELOAD button on the side of the unit's power supply or **RELOAD** button on the unit for about 20 seconds. The software image and configuration are deleted from the unit.
3. Follow the Firmware Download with the Bootloader procedure to download an image file.

7.8 Upgrade a New Firmware Using ScanTool in Bootloader Mode

To download the unit's firmware, you will need an Ethernet connection to the computer on which the TFTP server resides and to a computer that is running ScanTool (this is either two separate computers connected to the same network or a single computer running both programs).

ScanTool detects if a device does not have a valid software firmware installed. In this case, the TFTP Server and Image File Name parameters are enabled in the ScanTool's Change screen so you can download a new firmware to the unit. (These fields are grayed out if ScanTool does not detect a software firmware problem.)

NOTE: If you are unable to view the configuration parameters in ScanTool, it means that the device is not responding to your network. Hard reset the unit by unplugging and plugging the Power cable to PoE.

7.8.1 Preparing to Download the Firmware

Before starting, you need to know the unit's IP address, subnet mask, the TFTP Server IP Address, and the unit's firmware name. Make sure the TFTP server is running and configured to point to the folder containing the image to be downloaded.

7.8.1.1 Download Procedure

Follow these steps to use ScanTool to download the firmware to a device with a missing firmware:

1. Download the latest software from <http://support.proxim.com>.
2. Copy the latest software updates to your TFTP server.
3. Launch ScanTool.
4. Highlight the entry for the device you want to update and click **Change**.
5. Set the IP address type as per your choice, either **Static** or **Dynamic**.
Setting IP Addrtype to static:
Set IP Address Type to Static.
 - Enter an unused IP address that is valid on your network in the IP Address field. You may need to contact your network administrator to get this address.
 - Enter the network's Subnet Mask in the field provided.
 - Enter the network's Gateway IP Address, if necessary. You may need to contact your network administrator to get this address. You should only enter the default gateway address (169.254.128.132) if the device and the TFTP server are separated by a router.
 - Enter the IP address of your TFTP server in the field provided.
 - Enter the Image File Name (including the file extension). Enter the full directory path and file name. If the file is located in the default TFTP directory, you need to enter only the file name.Setting IP Addrtype to dynamic:
 - Set IP Addrtype to Dynamic.
 - Start a TFTP server and BOOTP server and enter all the configuration parameters (ipaddr, subnet mask etc).
6. Click **OK**. The device will reboot and the download will begin automatically. You should see downloading activity within the TFTP server's status screen.
7. Click **OK** when prompted that the device has been updated successfully to return to the Scan List screen.
8. Click **Cancel** to close the ScanTool.
9. When the download process is complete, configure the device as desired.

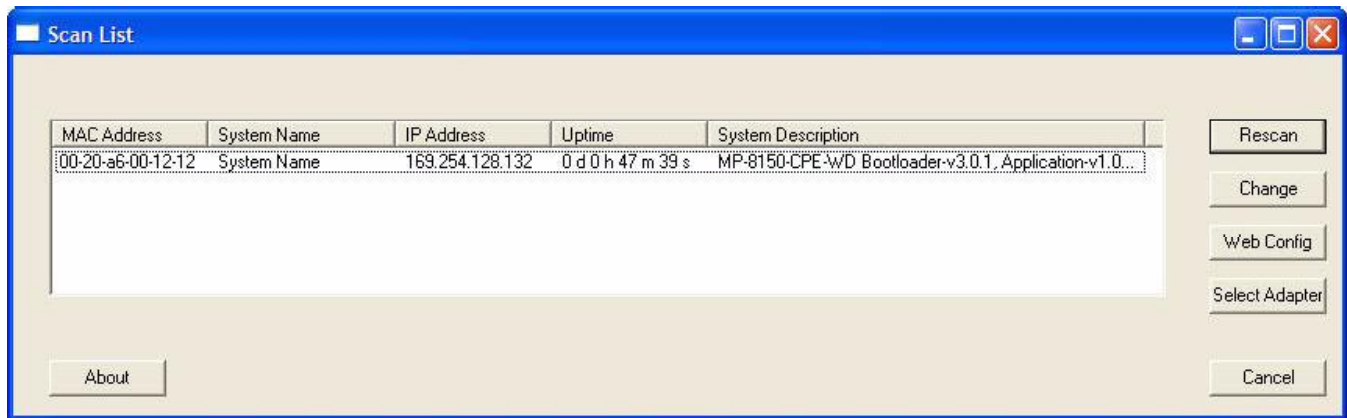


Figure 7-1 ScanTool Scanlist

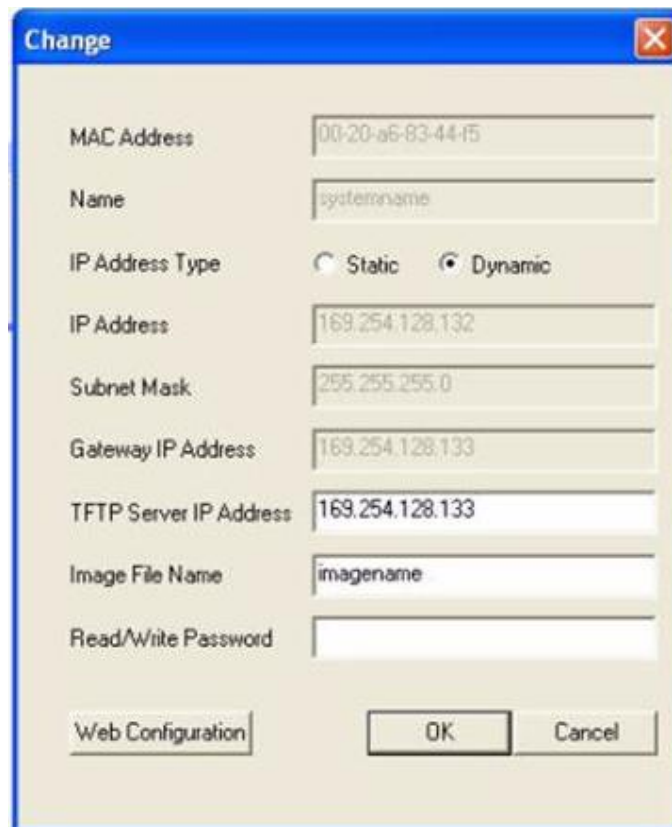


Figure 7-2 Modifying the IP Address

7.9 Download a New Firmware Using CLI from Bootloader

To download the unit's Image File, you will need an Ethernet connection to the computer on which the TFTP server resides. This can be any computer on the LAN or connected to the device with a cross-over Ethernet cable. You must also connect the

device to a computer with a standard serial cable and use a terminal client, such as HyperTerminal. From the terminal, enter CLI Commands to set the IP address and download unit's Image.

7.9.1 Preparing to Download the Firmware

Before starting, you need to know the Unit's IP address, subnet mask, the TFTP Server IP Address, and the UNIT'S firmware name. Make sure the TFTP server is running and configured to point to the folder containing the firmware to be downloaded.

7.9.1.1 Download Procedure

1. Download the latest software from <http://support.proxim.com>.
2. Copy the latest software updates to your TFTP server's default directory.
3. Use a cross-over serial cable to connect the Unit's serial port to your computer's serial port.
4. Open your terminal emulation program (like HyperTerminal) and set the following connection properties:
 - Com Port: <COM1, COM2, etc., depending on your computer>
 - Baud rate: 115200
 - Data Bits: 8
 - Stop bits: 1
 - Flow Control: None
 - Parity: None
5. Under **File > Properties > Settings > ASCII Setup**, enable the **Send line ends with line feeds** option.
6. HyperTerminal sends a line return at the end of each line of code.
7. Power Reset the device (by resetting the power on PoE).
8. The terminal display shows Power On Self Tests (POST) activity. After approximately 30 seconds, a message appears indicating, "**Starting ScanTool interface, press any key to enter CLI 5**" and starts a counter for 5 seconds.
9. If the above counter expires, bootloader enters the ScanTool mode. To enter the CLI, press any key before the counter expires. Now a prompt appears as below:

```
Bootloader=>
```

10. Enter only the following statements:

```
Bootloader=> show (to view configuration parameters and values)
Bootloader=> set ipaddr <device IP Address>
Bootloader=> set serverip <TFTP Server IP Address>
Bootloader=> set filename <Device's Image File Name, including file extension>
Bootloader=> set gatewayip <Gateway IP Address>
Bootloader=> set netmask <Network Mask>
Bootloader=> set ipaddrtype static
Bootloader=> show (to confirm your new settings)
Bootloader=> reboot
```

Example:

```
Bootloader=> show
Bootloader=> set ipaddr 169.254.128.132
Bootloader=> set serverip 169.254.128
Bootloader=> set filename <imagename>
Bootloader=> set gatewayip 169.254.128.132
Bootloader=> set netmask 255.255.255.0
Bootloader=> set ipaddrtype static
```

```
Bootloader=> show
Bootloader=> reboot
```

The device will reboot and then download the firmware. You should see the downloading activity within the TFTP server's status screen. When the download process is complete, configure the device as desired.

NOTE: *If the device is not responding to your network, hard reset the unit by unplugging and plugging the Power cable to POE.*

Troubleshooting

This chapter helps you to isolate and solve problems with your MP-8150-CPE unit. If the procedures discussed in this document does not provide a solution, or the solution does not solve your problem, check our support website at <http://support.proxim.com>.

Before you start troubleshooting, check the details in the product documentation. For details about RADIUS, TFTP, terminal and telnet programs, and Web browsers, refer to their appropriate documentation.

In some cases, rebooting the MP-8150-CPE unit clears the problem. If nothing else helps, consider a [Soft Reset to Factory Default](#) or a [Forced Reload](#). The Forced Reload option requires you to download a new firmware to the MP-8150-CPE unit.

The following topics are covered in this chapter:

- [Gigabit Ethernet PoE](#)
- [Connectivity Issues](#)
- [Communication Issues](#)
- [Setup and Configuration Issues](#)

8.1 Gigabit Ethernet PoE

8.1.1 The Unit Does Not Work

1. Verify that you are using a standard UTP Category 5e/Category 6 cable.
2. Try a different port on the same Gigabit Ethernet PoE hub (remember to move the input port accordingly) – if it works, there is probably a faulty port or bad RJ-45 port connection.
3. If possible, try to connect the unit to a different Gigabit Ethernet PoE hub.
4. Try using a different Ethernet cable – if it works, there is probably a faulty connection over the long cable, or a bad RJ-45 connection.
5. Check power plug and hub.
6. If the Ethernet link goes down, check the cable, cable type, switch, and hub.

8.1.2 There Is No Data Link

1. Verify that the indicator for the port is “on.”
2. Verify that the Gigabit Ethernet PoE hub is connected to the Ethernet network with a good connection.
3. Verify that the Ethernet cable is Category 5e or better and is less than 100 meters (approximately 325 feet) in length from the Ethernet source to the MP-8150-CPE unit.
4. Try to connect a different device to the same port on the Gigabit Ethernet PoE hub – if it works and a link is established, there is probably a faulty data link in the unit.
5. Try to re-connect the cable to a different output port (remember to move the input port accordingly) – if it works, there is probably a faulty output or input port in the Gigabit Ethernet PoE hub or a bad RJ-45 connection.

8.1.3 “Overload” Indications

1. Verify that you are not using a cross-over cable between the Gigabit Ethernet PoE output port and the unit.
2. Verify that there is no short over any of the twisted pair cables.
3. Move the device into a different output port (remember to move the input port accordingly); if it works, there is probably a faulty port or bad RJ-45 connection.

8.2 Connectivity Issues

8.2.1 MP-8150-CPE Does Not Boot

The MP-8150-CPE shows no activity (the power LED is off).

1. Ensure that the power supply is properly working and correctly connected.
2. Ensure that all cables are correctly connected.
3. Check the power source.
4. If you are using an Active Ethernet splitter, ensure that the voltage is correct.
5. If you are using Gigabit Ethernet PoE, make sure you are using a Category 5e/Category 6, foiled, twisted pair cable to power the unit.

8.2.2 Ethernet Link Does Not Work

1. First check the Ethernet LED:
 - Solid Green: Ethernet is up.
 - Blinking Green: Ethernet is down.
2. Verify pass-through versus cross-over cable.

8.2.3 Serial Link Does Not Work

1. Make sure you are using a standard, straight-through, 9-pin serial cable.
2. Double-check the physical network connections.
3. Make sure your PC terminal program (such as HyperTerminal) is active and configured to the following values:
 - Com Port: (COM1, COM2, etc. depending on your computer);
 - Baud rate: 115200; Data bits: 8; Stop bits: 1; Flow Control: None; Parity: None;
 - Line Feeds with Carriage Returns(In HyperTerminal select: **File > Properties > Settings > ASCII Setup > Send Line Ends with Line Feeds**)

8.2.4 Cannot Use the Web Interface

1. Open a command prompt window and enter ping <ip address unit> (for example ping 10.0.0.1). If the unit does not respond, make sure that you have the correct IP address. If the unit responds, the Ethernet connection is working properly, continue with this procedure.
2. Ensure that you are using Microsoft Internet Explorer 6.0 or later (version 7.0 or later recommended) or Mozilla Firefox 3 or later.
3. Ensure that you are not using a proxy server for the connection with your Web browser.
4. Ensure that you have not exceeded the maximum number of Web Interface or CLI sessions.
5. Double-check the physical network connections. Use a well-known unit to ensure the network connection is properly functioning.
6. Perform network infrastructure troubleshooting (check switches, routers, and so on).

NOTE: At any point of time, if your device is unable to connect to your network, power reset your device by unplugging and plugging PoE

8.3 Communication Issues

8.3.1 Two Units Are Unable to Communicate Wirelessly

If a wireless link cannot be established after testing the two units within close distance of each other, then there can be two reasons why wireless connectivity is not possible while the MP-8150-CPE devices are at their desired locations:

There may be a problem in the RF path, for example, a bad connector attachment (this is the most common problem in installations) or a bad cable (water ingress).

NOTE: The cables can be swapped with known good ones as a temporary solution to verify cable quality.

Another reason may be related to an interference problem caused by a high signal level from another radio. This can be checked by changing the frequency channel and then verifying whether another channel works better or by changing the polarization as a way of avoiding the interfering signal. To know in advance how much interference is present in a given environment, a Spectrum Analyzer can be attached to a (temporary) antenna for measuring the signal levels on all available channels.

NOTE: The antennas are usually not the problem, unless mounted upside down causing the drain hole to be quickly filled with radome.

If a wireless link is not established after testing two units within close distance of each other, then the problem is either hardware or configuration related, such as a wrong Network name, Encryption key, Network Secret or SU Name. To eliminate these issues from being a factor, resetting the both units to factory defaults is the recommended solution.

If a wireless link is not possible after resetting the units and verifying that one unit is a BSU with WORP BSU interface configured and the other is an SU, then the problem is not configuration related and the only remaining reason is a possible hardware problem. Acquiring a third unit and then testing it amongst the existing units will help pinpoint the broken unit.

8.3.2 Surge and Lightning preventive maintenance

In case of any lightning or surge occurrence, check for the conditions specified below:

- Check the RF signals by referring to RSSI statistics and if the signal strength has been lowered considerably, replace the surge arrester.
- Unscrew the N-Type connector at the top and visually inspect the surge arrester for electrical burns. If any, replace the surge arrester.

8.4 Setup and Configuration Issues

The following issues relate to setup and configuration problems.

8.4.1 Lost Password

If you have lost your password, you must reset the MP-8150-CPE device to the default settings. See [Hard Reset to Factory Default](#) The default password is **public**. If you record your password, keep it in a safe place.

8.4.2 The MP-8150-CPE Responds Slowly

If the MP-8150-CPE takes a long time to become available, it could mean that:

- No DHCP server is available.

- The IP address of the MP-8150-CPE is already in use. Verify that the IP address is assigned only to the MP-8150-CPE. Do this by switching off the MP-8150-CPE and then pinging the IP address. If there is a response to the ping, another device in the network is using the same IP address. If the MP-8150-CPE uses a static IP address, switching to DHCP mode could remedy this problem. Also see [Setting the IP Address with ScanTool](#).
- There is too much network traffic.

8.4.3 Device Has Incorrect IP Address

1. Default IP Address Assignment mode is **Dynamic**. If you do not have a DHCP server on your network, the default IP Address is 169.254.128.132 for the device. If you have more than one unit with default IP address connected to the network, you will not be able to communicate with them (due to an IP address conflict). In this case, assign each unit a unique static IP address via the serial cable or turn off all units but one and change the IP address using ScanTool one at a time.
2. The unit only contacts a DHCP server during boot-up. If your network's DHCP server is not available while the unit is booting, the device will use the default IP address (169.254.128.132 for the device). Reboot the unit once your DHCP server is on-line again or use the ScanTool to find the unit's current IP address.
3. To find the unit's current IP address if using DHCP, open the IP Client Table in the DHCP Server and match the unit's IP address to its MAC address (found on the product label). Alternatively, use ScanTool to identify the unit's current IP address.
4. Once you have the current IP address, use the HTTP or CLI Interface to change the unit's IP settings, if necessary.
5. If you use static IP Address assignments and cannot access the unit over Ethernet, follow the *Initializing the IP Address using CLI* procedure. Once the IP Address is set, you can use the Ethernet Interface to complete configuration. If the device contains the default or known IP and is not accessible, then you need to check the Management VLAN configuration.
6. Configure the device to "DHCP" mode and reboot. While bootup, if there is a DHCP Server on the network, the DHCP Server will assign an IP Address to the unit.

8.4.4 HTTP Interface Does Not Work

1. Make sure you are using a compatible browser:
 - Microsoft Internet Explorer 6 with Service Pack 1 or later
 - Mozilla Firefox 3.0 and above.
2. Make sure you have the proper IP address. Enter your unit's IP Address in the browser address bar, similar to this example: http://192.168.1.100. When the Enter Network Password window appears, enter the User Name and enter the HTTP password in the Password field. The default HTTP username is **admin** and password is **public**.
3. Use the CLI over the serial port to check the IP Access Table, which may be restricting access to HTTP.

8.4.5 Telnet CLI Does Not Work

1. Make sure you have the proper IP Address. Enter your device IP address in the Telnet connection dialog, from a DOS prompt, type: C:\> telnet <Device IP Address>
2. Use the CLI over the serial port to check the IP Access Table, which may be restricting access to Telnet and HTTP.

8.4.6 TFTP Server Does Not Work

With TFTP, you can transfer files to and from the MP-8150-CPE device. Also see [TFTP Server Setup](#). If a TFTP server is not properly configured and running, you cannot upload and download files.

The TFTP server:

- Can be situated either local or remote
- Must have a valid IP address

- Must be set for send and receive without time-out
- Must be running only during file upload and download

If the TFTP server does not upload or download files, it could mean:

- The TFTP server is not running
- The IP address of the TFTP server is invalid
- The upload or download directory is not correctly set
- The file name is not correct

8.4.7 Setting IP Address using Serial Port

Use the following procedure to set an IP address over the serial port using the CLI. The network administrator typically provides the device IP address.

8.4.7.1 Hardware and Software Requirements

- Standard cross-over serial data (RS-232) cable (not included with shipment).
- ASCII Terminal software, such as HyperTerminal.

8.4.7.2 Attaching the Serial Port Cable

1. Connect one end of the serial cable to the unit and the other end to a serial port on your computer.
2. Power on the computer and unit, if necessary.

8.4.7.3 Initializing the IP Address using CLI

After installing the serial port, you may use the CLI to communicate with the device. CLI supports most generic terminal emulation programs, such as HyperTerminal (which is included with the Windows operating systems). In addition, many web sites offer shareware or commercial terminal programs you can download. Once the IP address has been assigned, you can use the HTTP interface or the CLI over Telnet to complete the configuration.

Follow these steps to assign the MP-8150-CPE unit an IP address:

1. Open your terminal emulation program (like HyperTerminal) and set the following connection properties:
 - Com Port: <COM1, COM2, etc., depending on your computer>
 - Baud rate: 115200
 - Data Bits: 8
 - Stop bits: 1
 - Flow Control: None
 - Parity: None
2. Press the REBOOT button on the PoE of the unit.

The terminal display shows Power On Self Tests (POST) activity, displays the software version, and prompts to enter the CLI username and password similar to the example below. This process may take up to 90 seconds.

```
##### |
# +---+---+---+---+---+
# |p||r||o||x||i||m|
# +---+---+---+---+---+
# Version: 1.0.0 B208230
# Architecture: MIPS 9600
```



```
# Creation: 25-Aug-2009 (IST) 08:16:14 PM
#####
```

```
Username: admin
```

```
Password:
```

3. Enter the CLI Username and password (default username is **admin** and password is **public**). The terminal displays a welcome message and then the CLI Prompt:

```
System Name>
```

4. Enter show configure network to find the current IP address of the device.
5. Change the IP address and other network values using the following CLI commands, similar to the example below (use your own IP address and subnet mask).

```
System Name> enable
```

```
System Name# configure
```

```
System Name(config)#network
```

```
System Name(config-net)# ip
```

```
System Name(config-net-ip)# ethernet-ip-table
```

```
System Name(config-net-ip-etherip)# index 1 ipaddress <ipaddress>
```

```
System Name(config-net-ip-etherip)# index 1 mask <subnet mask>
```

```
System Name(config-net-ip-etherip)# index 1 address-type <Address Type>
```

```
System Name(config-net-ip-etherip)# default-gateway <IP Gateway>
```

```
System Name(config-net-ip)# default-gateway <IP Gateway>
```

```
System Name(config-net-ip-etherip)#exit
```

```
System Name(config-net-ip)#exit
```

```
System Name(config-net)#exit
```

```
System Name(config)# commit 1
```

```
System Name(config)# reboot 1
```

6. After the unit reboots, verify the new IP address by reconnecting to the CLI and enter a show configure network command. Alternatively, you can ping the device from a network computer to confirm that the new IP address has taken effect.
7. When the proper IP address is set, use the HTTP interface or CLI over Telnet to configure the rest of the unit's operating parameters.

8.4.8 TFTP Server

The "Trivial File Transfer Protocol" (TFTP) server allows you to transfer files across a network. You can upload the configuration files from the unit for backup or copying, and you can download configuration files or new firmware. The TFTP software is located on the installation CD. If a TFTP server is not configured and running, you will not be able to download and upload software and configuration files to/from the device. Remember that the TFTP server does not have to be local, so long as you have a valid TFTP IP address. Note that you do not need a TFTP server running unless you want to transfer files to or from the device.

After the TFTP server is installed:

- Check to see that TFTP is configured to point to the directory containing the device Image.

- Make sure you have the proper TFTP server IP Address, the proper device firmware name, and that the TFTP server is connected.
- Make sure the TFTP server is configured to both Transmit and Receive files (on the TFTP server's **Security** tab), with no automatic shutdown or time-out (on the **Auto Close** tab).

8.4.9 Recovery Procedures

The most common installation problems relate to IP addressing. For example, without the TFTP server IP Address, you will not be able to download a new device firmware to the unit. IP Address management is fundamental. We suggest you to create a chart to document and validate the IP addresses for your system. If the password is lost or forgotten, you will need to reset the unit to default values. The Soft Reset to Factory Defaults and Hard Reset to Factory Defaults procedures reset configuration settings, but do not change the current device firmware.

If the device has a corrupted firmware, follow the Forced Reload procedure to erase the current AP Image and download a new firmware.

8.4.10 Soft Reset to Factory Defaults

Use this procedure to reset the network configuration values, including the password, IP address, and subnet mask. The current unit Image is not deleted.

1. Click **Management > Reset to Factory**.
2. Click **Reset to Factory Default**. The device is reset to its factory default state.
3. The default IP address that the unit resets to is 169.254.128.132 for the device. If you want to make modification to the IP address setting, use the ScanTool or CLI. See Using CLI to Manage the Access Point for CLI information.

If you do not have access to the HTTP or CLI interfaces, use the procedure described in Hard Reset to Factory Defaults.

8.4.11 Hard Reset to Factory Defaults

If you cannot access the unit or you have lost its password, you can reset the unit to the factory default settings. Resetting to default settings leads to configuring the unit anew.

To reset to factory default settings, press and hold the **RELOAD** button on the side of the unit's PoE power supply or **RELOAD** button on the unit for 5 seconds. The current configuration is deleted from the unit and the unit reboots, with factory defaults.

CAUTION: *It you hold the RELOAD button for longer than 10 seconds, you may go into Forced Reload mode, which erases the unit's embedded software.*

8.4.12 Forced Reload

With Forced Reload, you bring the unit into bootloader mode by erasing the embedded software. Use this procedure only as a last resort if the unit does not boot and the procedure did not help.

CAUTION: *By completing this procedure, the embedded software in the unit will be erased. You will need to reload the software before the unit is operational.*

To do a forced reload

1. Reset the unit by resetting the power plug of PoE.
2. Press and hold the **RELOAD** button which is located on the PoE or **RELOAD** button on the unit for about 20 seconds. The unit deletes the current firmware.
3. Unit will try to load the required firmware using the default factory configuration parameters. If this fails, then it will enter either CLI mode or ScanTool mode as per the user's choice, with a message on the serial console "Starting ScanTool interface, press any key to enter CLI 5". Follow one of the procedures below to load a new firmware to the unit:

- Download a New Image Using ScanTool
- Download a New Image Using the Bootloader CLI

Because the CLI option requires a physical connection to the unit's serial port, Proxim recommends the ScanTool Option.

8.4.13 VLAN Operation Issues

The correct VLAN configuration can be verified by "pinging" both wired and wireless hosts from both sides of the device and the network switch. Traffic can be "sniffed" on the wired (Ethernet), if configured. Bridge frames generated by wireless clients and viewed on one of the backbones should contain IEEE 802.1Q compliant VLAN headers or tags. The VLAN ID in the headers should correspond to one of the VLAN User IDs configured for the unit.

The correct VLAN assignment can be verified by pinging:

- The unit to ensure connectivity
- The switch to ensure VLAN properties This should be checking not pinging
- Hosts past the switch to confirm the switch is functional

Ultimately, traffic can be "sniffed" on the Ethernet interface using third-party packages. Most problems can be avoided by ensuring that 802.1Q compliant VLAN tags containing the proper VLAN ID have been inserted in the bridged frames. The VLAN ID in the header should correspond to the assigned VLAN.

What if network traffic is being directed to a nonexistent host?

- All sessions are disconnected, traffic is lost, and a manual override is necessary.
- Workaround: You can configure the switch to mimic the nonexistent host.

I have just configured the Management ID and now I can't manage the device.

- Check to ensure your password is correct. If your password is incorrect or all inbound packets do NOT have the correct tag, then a Forced Reload is necessary.

CAUTION: *The Forced Reload procedure disconnects all users and resets all values to factory defaults.*

8.4.14 Changes Do Not Take Effect

Changes made in the Web Interface do not take effect:

1. Restart your Web browser.
2. Log into the radio unit again and make changes.
3. Reboot the radio unit when prompted to do so.

Wait until the reboot is completed before accessing the unit again.

8.4.15 Link Problems

While wireless networking emerges more and more, the number of wireless connections to networks grows every day. To successfully use the connections, technicians must be able to troubleshoot the system effectively. This section gives hints on how a Quick Bridge network could be analyzed in the case of "no link", a situation in which the customer thinks that the link is down because there is no traffic being passed.

The four general reasons that a wireless link may not work are related to:

- Hardware
- Configuration
- Path issues (such as distance, cable loss, obstacles)
- Environment (anything that is outside the equipment and not part of the path itself)

You have tested the equipment in the office and have verified that the hardware and configurations are sound. The path calculation has been reviewed, and the path has been double-checked for obstacles and canceling reflections. Still, the user reports that the link does not work.

Most likely, the problem reported is caused by the environment or by improper tests to verify the connection. The test method, cabling, antennas, and antenna alignment have been checked. Always do this before checking the environment.

8.4.16 General Check

Two general checks are recommended before taking any action:

- Check whether the software version on all devices is the most current version.
- Check for any reported alarm messages in the Event Log.

8.4.17 Statistics Check

Interference and other negative environment factors always have an impact on the number of correctly received frames. The Tsunami MP-8150-CPE models give detailed information about transmission errors in the Web interface, under Monitor (Section/Window etc.).

The windows that are important for validating the health of the link are:

- Monitor / Wireless Statistics: Check FCS errors: Rising FCS errors indicate interference or low fade margin. So does Failed count. If only one of those is high, this indicates that a source of interference is significant near one end of the link.
- Monitor / Ethernet Statistics: The information is given after the wireless Ethernet frame is converted into a normal Ethernet frame. The parameters shown are part of the MIB-II.
 - Both operational and admin status should be up. An admin status of down indicates that the interface is configured to be down.
 - In Discards and Out Discards indicate overload of the buffers, likely caused by network traffic, which is too heavy.
 - In Errors and Out Errors should never happen; however, it might happen if a frame's FCS was correct while the content was still invalid.
- Monitor / Wireless / WORM (Statistics on WORM): WORM runs on top of normal Ethernet, which means that the WORM frame is in fact the data field of the Ethernet frame. Send Failure or Send Retries must be low in comparison to Send Success. Low is about 1%. The same applies for Receive Success versus Receive Retries and Receive Failures. Note that the Receive Failures and Retries can be inaccurate. A frame from the remote site might have been transmitted without even being received; therefore, the count of that frame might not have been added to the statistics and the receiver simply could not know that there was a frame.
 - Remote Partners indicates whether a BSU is connected.

8.4.18 Analyzing the Spectrum

The ultimate way to discover whether there is a source of interference is to use a spectrum analyzer. Usually, the antenna is connected to the analyzer when measuring. By turning the antenna 360 degrees, one can check from which direction the interference is coming. The analyzer will also display the frequencies and the level of signal is detected. Proxim recommends performing the test at various locations to find the most ideal location for the equipment.

8.4.18.1 Avoiding Interference

When a source of interference is identified and when the level and frequencies are known, the next step is to avoid the interference. Some of the following actions can be tried:

- Changing the channel to a frequency away from the interference is the first step in avoiding interference. The installer can select a DFS Preferred Channel.
- Each antenna has a polarization; try to change to a polarization different from the interference.

- A small beam antenna looks only in one particular direction. Because of the higher gain of such an antenna, lowering the output power or adding extra attenuation might be required to stay legal. This solution cannot help when the source of interference is right behind the remote site.
- Lowering the antennas can help avoid seeing interference from far away.

Move the antennas to a different location on the premises. This causes the devices to look from a different angle, causing a different pattern in the reception of the signals. Use obstructions such as buildings, when possible, to shield from the interference.

8.4.18.2 Conclusion

A spectrum analyzer can be a great help to identify whether interference might be causing link problems on Tsunami MP-8150-CPE devices.

Before checking for interference, the link should be verified by testing in an isolated environment, to make sure that the hardware works and your configurations are correct. The path analysis, cabling and antennas should be checked as well.

Statistics in the web interface under Monitor indicates if there is a link, if the link is healthy, and a continuous test can be done using the Link Test.

- Base Announces should increase continuously.
- Registration Requests and Authentication Requests should be divisible by 3. WORP is designed in a way that each registration sequence starts with 3 identical requests. It is not a problem if, once in a while, one of those requests is missing. Missing requests frequently is to be avoided.
- Monitor / Per Station (Information per connected remote partner): Check that the received signal level (RSL) is the same on both sides. This should be the case if output power is the same. Two different RSLs indicate a broken transmitter or receiver. A significant difference between Local Noise and Remote Noise could indicate a source of interference near the site with the highest noise. Normally, noise is about -80 dBm at 36 Mbps. This number can vary from situation to situation, of course, also in a healthy environment.
- Monitor / Link Test (Information used by Administrators for on-the-spot checking): Check the received signal level (RSL) and noise level. Compare the RSL with the values from path analysis. If the figures differ significantly from the values recorded at the Per Station window, check for environment conditions that change over time.

Frequency Domains and Channels

Introduction

The Tsunami MP-8150-CPE is available in two SKUs one for US (US) and the Other for World (WD) Markets. Depending on the SKU, the device is hard programmed at factory to that Regulatory domain. Regulatory domain controls the list of frequency domains that are available in that SKU. Further each frequency domain will define the country specific regulatory rules and frequency bands. This is a configurable option.

The frequency domain can be easily configured using the WEB Interface as it is a drop down list with all the available domains. When using with CLI/SNMP, care has to be taken to set the domains using a predefined ENUM value. Below is the list of all available frequency domains in each SKU with their corresponding ENUM value in the braces:

For US SKU

- United States 5.8 GHz (1)

For World SKU

- World 5 GHz (3)
- World 4.9 GHz (4)
- Canada 5 GHz (8)
- Europe 5.8 GHz (9)
- Europe 5.4 GHz (10)
- Russia 5 GHz (12)
- Taiwan 5 GHz (13)
- United States 5 GHz (14)
- Canada 5.8 GHz (15)

Example: To set WORLD 5 GHz as Frequency Domain using CLI

```
System Name#configure
System Name(config)# system-configure
System Name(config-sysconfig)# frequency-domain ?
Possible completions:
<unitedstatesall (1), unitedstatesad hoc (2), unitedstates2p4 (3), worldall (4), w
orld4p9ghz (5), world2p4ghz (6), world2p3ghz (7), world2p5ghz (8), canada5ghz (9) ,
europe5p8ghz (10), europe5p4ghz (11), europe2p4ghz (12), russia5ghz (13), taiwan5
ghz (14), unitedstates5ghz (15), canada5p8ghz (16)>      configure the
Frequency Domain
System Name(config-radio)# interface 1 frequency-domain 4

Note:Changes in Frequency Domain requires Reboot.
```

5 GHz Channels/Frequencies by Country

Frequency Domain	Frequency Band	DFS	Allowed Channels (Center Frequency) for 20 MHz	Allowed Channels for 40 PLUS MHz	Allowed Channels for 40 MINUS MHz
United States 5 GHz	5.26 ~ 5.32 GHz. (DFS) 5.50 ~ 5.70 GHz. (DFS) 5.745 ~ 5.825 GHz. (Non-DFS)	DFS	52(5260), 56(5280), 60(5300), 64(5320), 100(5500), 104(5520), 108(5540), 112(5560), 116(5580), 120(5600), 124(5620), 128(5640), 132(5660), 136(5680), 140(5700). 149(5745), 153(5765), 157(5785), 161(5805), 165(5825).	52(5260), 60(5300). 100(5500), 108(5540), 116(5580), 124(5620), 132(5660), 149(5745), 157(5785),	56(5280), 64(5320). 104(5520), 112(5560), 120(5600), 128(5640), 136(5680), 153(5765), 161(5805).
United States 5.8 GHz	5.745 ~ 5.825 GHz. (Non-DFS)	Non-DFS	149(5745), 153(5765), 157(5785), 161(5805), 165(5825).	149(5745), 157(5785)	153(5765), 161(5805).
World 5 GHz	5.160 ~ 6.070 GHz	Non-DFS	32(5160), 33(5165), 34(5170).... 214(6070)	32(5160), 33(5165), 34(5170)... 210(6050)	36(5180), 37(5185), 38(5190)... 214(6070)
WORLD 4.9 GHz	4950 ~ 4990 GHz	Non-DFS	20(4950), 30(4955), 40(4960), 50(4965), 60(4970), 70(4975), 80(4980), 90(4985).	20(4950), 30(4955), 40(4960), 50(4965),	60(4970), 70(4975), 80(4980), 90(4985)
CANADA 5 GHz	5.260 ~ 5.320 GHz (DFS) 5.500 ~ 5.580 GHz (DFS) 5.660 ~ 5.700 GHz (DFS)	DFS	52(5260), 56(5280), 60(5300), 64(5320). 100(5500), 104(5520), 108(5540), 112(5560), 116(5580), 132(5660), 136(5680), 140(5700). 149(5745), 153(5765), 157(5785), 161(5805), 165(5825).	52(5260), 60(5300), 100(5500), 108(5540), 132(5660), 149(5745), 157(5785)	56(5280), 64(5320). 104(5520), 112(5560), 136(5680), 153(5765), 161(5805)
EUROPE 5.8 GHz	5.740 ~ 5.850 GHz	DFS	148(5740), 152(5760), 156(5780), 160(5800), 164(5820), 168(5840), 172(5860)	148(5740), 156(5780), 164(5820)	152(5760), 160(5800), 168(5840).
EUROPE 5.4 GHz	5.500 ~ 5.580 GHz 5.660 ~ 5.700 GHz	DFS	100(5500), 104(5520), 108(5540), 112(5560), 116(5580), 132(5660), 136(5680), 140(5700).	100(5500), 108(5540), 132(5660)	104(5520), 112(5560), 136(5680)
RUSSIA 5 GHz	5.160 ~ 6.070 GHz	Non-DFS	32(5160), 33(5165), 34(5170).... 214(6070)	32(5160), 33(5165), 34(5170)....210(6050)	36(5180), 37(5185), 38(5190)....214(6070)

Frequency Domains and Channels

Frequency Domain	Frequency Band	DFS	Allowed Channels (Center Frequency) for 20 MHz	Allowed Channels for 40 PLUS MHz	Allowed Channels for 40 MINUS MHz
Taiwan 5 GHz	5.500 ~ 5.700 GHz (DFS). 5.745 ~ 5805 GHz (Non-DFS).	DFS	100(5500), 104(5520), 108(5540), 112(5560), 116(5580), 120(5600), 124(5620), 128(5640), 132(5660), 136(5680), 140(5700), 149(5745), 153(5765), 157(5785), 161(5805)	100(5500), 108(5540), 116(5580), 124(5620), 132(5660), 149(5745), 157(5785),	104(5520), 112(5560), 120(5600), 128(5640), 136(5680), 153(5765), 161(5805).
United States 5 GHz	5.26 ~ 5.32 GHz. (DFS) 5.50 ~ 5.70 GHz. (DFS) 5.745 ~ 5.825 GHz. (Non-DFS)	DFS	52(5260), 56(5280), 60(5300), 64(5320), 100(5500), 104(5520), 108(5540), 112(5560), 116(5580), 120(5600), 124(5620), 128(5640), 132(5660), 136(5680), 140(5700), 149(5745), 153(5765), 157(5785), 161(5805), 165(5825).	52(5260), 60(5300), 100(5500), 108(5540), 116(5580), 124(5620), 132(5660), 149(5745), 157(5785),	56(5280), 64(5320), 104(5520), 112(5560), 120(5600), 128(5640), 136(5680), 153(5765), 161(5805).
CANADA 5.8 GHz	5.740 ~ 5.850 GHz	Non-DFS	148(5740), 152(5760), 156(5780), 160(5800), 164(5820), 168(5840).	148(5740), 156(5780), 164(5820),	152(5760), 160(5800), 168(5840).

NOTE: While choosing a 40 MHz bandwidth, you can select 40 PLUS or 40 MINUS. 40 PLUS means the center frequency calculation is to be done for 20 MHz and add another 20 MHz to the top edge of 20 MHz. 40 MINUS means the center frequency calculation is to be done for 20 MHz and add another 20 MHz to the bottom edge of 20 MHz.

Details for 40MHz Bandwidth

For 40 PLUS

- 5 GHz -> Channel 52 = 5260
- Bandwidth starts from 5250 and ends at 5290

For 40 MINUS

- 5 GHz -> Channel 56 = 5280
- Bandwidth starts from 5250 and ends at 5290

Dynamic Frequency Selection (DFS)

The Tsunami MP-8150-CPE supports Dynamic Frequency Selection (DFS) for FCC, IC, and ETSI regulatory domains per FCC Part 15 Rules for U-NII devices, IC RSS-210, and ETSI EN 301-893 and 302-502 regulations, respectively. These rules and regulations require that the devices operating in the 5 GHz band must use DFS to prevent interference with radar systems.

Radar detection is performed only by the BSU and not by the SU. When an SU is set to a country/band in which DFS is used, it passively scans all available channels upon startup looking for a BSU that best matches its connection criteria (such as BSU Node System Name, Network Name, and Shared Secret). The SU connects to the BSU automatically on whatever frequency

the BSU has selected. Because of this procedure, it is best to set up the BSU and have it fully operational before installing the SU, although this is not required. If a BSU rescans because of radar interference, the SU loses its wireless link. The SU waits for 30 seconds and if it finds that it could not receive the BSU in this amount of time, it rescans the available frequencies for an available BSU.

Boot Loader CLI and ScanTool

Boot Loader CLI

The Boot Loader CLI is a minimal subset of the normal CLI used to perform initial configuration of the unit. The Boot Loader CLI is available when the unit's embedded software is not running.

This interface is only accessible through the serial interface, if:

- The device does not contain a software image
- An existing image is corrupted
- An automatic (default) download of image over TFTP has failed.

The Boot Loader CLI provides you with the ability to configure the initial setup parameters; and depending on this configuration, a software file is downloaded to the device during startup.

The Boot Loader CLI supports the following commands:

- **factory_reset**: Restore the factory settings
- **help**: Print Online Help
- **reboot**: Reboot the device
- **set**: Set the parameters
- **show**: Show the parameters

The Boot Loader CLI supports the following parameters (for viewing and modifying):

- **ipaddr**: IP Address
- **systemname**: System Name
- **gatewayip**: Gateway IP Address
- **serverip**: Server IP Address
- **ipaddrtype**: IP Address Type
- **netmask**: Net Mask
- **filename**: Image file name (including the file extension)

If the Boot Loader fails to load the firmware from flash, it tries to get the firmware from the network. The default configuration of the Boot Loader parameters are as follows:

Parameter	Value
ipaddr	169.254.128.132
netmask	255.255.255.0
gatewayip	169.254.128.132
systemname	systemname
serverip	169.254.128.133
filename	imagenam
ipaddrtype	dynamic

To Load the Firmware from the Network

- Use the **show** command to view the parameters and their values and use the **set** command to set the values to the parameters as per the requirement.

To Get the IP Parameters Dynamically for Loading the Firmware

1. Set the ipaddrtype to dynamic.
2. Run the BOOTP and TFTP Servers along with a reboot of the unit.

When the device reboots, the device gets the IP Address and Boot filename from the BOOTP server. You need not change any of the above parameters. After BOOTP succeeds, the device initiates a TFTP request with the filename it gets from BOOTP.

To Load the Firmware by Using Static IP Parameters

1. Use the **set** command to set the IP parameters like 'ipaddr', 'serverip', 'filename' and also set the parameter 'ipaddrtype' to static.
2. Run the TFTP Server along with a reboot of the unit.

When the device reboots, the TFTP request is initiated with the value taken from the parameter "filename". This request is sent to the IP address set to the parameter "serverip". In this case, the TFTP Server should be reachable to the device.

ScanTool

If you want to access the device with Scantool, then the host running the ScanTool should also be in the same network as the device. The ScanTool broadcast requests are discarded by the routers if the device and the host running the ScanTool are in different network. This means that the ScanTool cannot discover the device.

A device in Boot Loader can be recognized by looking at the system description. If the system description does not contain any build number in braces, conclude that the device is in Boot Loader mode.

For example:

MP-8150-CPE	is the name of the board
WD	is the Regulatory Domain
V3.0.1	is the Firmware Version

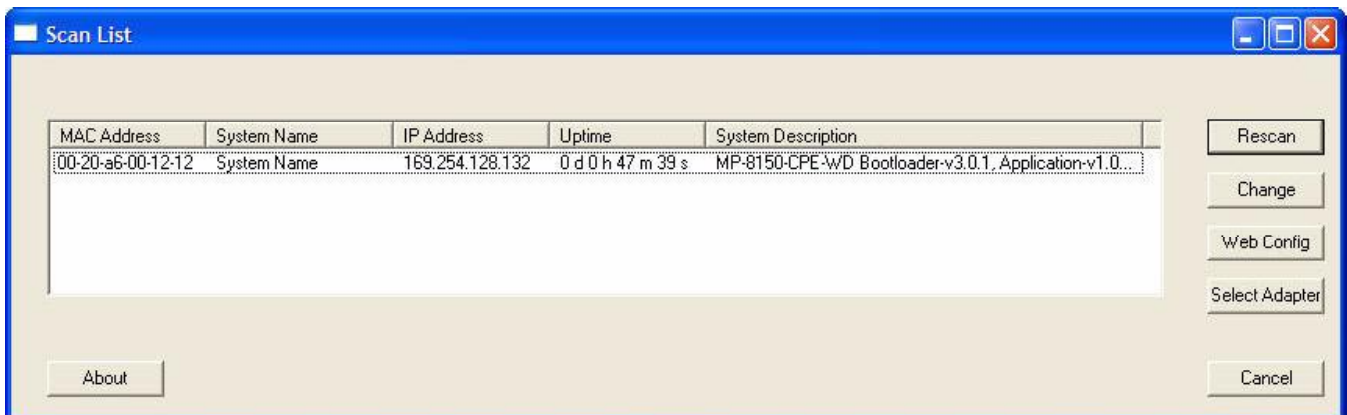


Figure B-1 Scan Tool View of a Device in Boot Loader Mode

Technical Specifications

This chapter provides information on the following topics:

- [Part Numbers](#)
- [Regulatory Approval and Frequency Domains](#)
- [Integrated Panel Antenna Specifications](#)
- [Radio and Transmission Specifications](#)
- [OFDM Modulation Rates](#)
- [Wireless Protocol](#)
- [Interfaces](#)
- [Transmit Power Settings](#)
- [Receive Sensitivity](#)
- [Receive Sensitivity](#)
- [Latency](#)
- [Management](#)
- [Power Supply](#)
- [LEDs](#)
- [Software Features](#)
- [Hardware Specifications](#)
- [Physical and Environmental Specifications](#)
- [MTBF and Warranty](#)

Part Numbers

MP-8150-CPE Units

Model #	CPN #	Description
MP-8150-CPE-US	76795	Tsunami MP 8150, Customer Premises Equipment, 5 GHz, MIMO 2X2, 16 dBi Integrated antenna - US PoE
MP-8150-CPE-WD	76796	Tsunami MP 8150, Customer Premises Equipment, 5 GHz, MIMO 2X2, 16 dBi Integrated antenna - WD PoE

Accessories

Outdoor Ethernet Cables	
76590	25m, RJ45 terminated, UV Rated, STP CAT5e cable for outdoor use
76591	50m, RJ45 terminated, UV Rated, STP CAT5e cable for outdoor use
76592	75m, RJ45 terminated, UV Rated, STP CAT5e cable for outdoor use
Miscellaneous	
76394	Gigabit Ethernet PoE (Power-over-Ethernet) Surge Arrestor
1087-UMK	Proxim universal pole mounting kit

Regulatory Approval and Frequency Domains

- **Regulatory Certifications:** FCC, IC and ETSI

5 GHz Channels/Frequencies

Region/Country	Frequency Domain	Frequency Band (GHz)	No. of Channels		
			40 PLUS MHz	40 MINUS MHz	20 MHz
North America	United States 5 GHz	5.26 ~ 5.32, 5.50 ~ 5.70, 5.745 ~ 5.825	Up to 9	Up to 9	Up to 20
	United States 5.8 GHz	5.745 ~ 5.825	Up to 2	Up to 2	Up to 5
	Canada 5 GHz	5.260 ~ 5.320 5.500 ~ 5.580 5.660 ~ 5.700	Up to 5	Up to 5	Up to 12
	Canada 5.8 GHz	5.740 ~ 5.850	Up to 3	Up to 3	Up to 6
EU Countries	Europe 5.8 GHz	5.740 ~ 5.865	Up to 3	Up to 3	Up to 7
	Europe 5.4 GHz	5.500 ~ 5.580 5.660 ~ 5.700	Up to 3	Up to 3	Up to 8
	Russia 5 GHz	5.160 ~ 6.070	Up to 178	Up to 178	Up to 182
APAC	Taiwan 5 GHz	5.500 ~ 5.700 5.745 ~ 5.805	Up to 7	Up to 7	Up to 15
World	World 5 GHz	5.160 ~ 6.070	Up to 178	Up to 178	Up to 182
	World 4.9 GHz	4.950 ~ 4.980	Up to 3	Up to 3	Up to 7
	United States 5 GHz	5.26 ~ 5.32 5.50 ~ 5.70 5.745 ~ 5.825	Up to 9	Up to 9	Up to 20

Integrated Panel Antenna Specifications

Feature	Specification
Frequency band	5.3 – 6.1 GHz
Gain	15-16 dBi
3dB Beamwidth	16.5°-20.5° (Hplane)

Feature	Specification
3dB Beamwidth	15°-19° (Eplane)
Polarization	Dual (Vertical + Horizontal)
Cross Polarization	-25 dB
Isolation	20 dB
Power Handling	2 W (cw)
VSWR	2.0:1 Max
Cable	Phi 1.32, 160 mm x 2
Connector	U.FL X 2
Standard Compliance	Co-pol. ETSI EN 302 085 V1.2.3 TS1 – TS2

Radio and Transmission Specifications

Category	Specification
Modulation Method	OFDM
Radio Speeds	Upto 300 Mbps

OFDM Modulation Rates

NOTE: Maximum packet size: 1526 Bytes.

Data Rate		40 MHz		20 MHz
		GI 400 ns	GI 800 ns	GI 800 ns
Single Stream	BPSK 1/2	15	13.5	6.5
	QPSK 1/2	30	27	13
	QPSK 3/4	45	40.5	19.5
	16QAM 1/2	60	54	26
	16QAM 3/4	90	81	39
	64QAM 2/3	120	108	52
	64QAM 3/4	135	121.5	58.5
	64QAM 5/6	150	135	65

Data Rate		40 MHz		20 MHz
Dual Stream	BPSK 1/2	30	27	13
	QPSK 1/2	60	54	26
	QPSK 3/4	90	81	39
	16QAM 1/2	120	108	52
	16QAM 3/4	180	162	78
	64QAM 2/3	240	216	104
	64QAM 3/4	270	243	117
	64QAM 5/6	300	270	130

Wireless Protocol

Category	Specification
Wireless Protocol	WORP (Wireless Outdoor Router Protocol)

Interfaces

Category	Specification
Wired Ethernet	One auto MDI-X RJ45 Gigabit Ethernet – Port #1 with PoE in & Data (802.3af compliant)
Serial Connector	RS-232

Transmit Power Settings

- Output Power Attenuation: 0 – 18 dB, in 1 dB steps
- Output Power Values will have a tolerance of +/-1 dB
- Total EIRP must be calculated based on integrated 16 dBi antenna gain

Modulation		Tx power for 40/20 MHz, 5 GHz
SINGLE (or) DUAL STREAM	64 QAM 5/6	13 dBm
	64 QAM 3/4	14 dBm
	64 QAM 2/3	15 dBm
	16 QAM 3/4	17 dBm
	16 QAM 1/2	17 dBm
	QPSK 3/4	17 dBm
	QPSK 1/2	17 dBm
	BPSK 1/2	17 dBm

Receive Sensitivity

NOTE: Rx Sensitivity values should be considered with a tolerance +/- 2 dB.

Channel Size	40 MHz	20 MHz
Frequency	5 GHz	5 GHz
BPSK 1/2	-87	-93
BPSK 3/4	-86	-90
QPSK 1/2	-85	-88
QPSK 3/4	-82	-85
16-QAM 1/2	-80	-80
16-QAM 3/4	-75	-78
64-QAM 2/3	-74	-75
64-QAM 3/4	-71	-75

Latency

Category	Specification
Typical at Max Latency	5 msec (typical)

Management

Category	Specification
Local	RS232 serial CLI (up to 115200 bps)
Remote	<ul style="list-style-type: none"> • Telnet and SSH, Web GUI (http) and SSL (https), TFTP • SNMP v1, v2c and v3 • SNMP trap and Syslog

Power Supply

Category	Specification
Input Voltage	<ul style="list-style-type: none"> • Via RJ-45 Ethernet interface supplying 48v and 0.67A on Ethernet Port • 12 V-DC through serial port DB9 Connector (only for debugging) • Consumption 5.3 Watt typical
Power over Ethernet Injector	<ul style="list-style-type: none"> • Input: 100 – 250 V-AC (47 – 63 Hz) • Output: 48 V-DC at 0.67 A (32 Watt) • Pin-out: +48 V-DC on pins 4/5, -48 V-DC on pins 7/8 • Size: 5.24x2.13x1.42 inches (133x54x36 mm) • Weight: 7 ounces (200 g) • Temp: 0 to 40 °C

LEDs

Category	Specification
Types	Power Radio Activity Ethernet Activity Reload

Software Features

Category	Specification
Key Features	<ul style="list-style-type: none"> • WORP protocol • Transmit Power Control • Antenna Alignment • Integrity Check for Software Upload • Satellite Density • Enhanced Frequency Selection

Category	Specification
Bridging and Routing	<ul style="list-style-type: none"> • Bridge (802.1d) • IP/ RIPv1 (RFC 1058) • IP/ RIPv2 (RFC 1388) • CIDR (RFC 1519) • ICMP (RFC 792) • IP (RFC 791) • ARP (RFC 826)
Filtering	<ul style="list-style-type: none"> • Ethernet protocol (Ethertype) • Static MAC • IP address • Broadcast protocol
Services	<ul style="list-style-type: none"> • DHCP Server (RFC 2131) • DHCP Client (RFC 2131) • Bi-Directional Bandwidth Control • NAT (RFC 3022) • DHCP Relay (RFC 2131)
Security Features	<ul style="list-style-type: none"> • Critical feature support via WORM for secure long-range wireless deployments in unlicensed frequency spectrum • MD5 (embedded in WORM) authentication between BSU and SU • Secure "over the air encryption" and AES-CCM, WEP and TKIP
Tools	<ul style="list-style-type: none"> • Site Survey • Link Test to determine the local/remote signal/noise levels.
Management Interface	Flexible and responsive management interfaces through Web, CLI and SNMP. SNMPv3 support facilitates secure management.

Hardware Specifications

Category	Specification
Radio	5 GHz MIMO dual band radio
Clock Speed	400 MHz
Memory	Flash: 8 MB RAM: 64 MB
Input Power	Power-over-Ethernet 48 VDC, 0.67 A

Physical and Environmental Specifications

Category	Specification
Physical	
Dimensions (L x W x H)	4.0 x 8.5 x 10.2 inches (98 x 215 x 259 mm)
Weight	2.4 lbs (1.02 kg)
Environmental	
Storage Temperature	-55° to 80°C (-41° to 176° Fahrenheit)
Operating Temperature	-30° to 60°C (-22° to 140° Fahrenheit)
Humidity	100% (non-condensing)

MTBF and Warranty

Category	Specification
MTBF	>167750 hours
Warranty	1 year parts and labor; ServPak extended support available

Regulatory Compliance Information

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment.

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.

IMPORTANT NOTE

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 50 cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 50 cm between the radiator & your body.

CAUTION: The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.

CAUTION: High power radars are allocated as primary users (meaning they have priority) of 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- EN60950-1: 2006
Safety of Information Technology Equipment
- EN 50385: 2002
Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public
- EN 301 489-1 V1.8.1 (2008-04)
Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- EN 301 489-17 V1.3.2 (2008-04)
Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 5 GHz high performance RLAN equipment
- EN 301 893 V1.4.1 (2007-07)
Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive

This device is a 5 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy, the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information, the end-user should contact the national spectrum authority in France.

CE 0560

Česky [Czech]	<i>[Jméno výrobce]</i> tímto prohlašuje, že tento <i>[typ zařízení]</i> je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
da Dansk [Danish]	Undertegnede <i>[fabrikantens navn]</i> erklærer herved, at følgende udstyr <i>[udstyrets typebetegnelse]</i> overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
de Deutsch [German]	Hiermit erkläre <i>[Name des Herstellers]</i> , dass sich das Gerät <i>[Gerätetyp]</i> in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
et Eesti [Estonian]	Käesolevaga kinnitab <i>[tootja nimi = name of manufacturer]</i> seadme <i>[seadme tüüp = type of equipment]</i> vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
en English	Hereby, <i>[name of manufacturer]</i> , declares that this <i>[type of equipment]</i> is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
es Español [Spanish]	Por medio de la presente <i>[nombre del fabricante]</i> declara que el <i>[clase de equipo]</i> cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ <i>[name of manufacturer]</i> ΔΗΛΩΝΕΙ ΟΤΙ <i>[type of equipment]</i> ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
fr Français [French]	Par la présente <i>[nom du fabricant]</i> déclare que l'appareil <i>[type d'appareil]</i> est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
it Italiano [Italian]	Con la presente <i>[nome del costruttore]</i> dichiara che questo <i>[tipo di apparecchio]</i> è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo <i>[name of manufacturer, /izgatavotāja nosaukums]</i> deklarē, ka <i>[type of equipment / iekārtas tips]</i> atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Siuo <i>[manufacturer name]</i> deklaruoją, kad šis <i>[equipment type]</i> atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart <i>[naam van de fabrikant]</i> dat het toestel <i>[type van toestel]</i> in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
mt Malti [Maltese]	Hawnhekk, <i>[isem tal-manifattur]</i> , jiddikjara li dan <i>[il-mudel tal-prodott]</i> jikkonforma mal-ftigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 1999/5/EC.
hu Magyar [Hungarian]	Alulírott, <i>[gyártó neve]</i> nyilatkozom, hogy a <i>[... típus]</i> megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
pl Polski [Polish]	Niniejszym <i>[nazwa producenta]</i> oświadczam, że <i>[nazwa wyrobu]</i> jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt Português [Portuguese]	<i>[Nome do fabricante]</i> declara que este <i>[tipo de equipamento]</i> está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
sl Slovensko [Slovenian]	<i>[Ime proizvajalca]</i> izjavlja, da je ta <i>[tip opreme]</i> v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	<i>[Meno výrobcu]</i> týmto vyhlasuje, že <i>[typ zariadenia]</i> spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
fi Suomi [Finnish]	<i>[Valmistaja = manufacturer]</i> vakuuttaa täten että <i>[type of equipment = laitteen tyyppimerkintä]</i> tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar <i>[företag]</i> att denna <i>[utrustningstyp]</i> står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Lightning Protection

Lightning protection is used to maximize the reliability of the communications equipment by safely re-directing current from a lightning strike or a power surge traveling along the Cat 5e/Cat 6 Ethernet cabling to the ground using the shortest path possible. Designing a proper grounding system prior to installing any communications equipment is critical to minimize the possibility of equipment damage, void warranties, and cause serious injury.

The surge arrester (sometimes referred to as a lightning protector) can protect your sensitive electronic equipment from high-voltage surges caused by discharges and transients at the PoE.

Proxim Wireless offers superior lightning and surge protection for Tsunami MP-8150-CPE series products. Contact your reseller or distributor for more information.

Statement of Warranty

Warranty Coverage

Proxim Wireless Corporation warrants that its Products are manufactured solely from new parts, conform substantially to specifications, and will be free of defects in material and workmanship for a Warranty Period of 1 year from the date of purchase.

Repair or Replacement

In the event a Product fails to perform in accordance with its specification during the Warranty Period, Proxim offers return-to-factory repair or replacement, with a thirty (30) business-day turnaround from the date of receipt of the defective Product at a Proxim Wireless Corporation Repair Center. When Proxim Wireless has reasonably determined that a returned Product is defective and is still under Warranty, Proxim Wireless shall, at its option, either: (a) repair the defective Product; (b) replace the defective Product with a refurbished Product that is equivalent to the original; or (c) where repair or replacement cannot be accomplished, refund the price paid for the defective Product. The Warranty Period for repaired or replacement Products shall be ninety (90) days or the remainder of the original Warranty Period, whichever is longer. This constitutes Buyer's sole and exclusive remedy and Proxim Wireless's sole and exclusive liability under this Warranty.

Limitations of Warranty

The express warranties set forth in this Agreement will not apply to defects in a Product caused; (i) through no fault of Proxim Wireless during shipment to or from Buyer, (ii) by the use of software other than that provided with or installed in the Product, (iii) by the use or operation of the Product in an application or environment other than that intended or recommended by Proxim Wireless, (iv) by modifications, alterations, or repairs made to the Product by any party other than Proxim Wireless or Proxim Wireless's authorized repair partners, (v) by the Product being subjected to unusual physical or electrical stress, or (vii) by failure of Buyer to comply with any of the return procedures specified in this Statement of Warranty.

Buyers should return defective Products within the first 30 days to the merchant from which the Products were purchased. Buyers can contact a Proxim Wireless Customer Service Center either by telephone or via web. Calls for support for Products that are near the end of their warranty period should be made not longer than seven (7) days after expiration of warranty. Support and repair of products that are out of warranty will be subject to a repair fee. Contact information is shown below. Additional support information can be found at Proxim Wireless's web site at <http://support.proxim.com>.

USA & Canada Customers

Call Technical Support: Phone: 408-383-7700

Toll Free: 866-674-6626

Hours: 6:00 AM to 6:00 P.M. Monday - Friday, Pacific Time

APAC Customers

Call Technical Support: Phone: +91 40 23115490

Hours: 9:00 AM to 6:00 P.M. Monday - Friday, IST (UTC/GMT +5:30 hrs)

International Customers

Call Technical Support: Phone: 408-383-7700

Hours: 6:00 AM to 6:00 P.M. Monday - Friday, Pacific Time

Hours of Operation

When contacting the Customer Service for support, Buyer should be prepared to provide the Product description and serial number and a description of the problem. The serial number should be on the product.

In the event the Customer Service Center determines that the problem can be corrected with a software update, Buyer might be instructed to download the update from Proxim Wireless's web site or, if that's not possible, the update will be sent to Buyer. In the event the Customer Service Center instructs Buyer to return the Product to Proxim Wireless for repair or replacement, the Customer Service Center will provide Buyer a Return Material Authorization ("RMA") number and shipping instructions. Buyer must return the defective Product to Proxim Wireless, properly packaged to prevent damage, shipping prepaid, with the RMA number prominently displayed on the outside of the container.

Calls to the Customer Service Center for reasons other than Product failure will not be accepted unless Buyer has purchased a Proxim Wireless Service Contract or the call is made within the first thirty (30) days of the Product's invoice date. Calls that are outside of the 30-day free support time will be charged a fee of \$250.00 (US Dollars) per Support Call.

If Proxim Wireless reasonably determines that a returned Product is not defective or is not covered by the terms of this Warranty, Buyer shall be charged a service charge and return shipping charges.

Other Information

Search Knowledgebase

Proxim Wireless stores all resolved problems in a solution database at the following URL: <http://support.proxim.com>.

Ask a Question or Open an Issue

Submit a question or open an issue to Proxim Wireless technical support staff at the following URL: <http://support.proxim.com/cgi-bin/proxim.cfg/php/enduser/ask.php>.

Technical Services and Support

Obtaining Technical Service and Support

If you are having trouble using the Proxim product, please read this manual and the additional documentation provided with your product. If you require additional support to resolve your issue, please be ready to provide the following information before you contact Proxim's Technical Services:

- Product information
 - Part number of suspected faulty unit
 - Serial number of suspected faulty unit
- Trouble/error information
 - Trouble/symptom being experienced
 - Activities completed to confirm fault
 - Network information (what kind of network are you using?)
 - Circumstances that preceded or led up to the error
 - Message or alarms viewed
 - Steps taken to reproduce the problem
- ServPak information (if a Servpak customer):
 - ServPak account number
- Registration information
 - If the product is not registered, date when you purchased the product
 - If the product is not registered, location where you purchased the product

NOTE: Technical Support is free for the first 90 days from the date of purchase.

Support Options

Proxim eService Web Site Support

The Proxim eService Web site is available 7x24x365 at <http://support.proxim.com>.

On the Proxim eService Web Site, you can access the following services:

- **New Product Registration:** Register your product to gain access to technical updates, software downloads, and free technical support for the first 90 days from receipt of hardware purchase.
- **Open a Ticket or RMA:** Open a ticket or RMA
- **Search Knowledgebase:** Locate white papers, software upgrades, and technical information.
- **ServPak Support:** Learn more about Proxim's ServPak global support service options.
- **Your Stuff:** Track status of your tickets or RMAs and receive product update notifications.
- **Provide Feedback:** Submit suggestions or other types of feedback.
- **Customer Survey:** Submit an On-Line Customer Survey response.

Telephone Support

Contact technical support via telephone as follows:

USA & Canada Customers

Call Technical Support: Phone: 408-383-7700

Toll Free: 866-674-6626

Hours: 6:00 AM to 6:00 P.M. Monday - Friday, Pacific Time

APAC Customers

Call Technical Support: Phone: +91 40 23115490

Hours: 9:00 AM to 6:00 P.M. Monday - Friday, IST (UTC/GMT +5:30 hrs)

International Customers

Call Technical Support: Phone: 408-383-7700

Hours: 6:00 AM to 6:00 P.M. Monday - Friday, Pacific Time

ServPak Support

To provide even greater investment protection, Proxim Wireless offers a cost-effective support program called ServPak. ServPak is a program of enhanced service support options that can be purchased as a bundle or individually, tailored to meet your specific needs. Whether your requirement is round the clock technical support or advance replacement service, we are confident that the level of support provided in every service in our portfolio will exceed your expectations.

- **Advanced Replacement of Hardware:** Can you afford to be down in the event of a hardware failure? Our guaranteed turnaround time for return to factory repair is 30 days or less. Those customers who purchase this service are entitled to advance replacement of refurbished or new hardware guaranteed to be shipped out by the Next Business Day. Hardware is shipped Monday – Friday, 8:00 AM – 2:00 PM (PST).
- **Extended Warranty:** Extend the life of your networking investment by adding 1, 2, or 3 years to your products standard warranty. This service coverage provides unlimited repair of your Proxim hardware for the life of the service contract. The cost of an extended warranty is far less than the cost of a repair providing a sensible return on your investment.
- **7x24x365 Technical Support:** This service provides unlimited, direct access to Proxim's world-class Tier 3 technical support engineers 24 hours a day, 7 days a week, 365 days a year including Holidays. Customers who purchase this service can rest assured that their call for technical assistance will be answered and a case opened immediately to document the problem, troubleshoot, identify the solution and resolve the incident in a timely manner or refer to an escalation manager for closure.
- **8x5 Technical Support:** This service provides unlimited, direct access to Proxim's world-class technical support 8 hours a day, 5 days a week from 8:00 AM - 5:00 PM (PST(US)). Technical Support is available at no charge for the first 90 days from the purchase date. Beyond this period, a ServPak support agreement will be required for technical support. Self-help will be made available by accessing Proxim's extensive eService knowledgebase.
- **Software Maintenance:** It's important to maintain and enhance security and performance of wireless equipment and Proxim makes this easy by providing a Software Maintenance program that enables customers to access new features and functionality, rich software upgrades and updates. Customers will also have full access to Proxim's vast knowledgebase of technical bulletins, white papers and troubleshooting documents.
- **Priority Queuing Phone Support:** This service provides customers with a one hour response time for technical phone support. There is no waiting in line for those urgent calls for technical support.

Technical Services and Support

ServPak Service	24x7 Enhanced (Bundled Serv.)	8x5 Standard (Bundled Serv.)	Extended Warranty	Advance Hardware Replacement	Software Maintenance	24x7 Technical Support
Product Coverage Duration	Renewable Contracts	Renewable Contracts	Renewable Contracts	Renewable Contracts	No	Renewable Contracts
Software Coverage Duration	Renewable Contracts	Renewable Contracts	No	No	Renewable Contracts	No
Proxim TAC Support	Yes	Yes	No	No	No	Yes
Software Updates & Upgrades	Yes	Yes	No	No	Yes	No
Registered Access to Proxim.com	Yes	Yes	Yes	Yes	Yes	Yes
Registered Access to Knowledge Tool	Yes	Yes	Yes	Yes	Yes	Yes
Advance Replacement	Yes	No	No	Yes	No	No
Depot Repair	No	Yes	Yes	No	No	No

To purchase ServPak support services, please contact your authorized Proxim distributor. To receive more information or for questions on any of the available ServPak support options, call Proxim Support at 408-383-7700 or send an email to servpak@proxim.com.