

# Tsunami® 8100 Series (Point-to-point and Point-to-multipoint Products)

## Software Management Guide

### Products Covered

- Tsunami® MP-8100-BSU / MP-8100-WD-HP
  - Tsunami® MP-8100-SUA / MP-8100-WD-HP
  - Tsunami® MP-8150-SUR / MP-815-WD-HP
  - Tsunami® MP-8150-CPE
- Tsunami® MP-8160-BSU
  - Tsunami® MP-8160-SUA
  - Tsunami® MP-8160-CPE
- Tsunami® QB-8100-EPA
- Tsunami® QB-8100-LNK
- Tsunami® QB-8150-EPR
- Tsunami® QB-8150-LNK
- Tsunami® QB-8150-LNK-12/50



---

## Copyright

© 2011 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. The content 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 the 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® products include 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, visit the Proxim Web site (<http://support.proxim.com>) 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.

## **Tsunami® 8100 Series - Software Management Guide**

**Documentation Version:** 4.0  
P/N 765-00131, November 2011

# Contents

Preface . . .	8
<b>1 Overview . . . . .</b>	<b>10</b>
About Tsunami® 8100 Products . . . . .	. 10
Wireless Network Topology . . . . .	. 11
Point-to-Multipoint (PTMP) . . . . .	11
Point-to-Point Link . . . . .	14
Multiple-Input-Multiple-Output (MIMO) . . . . .	. 17
Wireless Outdoor Router Protocol (WORP) . . . . .	. 17
<b>2 Management and Monitoring Capabilities . . . . .</b>	<b>19</b>
Web (HTTP/HTTPS) Interface . . . . .	. 19
Command Line Interface . . . . .	. 19
HyperTerminal . . . . .	19
Telnet . . . . .	20
Secure Shell (SSH) . . . . .	20
SNMP Management . . . . .	. 20
ProximVision ES . . . . .	. 20
<b>3 Device Initialization . . . . .</b>	<b>21</b>
Initialization . . . . .	. 21
ScanTool . . . . .	21
Initialize Device using ScanTool . . . . .	22
Modifying the IP Address of the Device using ScanTool . . . . .	23
Logging onto the Web Interface . . . . .	. 23
Home Page . . . . .	25
COMMIT . . . . .	26
REBOOT . . . . .	27
Factory Default Configuration . . . . .	. 27
<b>4 Basic Configuration . . . . .</b>	<b>29</b>
<b>5 Advanced Configuration . . . . .</b>	<b>34</b>
System . . . . .	. 34
Network . . . . .	. 35
IP Configuration (Bridge Mode) . . . . .	36
IP Configuration (Routing Mode) . . . . .	38
IP Configuration (Routing Mode with PPPoE Client Enabled)	40
Ethernet . . . . .	. 42
Basic Ethernet Configuration . . . . .	42
Advanced Configuration . . . . .	43
Wireless . . . . .	. 44

Wireless Outdoor Router Protocol (WORP) . . .	44
Wireless Interface Properties . . .	49
MIMO Properties . . .	57
Dynamic Frequency Selection (DFS) . . .	59
DDRS . . .	64
Security . . .	68
Wireless Security . . .	68
RADIUS . . .	71
MAC ACL . . .	73
Quality of Service (QoS) . . .	74
QoS Concepts and Definitions . . .	74
QoS Configuration . . .	79
QoS Configuration for a Management Station . . .	96
RADIUS Based SU QoS Configuration	100
VLAN (Bridge Mode Only) . . .	101
System-Level VLAN Configuration . . .	101
Ethernet VLAN Configuration . . .	102
RADIUS Based SU VLAN Configuration	107
Filtering (Bridge Only)	109
Protocol Filter . . .	110
Static MAC Address Filter . . .	113
Advanced Filtering . . .	116
TCP/UDP Port Filter . . .	118
Storm Threshold Filter . . .	120
WORP Intra Cell Blocking . . .	121
DHCP . . .	125
DHCP Pool . . .	125
DHCP Server . . .	126
DHCP Relay (Routing Mode only) . . .	127
IGMP Snooping . . .	128
Routing Mode Features . . .	130
Static Route Table . . .	130
Network Address Translation (NAT) . . .	132
RIP . . .	135
PPPoE End Point (SU Only) . . .	136
IP over IP Tunneling . . .	142
<b>6 Management . . . . .</b>	<b>147</b>
System	147
System Information . . .	147
Inventory Management . . .	148
Licensed Features . . .	149

File Management . . .	. 150
TFTP Server . . .	150
Text Based Configuration (TBC) File Management . . .	151
Upgrade Firmware . . .	153
Upgrade Configuration . . .	154
Retrieve From Device . . .	156
Services . . .	. 159
HTTP/HTTPS . . .	159
Telnet/SSH . . .	160
SNMP . . .	162
Logs . . .	165
Simple Network Time Protocol (SNTP)	. 167
Access Control	. 169
Reset to Factory . . .	. 170
Convert QB to MP . . .	. 171
<b>7 Monitor . . .</b>	<b>173</b>
Interface Statistics	. 173
Ethernet Statistics . . .	173
Wireless Statistics	175
PPPoE Statistics . . .	176
IP Tunnels . . .	177
WORP Statistics . . .	. 179
General Statistics . . .	179
SU / End Point B Link Statistics . . .	181
BSU/End Point A Link Statistics . . .	184
QoS Statistics (BSU or End Point A Only) . . .	185
Active VLAN	. 186
Bridge . . .	. 187
Bridge Statistics . . .	187
Learn Table . . .	188
Network Layer . . .	. 189
Routing Table . . .	189
IP ARP . . .	189
ICMP Statistics . . .	190
RIP Database . . .	191
RADIUS (BSU or End Point A only) . . .	. 192
Authentication Statistics . . .	192
IGMP . . .	. 193
Ethernet or Wireless Multicast List . . .	193
Router Port List . . .	194

DHCP . . .	. 194
Logs	. 195
Event Log . . .	195
Syslog . . .	196
Debug Log . . .	196
Temperature Log . . .	197
Tools	. 198
Wireless Site Survey. . .	198
Scan Tool. . .	199
sFlow® . . .	199
Console Commands . . .	204
SNMP v3 Statistics . . .	. 204
<b>8 Troubleshooting . . .</b>	<b>205</b>
PoE Injector . . .	. 206
Connectivity Issues	. 206
Surge or Lightning Issues (For Connectorized devices)	. 207
Setup and Configuration Issues . . .	. 208
Application Specific Troubleshooting	. 209
Wireless Link Issues	. 210
Wired (Ethernet) Interface Validation . . .	. 211
Wireless Interface Validation	. 212
Recovery Procedures	. 213
Soft Reset to Factory Defaults . . .	213
Hard Reset to Factory Defaults. . .	213
Forced Reload . . .	214
Setting IP Address using Serial Port . . .	216
Spectrum Analyzer	. 217
Avoiding Interference . . .	218
Conclusion . . .	218
Miscellaneous	. 218
Unable to Retrieve Event Logs through HTTPS . . .	218
<b>A Feature Applicability . . .</b>	<b>219</b>
<b>B Parameters Requiring Reboot . . .</b>	<b>220</b>
<b>C Frequency Domains and Channels . . .</b>	<b>223</b>
<b>D SNR Information. . .</b>	<b>231</b>
<b>E Bootloader CLI and ScanTool. . .</b>	<b>235</b>

---

F Lightning Protection . . . . .	237
G Abbreviations . . . . .	238
H Statement of Warranty . . . . .	242
I Technical Services and Support. . . . .	244

# Preface

This chapter contains information on the following:

- [About this Guide](#)
- [Products Covered](#)
- [Audience](#)
- [Prerequisites](#)
- [Related Documents](#)
- [Documentation Conventions](#)

## About this Guide

This manual gives a jump-start working knowledge on the Tsunami® 8100 products. It explains the step-by-step procedure to configure, manage and monitor these products by using Web Interface.

## Products Covered

Tabulated below are the Tsunami® products that are covered in this guide along with the latest software version supported.

Product(s)	Software Version Supported
Tsunami® MP-8100-BSU	2.4.0
Tsunami® MP-8100-SUA	2.4.0
Tsunami® MP-8150-SUR	2.4.0
Tsunami® MP-8150-CPE	2.4.0
Tsunami® MP-8160-BSU	2.4.0
Tsunami® MP-8160-SUA	2.4.0
Tsunami® MP-8160-CPE	2.4.0
Tsunami® QB-8100-EPA	2.4.0
Tsunami® QB-8100-LNK	2.4.0
Tsunami® QB-8150-EPR	2.4.0
Tsunami® QB-8150-LNK	2.4.0
Tsunami® QB-8150-LNK-12/50	2.4.0

## Audience

The intended audience for this guide is the Network Administrator who installs and/or manages the 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

In addition to this guide, you can refer to the following documents that are available on the Proxim's support site <http://support.proxim.com>.




- **Quick Installation Guide (QIG)** - A quick reference guide that provides essential information to install and configure the device.
- **Hardware Installation Guide** - A guide that provides an overview about the Tsunami® products, their installation methods and hardware specifications.
- **Reference Guide** - A guide that provides instructions on how to configure, manage and monitor the device by using Command Line Interface.
- **Antenna Guides** - A guide that gives insight on the recommended antennas and the ways to align them.
- **Safety and Regulatory Compliance Guide** - A guide that provides country specific safety and regulatory norms to be followed while installing the devices.

## Documentation Conventions

### Screenshots

This guide uses screenshots to explain the method to configure and manage the device using Web Interface. Based on your device, the screenshots may vary. Hence, we request you to refer to the screenshots that are valid for your device.

### Icon Representation

Name	Image	Meaning
Note		A special instruction that draws attention of a user.
Important		A note of significant importance that a user should be aware of.
Caution		A warning that cautions a user of the possible danger.

### Device Naming Conventions

Naming Convention	Description
BSU	Refers to a Base Station Unit
Subscriber / SU Mode / SU	Refers to both SU and CPE
End Point A mode	Refers to a device in End Point A mode
End Point B mode	Refers to a device in End Point B mode



: A feature specific to a device is referred to by its name else by the common naming convention as tabulated above.

# Overview






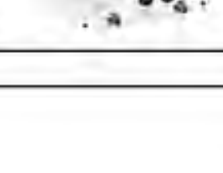
This chapter contains information on the following:








- [About Tsunami® 8100 Products](#)
- [Wireless Network Topology](#)
  - [Point-to-Multipoint \(PTMP\)](#)
  - [Point-to-Point Link](#)
- [Multiple-Input-Multiple-Output \(MIMO\)](#)
- [Wireless Outdoor Router Protocol \(WORP\)](#)

## 1.1 About Tsunami® 8100 Products

Proxim's Tsunami® 8100 product series, consists of point-to-point and point-to-multipoint devices that are designed to provide wireless networking solutions to enterprises and business markets.

This product series consists of the following products:

Product	Description	Image
Tsunami® MP-8100-BSU	The Tsunami® MP-8100 Base Station unit, is a flexible wireless outdoor product that operates in 2.3 - 2.5 and 4.9 - 6.0 GHz frequency bands. This connectorized device comes with a 3x3 MIMO radio and three N-Type connectors to connect external antennas.	
Tsunami® MP-8100-SUA	The Tsunami® MP-8100 Subscriber unit, is a flexible wireless outdoor product that operates in 2.3 - 2.5 and 4.9 - 6.0 GHz frequency bands. This connectorized device comes with a 3x3 MIMO radio and three N-Type connectors to connect external antennas.	
Tsunami® MP-8150-SUR	The Tsunami® MP-8150 Subscriber unit comes with a 3x3 MIMO radio operating in 4.9 - 6.0 GHz frequency band. This connectorized device comes with a 3x3 MIMO Radio and three N-Type connectors to connect external antennas.	
Tsunami® MP-8150-CPE	The Tsunami® MP-8150 Customer Premises Equipment comes with a high power 2x2 MIMO radio and 16 dBi integrated dual-polarized panel antenna operating in 5.3 - 6.1 GHz frequency band.	
Tsunami® MP-8160-BSU	The Tsunami® MP-8160 Base Station unit, is a flexible outdoor product that operates in 5.9 - 6.4 GHz frequency band. This connectorized device comes with a high power 2x2 MIMO radio and two N-Type connectors to connect external antennas.	
Tsunami® MP-8160-SUA	The Tsunami® MP-8160 Subscriber unit, is a flexible outdoor product that operates in 5.9 - 6.4 GHz frequency band. This connectorized device comes with a high power 2x2 MIMO radio and two N-Type connectors to connect external antennas.	

Tsunami® MP-8160-CPE	The Tsunami® MP-8160 Customer Premises Equipment comes with a single high power 2x2 MIMO radio and 15 dBi integrated dual-polarized panel antenna operating in 5.9 - 6.4 GHz frequency band.	
Tsunami® QB-8100-EPA	The Tsunami® QB-8100-EPA QuickBridge operates in 2.3 - 2.5 and 4.9 - 6.0 GHz frequency bands. This connectorized device comes with a 3x3 MIMO radio and three N-Type connectors to connect external antennas.	
Tsunami® QB-8100-LNK	A pair of Tsunami® QB-8100-EPA devices form a link.	
Tsunami® QB-8150-EPR	The Tsunami® QB-8150-EPR QuickBridge comes with a 2x2 MIMO radio and 23 dBi integrated dual-polarized panel antenna operating in 4.9 - 6.0 GHz Band.	
Tsunami® QB-8150-LNK	A pair of Tsunami® QB-8150-EPR devices form a link.	
Tsunami® QB-8150-LNK-12	A pair of Tsunami® QB-8150-EPR-12 devices form a link.  The Tsunami® QB-8150-EPR-12 device comes with a high power 2x2 MIMO radio, 12 Mbps speed and 16 dBi integrated dual-polarized panel antenna operating in 5.3 - 6.1 GHz frequency band.	
Tsunami® QB-8150-LNK-50	A pair of Tsunami® QB-8150-EPR-50 devices form a link.  The Tsunami® QB-8150-EPR-50 device comes with a high power 2x2 MIMO radio, 50 Mbps and 16 dBi integrated dual-polarized panel antenna operating in 5.3 - 6.1 GHz frequency band.	

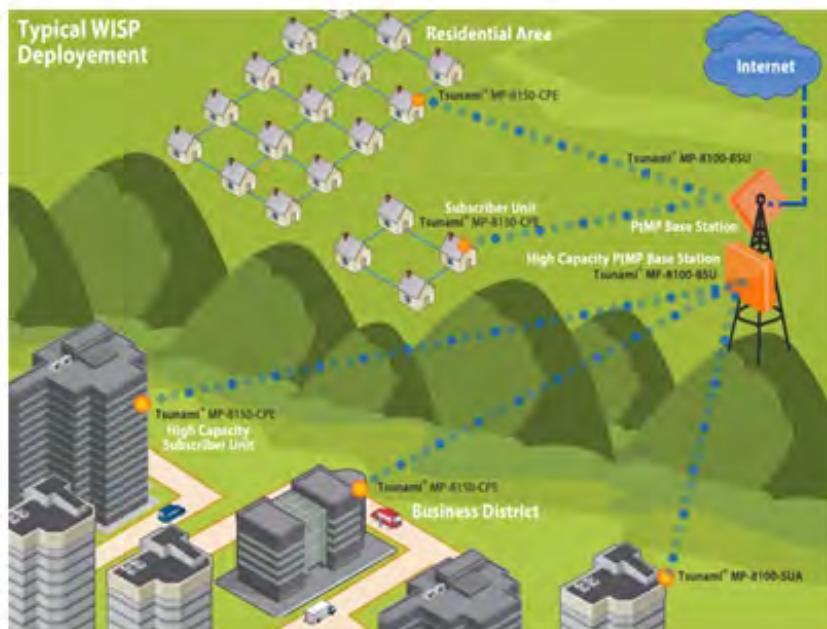
## 1.2 Wireless Network Topology

### 1.2.1 Point-to-Multipoint (PTMP)

Point-to-multipoint is a wireless network that has a central communication device such as a Base Station Unit (BSU), providing connectivity to multiple devices such as Subscribers (SUs) or clients. Any transmission of data that originates from the BSU is received by all SUs; whereas, the data originating from any of the SU is received only by the BSU. This allows numerous sites in a wide area to share resources, including a single high-speed connection to the Internet.

Listed below are the applications, where Proxim's Point-to-multipoint devices can be used:

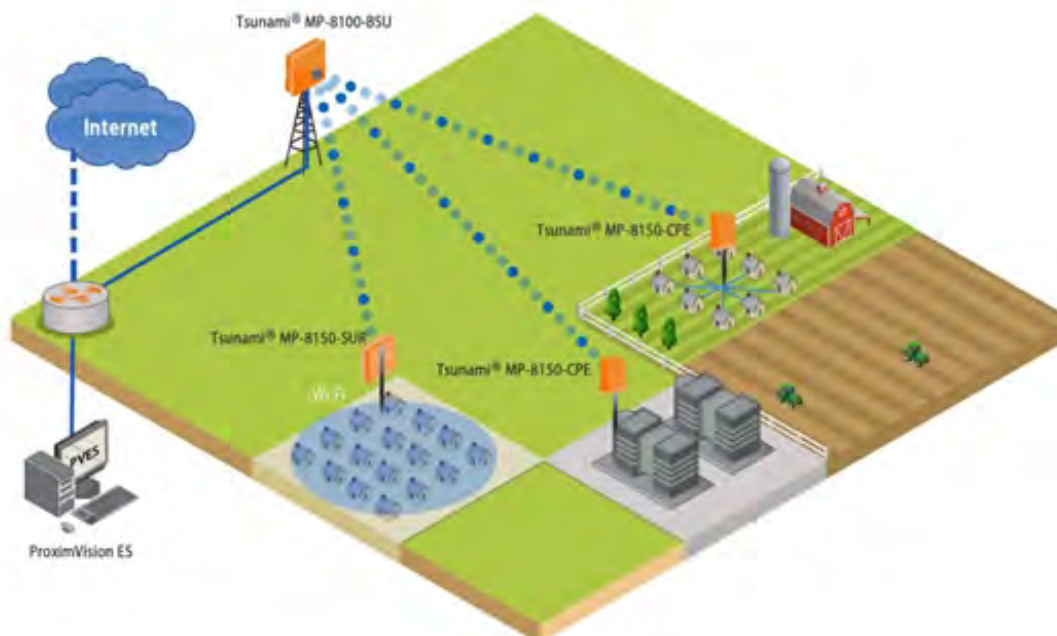
- **Last Mile Access:** Competitive broadband service access alternative to Digital Subscriber Line (DSL) or cable for residences and T1 or Ethernet for businesses.



- **Security and Surveillance:** High definition IP-surveillance cameras for monitoring city streets, airports, bridges, seaports, transportation hubs, offices and warehouses.



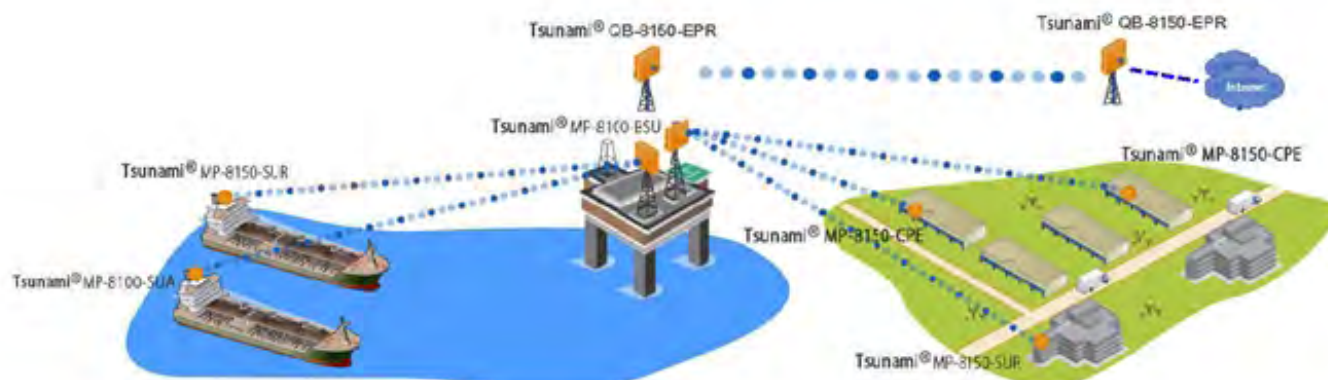
- **Metropolitan Area Network:** Secure and reliable connectivity between city buildings.



- **Enterprise Campus Connectivity:** Extend the main network to remote offices, warehouses or other buildings without leased lines.



- **Offshore Communications:** Establishes connectivity between seashore and the ships that are nearing the port locations, or connectivity between off-shore oil rigs and sea shore and so on.



- **Wireless Intelligent Transportation System (ITS):** Increases the traffic efficiency and reduces the commuting time in cities and metropolitan areas.



### 1.2.2 Point-to-Point Link

A point-to-point link is a dedicated wireless link that connects only two stations.

With a point-to-point link, you can set up a connection between two locations as an alternative to:

- Leased lines in building-to-building connections
- Wired Ethernet backbones between wireless access points in difficult-to-wire environments.

It is easy to set up a wireless point-to-point link as shown in the following figure. Each device is set up as either an End Point A or an End Point B.

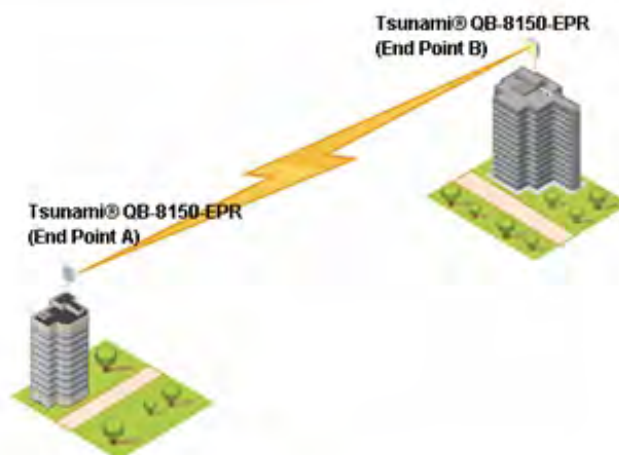


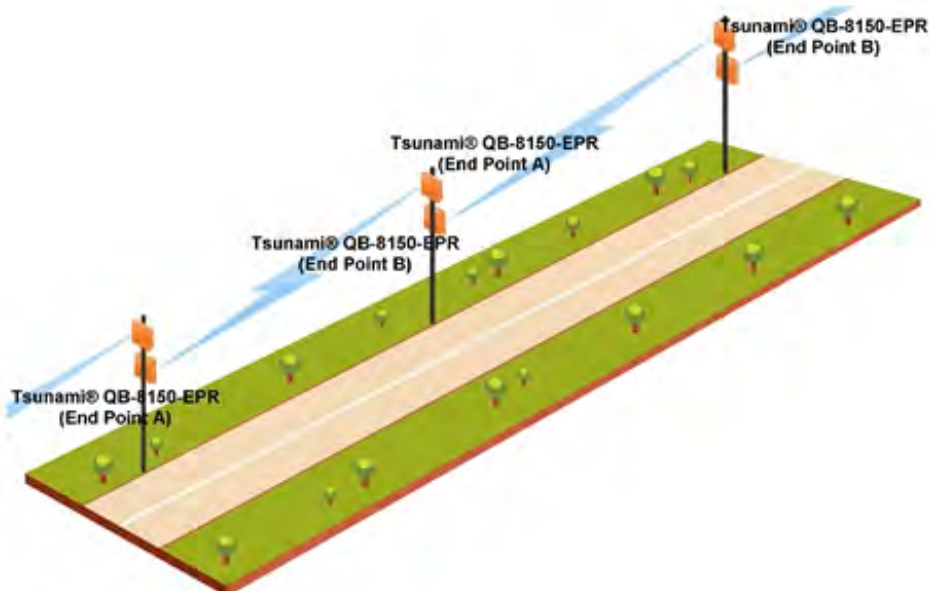
Figure 1-1 Point-to-Point-Link

Listed below are the applications, where Proxim's Point-to-Point devices can be used:

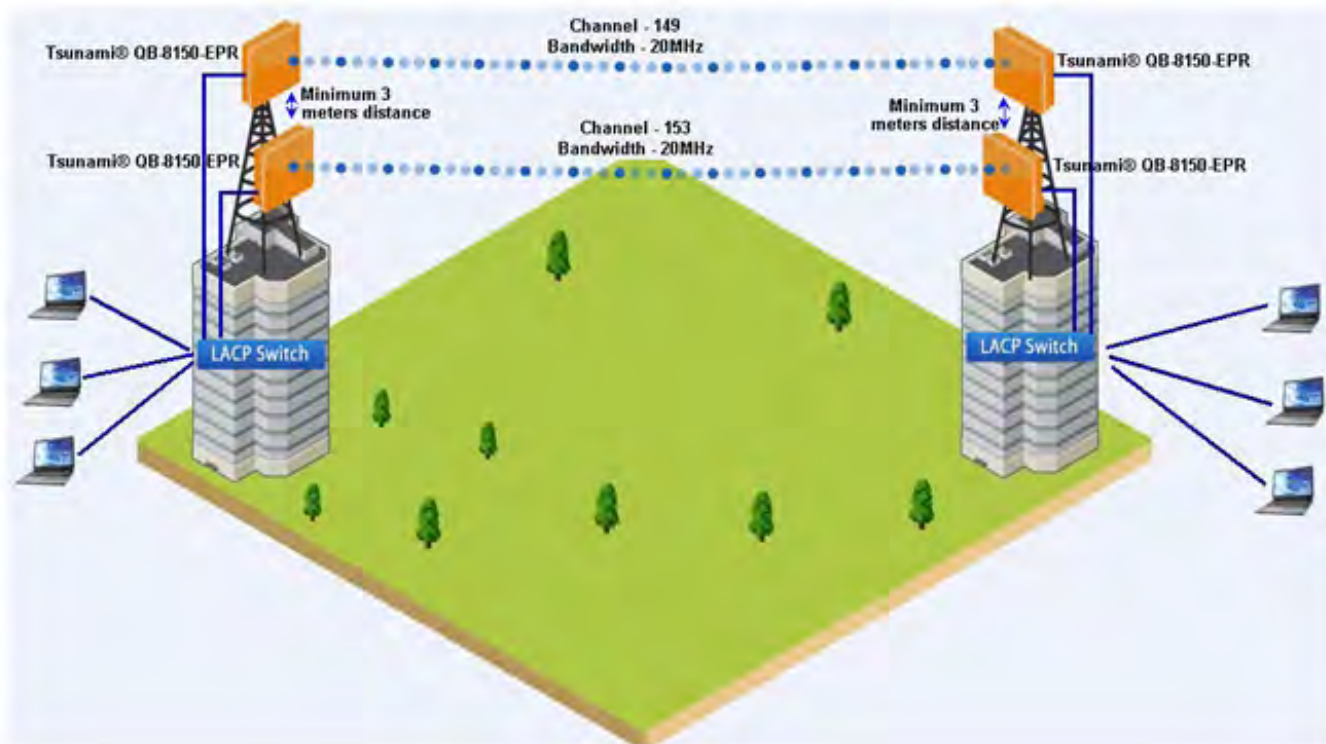
- **Backhaul to a Central POP:** Avoids expensive installation and recurring charge of a second wireline backhaul to a remote virtual POP.



- **Repeater:** Extends distance or overcomes path blockage by adding point-to-point hops



- **High-bandwidth Last Mile Access:** Delivers Transparent LAN Services (TLS) to corporate parks.
- **High Availability and Link Aggregation:** Achieves high availability and link aggregation in wireless medium by using two parallel links and additional Link Aggregation Control Protocol (LACP) capable switches. This is applicable only for QB-8100-EPA/LNK and QB-8150-EPR/LNK devices.





- **Leased Line Redundancy:** Eliminates recurring DS-3 leased line charges with one time installation charge of a QuickBridge link.
- **Inter-POP Redundancy:** Avoids downtimes caused by a wireline backhaul failure by adding a QuickBridge link as an inter-POP redundancy.

### 1.3 Multiple-Input-Multiple-Output (MIMO)

Proxim's 81xx Point-to-point and Point-to-multipoint devices support Multiple-Input-Multiple-Output (MIMO) antenna technology that uses multiple antennas at both the transmitter and receiver to improve communication performance. The underlying technology of Proxim's product radio(s) are based on a combination of MIMO and OFDM (Orthogonal Frequency Division Multiplexing). MIMO-OFDM combination radios solve interference, fading and multipath problems. 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.

MIMO also uses Spatial multiplexing transmission technique to transmit independent and separately encoded data signals from each of the multiple transmit antennas while reusing or multiplexing in the space dimension. These independent data signals are called Spatial streams. The transmitting antenna uses multiple radio Tx chains and signal paths to simultaneously transmit different data streams, whereas the receiver combines the Rx signals resulting in higher throughput.

By increasing the number of receiving and transmitting antennas, the throughput of the channel increases linearly resulting in high spectral efficiency.

### 1.4 Wireless Outdoor Router Protocol (WORP)

WORP is a protocol, designed by Proxim to optimize the performance of multi-play outdoor wireless Point-to-Point (PtP) and Point-to-Multipoint (PTMP) links using packet radio technology, including the use of cutting edge Multiple-Input-Multiple-Output (MIMO) technology.

WORP overcomes the performance degradation, which standards-based wireless technologies are susceptible to when used for outdoor long-range connectivity.

#### Benefits:

- **More Net Bandwidth:** WORP increases the overall net bandwidth of the multipoint system. The net bandwidth using WORP is higher than any other protocol solution used in an outdoor environment. WORP is a more efficient protocol that protects the system from packet collisions and transmits the data in an optimal way, which increases the overall performance.
- **More Concurrent Subscribers:** An outdoor point-to-multipoint solution based on 802.11 may connect from 5 to 10 remote nodes, but sometimes performance starts to suffer from collisions with as little as only 2 remote nodes. A solution using WORP, on the other hand, can connect up to 100 remote nodes without adverse effects on usable bandwidth, allowing more concurrent Subscriber Units (SU) to be active in a wireless multipoint environment.
- **Smart Scheduling:** WORP uses smart scheduling for remote node polling to avoid wasting bandwidth on nodes that have no traffic to be sent. The Base Station Unit (BSU) dynamically decides how frequently a remote node should be polled based on the current traffic to and from each remote node and the priority settings for that traffic. The scheduling is adapted dynamically to the actual traffic and further optimized by following the bandwidth limits as configured for each remote node.
- **Dynamic Data Rate Selection (DDRS):** DDRS enables WORP to dynamically adjust the data rate at which the wireless traffic is sent. This feature is especially important in point-to-multipoint networks, when different SUs can sustain different data rates because of the different distances from the BSU. With DDRS, WORP dynamically optimizes the wireless data rate to each of the SUs independently, keeping the overall net throughput at the highest possible level. This feature optimizes throughput even for links with different RF conditions on the BSU and SU, by optimizing downlink

- **Quality of Service:** WORP ensures that the most important data arrives with priority by differentiating between priorities of traffic as defined in the profiles for QoS (Quality of Service), similar to the 802.16 WiMAX QoS standard definition.
- **Bandwidth Control:** WORP allows service providers to control network bandwidth, protecting the network from excessive bandwidth use by any one station. Additionally, it allows service providers to differentiate their service offerings.
- **Asymmetric Bandwidth Controls:** Asymmetric bandwidth gives network managers the ability to set different maximum bandwidth rates for a variety of customer groups. This allows service providers to further differentiate their service offerings and maximize revenues.

## Management and Monitoring Capabilities

A Network administrator can use the following interfaces to configure, manage and monitor the devices.

- Web Interface
- Command Line Interface
- Simple Network Management Protocol (SNMP)
- ProximVision ES (PVES)

### 2.1 Web (HTTP/HTTPS) 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, through LAN (switch, hub and so on), the Internet, or with an Ethernet cable connected directly to your computer's Ethernet port.

HTTPS interface provides an HTTP connection over a Secure Socket Layer (SSL). HTTPS allows the user to access the device in a secure fashion using SSL over port 443. The device supports SSLv3 with a 128-bit encryption certificate maintained by the device for secure communication between the device and the HTTP client. All communications are encrypted using the server and the client-side certificate.

### 2.2 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, manage and monitor the device. You can enter the command statements composed of CLI commands and their associated parameters. Commands can be issued from the keyboard for real-time control, or from scripts that automate configuration. For example, when downloading a file, an administrator enters the download CLI Command along with the IP Address, file name, and file type parameters.

#### 2.2.1 HyperTerminal

You can access the CLI over a HyperTerminal serial connection. HyperTerminal is a program that connects to other Computers, Telnet Sites, Bulletin Board Systems (BBS), Online Services, and Host Computers, by using either modem or a null modem cable.

If you are using RS-232 cable, verify the following information in the HyperTerminal serial port setup:

<b>Port</b>	COM1 (default)
<b>Baud Rate</b>	115200
<b>Data</b>	8-bit
<b>Parity</b>	None
<b>Stop</b>	1-bit
<b>Flow Content</b>	None



: If you are using Windows 7 then use Terminal Emulator program like Teraterm Pro for serial connection.

### 2.2.2 Telnet

You can access the device through CLI by using Telnet. With Telnet, you can communicate with the device through LAN (switch, hub and so on), the Internet, or with an Ethernet cable connected directly to your computer's Ethernet port.

### 2.2.3 Secure Shell (SSH)

You can securely access the device through CLI by using Secure Shell (SSH). The device supports SSH version 2, for secure remote CLI (Telnet) sessions. SSH provides strong authentication and encryption of session data. The SSH server has host keys - a pair of asymmetric keys (a private key that resides on the device) and a public key that is distributed to clients that need to connect to the device. Clients need to verify that it is communicating with the correct SSH server.

## 2.3 SNMP Management

You can also configure, manage and monitor the device by using the Simple Network Management Protocol (SNMP). This requires an SNMP Manager Program (sometimes called MIB browser) or a Network Manager program using SNMP. The device supports the following Management Information Base (MIB) files that describe the parameters that can be viewed and/or configured over SNMP:

- PXM-SNMP.mib (Enterprise MIB)
- RFC-1213.mib (MIB-II)
- RFC-1215.mib (Trap MIB)
- RFC-1757-RMON.mib (Remote Monitoring)
- RFC-2571.mib (SNMP Framework)
- RFC-3411-SNMP-FRAME-WORK.mib (SNMP Framework)
- RFC-2790.mib (Host Resources)
- RFC-3291-INET-ADDRESS-MIB.mib
- RFC-3412.mib (SNMP-MPD-MIB)
- RFC-3414.mib (SNMP-USER-BASED-SM-MIB)
- SFLOW.mib

The PXM MIB files are available on the Proxim support site (<http://support.proxim.com>). You must compile one or more of these MIB files into your SNMP program's database before you manage your device using SNMP.

The enterprise MIB (PXM-SNMP.mib) defines the Read and Read/Write objects that can be viewed or configured using SNMP. These objects correspond to most of the settings and statistics that are available with other management interfaces. The MIB can be opened with any text editor, such as Microsoft Word, Notepad, or WordPad.

## 2.4 ProximVision ES

ProximVision ES (commonly known as PVES) is Proxim's Network Management System that helps to manage and administer your wireless network effectively and efficiently. ProximVision ES combines industry-leading functionality with an intuitive user interface, enabling Network Administrators and Help Desk staff to support and control a wireless network.

ProximVision ES offers you a single intelligent console from which you can manage, monitor, analyze and even configure your device. For more information, see ProximVision ES user guide available at the Proxim's support site at <http://support.proxim.com>.



***This user guide explains the method to initialize and manage the device using Web Interface only. The Reference Manual, a guide that explains the method to manage the device using Command Line Interface, can be found at Proxim's support site (<http://support.proxim.com>).***

## Device Initialization

This chapter contains information on the following:

- Initialization
  - ScanTool
  - Initialize Device using ScanTool
  - Modifying the IP Address of the Device using ScanTool
- Logging onto the Web Interface
  - Home Page
  - COMMIT
  - REBOOT
- Factory Default Configuration

### 3.1 Initialization

Once the device installation completes, you can access the device either through Command Line Interface, Web Interface or an SNMP Interface.



: For installation procedure, please refer to the **Hardware Installation guide** available at Proxim's support site (<http://support.proxim.com>).

- To access the device using CLI commands, connect a serial RS-232 cable to the Serial port of the device.
- To access the device using Web or SNMP interface, connect an Ethernet cable to the Ethernet port of the device.

For all the modes of connection, you will need to configure the IP address of the device. As each network is different, a suitable IP address on the network must be assigned to the device. This IP address helps you to configure, manage and monitor the device through the Web Interface, SNMP, or Telnet/CLI. The device can have either a **static** or **dynamic** IP address. When set to **static**, the user has to set the IP address manually; and if set to **dynamic**, the IP address is obtained dynamically from the Dynamic Host Configuration Protocol (DHCP) server.

By default, the device IP Address is set to 169.254.128.132.



: Tsunami® MP-8160-CPE device does not have a Serial Port. However, the user has the flexibility to configure, manage and monitor the device through command mode via Telnet.

#### 3.1.1 ScanTool

Proxim's ScanTool (Answer ID - 1735) is a software utility that runs on Microsoft Windows machine. By using ScanTool, you can

- Scan devices (Proxim devices only) available on the network
- Obtain device's IP address
- Modify device's IP Configuration parameters (IP Address, Address Type, Gateway and so on)
- Launch the Web interface
- Switch between the network adapters, if there are multiple network adapters in the Personal Computer



: ScanTool works only for Proxim devices. Also note that you may need to disable Windows Firewall (or add an exception) for ScanTool to function or to detect the radio.

### 3.1.2 Initialize Device using ScanTool

To scan and locate the devices on a network by using ScanTool, do the following:

1. Power on, or reset the device.
2. To download Proxim's ScanTool, log on to Proxim's support site at <http://support.proxim.com> and search for ScanTool with (Answer ID 1735). Upon successful download, start ScanTool by double-clicking the downloaded icon.
3. If your computer has more than one network adapter installed, you will be prompted to select the adapter for scanning Proxim devices. You can use either an Ethernet or a Wireless Adapter. Select an adapter and click **OK**. The following **ScanList** screen appears, which displays all devices that are connected to selected adapter.

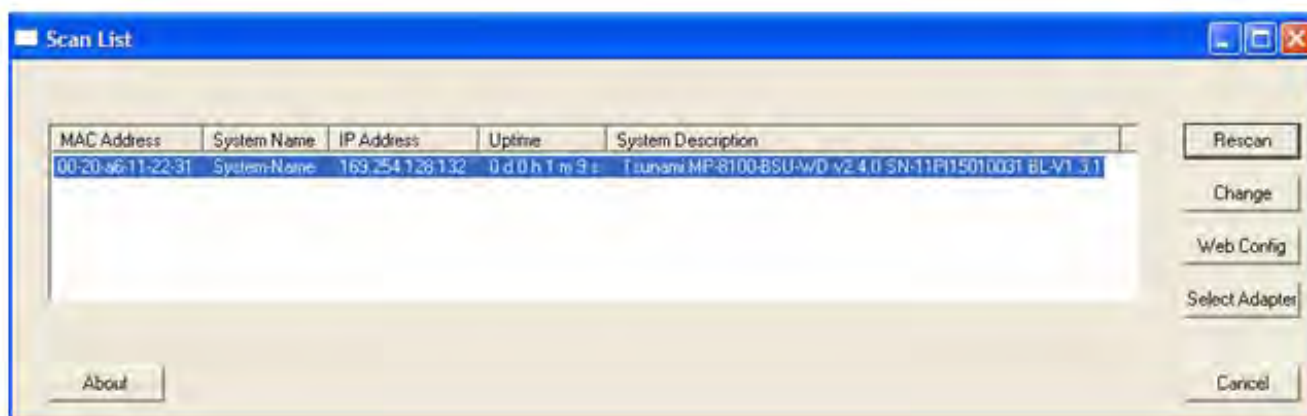


Figure 3-1 ScanList - An Example

This screen contains the following device information:

- **MAC Address**
  - **System Name**
  - **IP Address**
  - **Uptime**
  - **System Description:** The system description comprises the following information:
    - **Device Description:** For example, Tsunami MP-8100-BSU-WD
    - **Firmware Version:** For example, v2.4.0
    - **Serial Number :** For example, SN-11P15010031
    - **Bootloader Version:** For example, BL - V1.3.1
4. Click **Select Adapter**, to change adapter settings.
  5. Identify and select the MAC address of the device you want to initialize from the list and click **Web Config** to log on to the Web Interface.



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

### 3.1.3 Modifying the IP Address of the Device using ScanTool

To modify the IP address of a device using ScanTool, select the device from the scan list and click **Change**. A **Change** screen appears as shown in the following figure. The system automatically populates the **MAC Address**, **System Name**, **TFTP Server IP Address** and **Image File Name** of the device, which are read-only.

Figure 3-2 Modifying Device's IP Address

1. Select the **IP Address Type** as either **static** or **dynamic**.
  - **Static**: When set to static, the IP address of the device is changed manually.
  - **Dynamic**: When set to dynamic, the IP address is dynamically generated by the DHCP server.
2. Type the appropriate **IP Address**, **Subnet Mask**, and the **Gateway IP Address** parameters.
3. Enter the SNMP Read/Write password in the **Read/Write Password** box. By default, it is **public**.
4. Click **OK** to save the details. The device automatically reboots.

To log on to the Web Interface, click **Web Configuration**.

The user is then prompted to enter its username and password. For more information on how to login, please see [Logging onto the Web Interface](#).

## 3.2 Logging onto the Web Interface

Once the device is connected to your network, use a web browser to configure, manage and monitor the device. Enter the default IP address of the device (For example, <http://169.254.128.132>) in the address bar or access the Web Interface using ScanTool (see [Initialization](#)).

You are now prompted to enter your username and password.



Figure 3-3 Login Screen

Based on the access credentials, two types of users can access the device. They are,

1. **Administrator User:** The Administrator user administers the entire device. This user type has the write access to all the features of the device and also has the privilege to change his or her own password and that of the Monitor user (the other user type). To change the password, refer to [Services](#).
2. **Monitor User** - The Monitor user has only view access to all the features of the device. This user is restricted from the following privileges:
  - Change the device functionality
  - Change his or her own password
  - Run any of the test tools like Link Test, Wireless Site Survey and so on. However, the user can view the logs and statistics of the test tools.

The Monitor user is given the privilege to retrieve event logs and temperature logs for debugging.

To logon to the device,

1. Type a valid user name in the **User Name** box. The user name is **admin** for the Administrator user and **monitor** for the Monitor user.
2. Type the password in the **Password** box. By default, the password is **public** for both the Administrator user and the Monitor user.



- By default the password is **public**. For security reasons, it is recommended to change the password after your first logon to the device.
- 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 on to the configuration pages by using default user name and password, please check with the administrator or follow [Forced Reload](#) procedures.
- If using Internet Explorer, and you enter wrong password consecutively for three times, the HTTP session will get disconnected. In case of other browsers, the login screen will reset until you enter correct password.
- In the Internet Explorer, to get best results, click on **Tools > Internet Options > General**. Click **Settings** in the Browsing History and select "**Every visit to the webpage**".



### 3.2.1 Home Page

Upon successful login, the device home page appears.

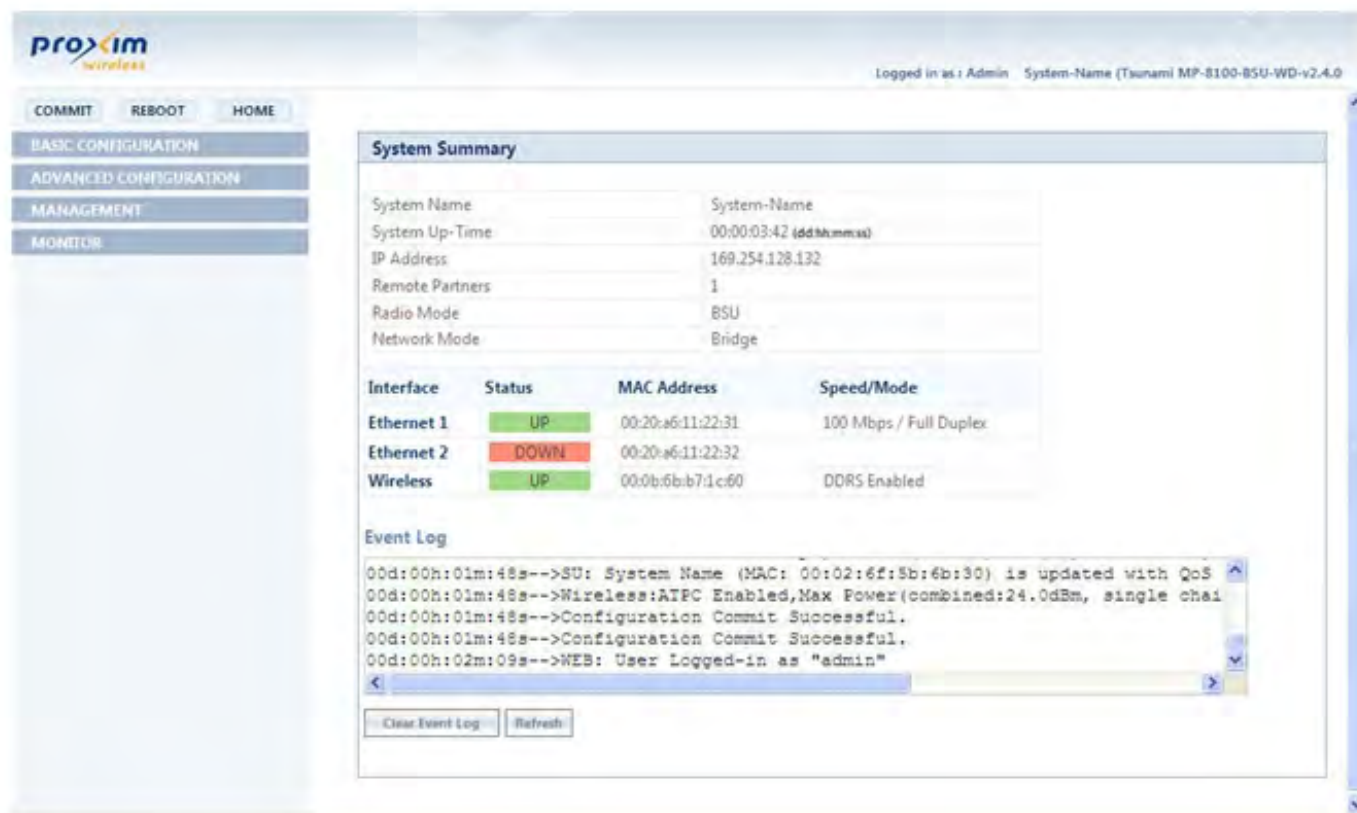


Figure 3-4 Home Page

The home page contains the following information:

- **Device Description:** The device description is displayed on the top-right corner of the home page. It displays the logged in user type and the device name along with the latest firmware version.
- **System Summary:** The System Summary screen displays the summary of system information such as System Name, IP Address, Radio Mode, Interface Status, Event Log and so on.
- **COMMIT Button:** See [COMMIT](#)
- **REBOOT Button:** See [REBOOT](#)
- **Home:** Display System Summary screen.
- **BASIC CONFIGURATION:** The BASIC CONFIGURATION tab allows the user to configure the minimum set of parameters required for a device to be operational and establish link in the network. For more details, see [Basic Configuration](#).
- **ADVANCED CONFIGURATION:** The ADVANCED CONFIGURATION tab allows the user to configure the advanced parameters of the device. For more details, see [Advanced Configuration](#).
- **MANAGEMENT Tab:** The MANAGEMENT tab allows the user to manage the device. For more details, see [Management](#).
- **MONITOR Tab:** The MONITOR tab allows the user to monitor the device. For more details, see [Monitor](#).

### 3.2.2 COMMIT

**COMMIT** operation is used to apply the configuration changes onto the device. When changes are made to the configuration parameters of the device, the changes will not take effect, until **COMMIT** is clicked. 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:

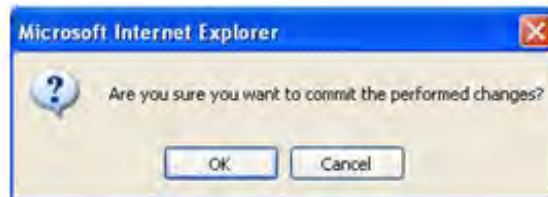


Figure 3-5 Commit

Click **OK**, if you wish to commit the changed parameters.

On successful **COMMIT** operation, the following screen appears:



Figure 3-6 Commit Status

If the configured parameters requires reboot, on committing the following screen appears.

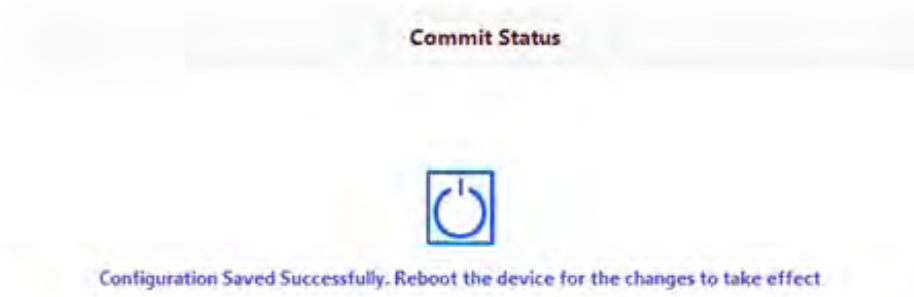


Figure 3-7 Commit Status with Reboot Message

### 3.2.3 REBOOT

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. On clicking **Reboot**, system displays a confirmation window, as shown below.

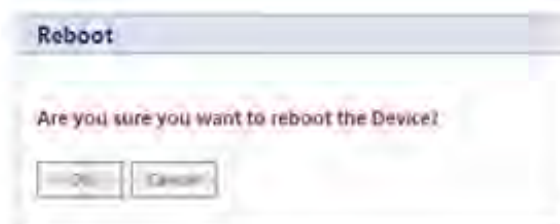


Figure 3-8 Reboot



It is always mandatory to commit the changes before **REBOOT**, otherwise the changes will not take effect. To reboot the device, click **OK**.

### 3.3 Factory Default Configuration

Parameter	BSU Mode/ End Point A	SU Mode/ End Point B
User Password	Public	Public
System Name	System-Name	System-Name
Network Mode	Bridge	Bridge
Routing	Disabled	Disabled
IP Address	169.254.128.132	169.254.128.132
Subnet Mask	255.255.255.0	255.255.255.0
Address Type	Static	Static
Gateway IP Address	169.254.128.132	169.254.128.132
Network Name	MY_NETWORK	MY_NETWORK
Maximum Number of SUs (per BSU)	As per license	Not Applicable
Registration Timeout	10 Seconds	10 Seconds
DDRS	Enabled	Enabled
Input Bandwidth Limit	As per license	As per license
Output Band Limit	As per license	As per license
Security Profile	Enabled with profile name "WORP Security"	Enabled with profile name "WORP Security"

Parameter	BSU Mode/ End Point A	SU Mode/ End Point B
RADIUS Profile	Enabled with profile name "Default Radius"	Not Applicable
MAC Authentication	Disabled	Not Applicable
RADIUS MAC Authentication	Disabled	Not Applicable
Channel Bandwidth	20 MHz	20 MHz
Active Channel Selection	Disabled	Enabled
ATPC	Enabled	Enabled
Network Secret	Public	Public
QoS	Unlimited BE	Not Applicable
Management VLAN	Disabled	Disabled
VLAN Status	Disabled	Disabled
VLAN Mode (Ethernet)	Transparent	Transparent
Global Filtering	Disabled	Disabled
DHCP Server	Disabled	Disabled
STP/LACP	Enabled (configured as "passthru")	Enabled (configured as "passthru")
DHCP Relay	Disabled	Disabled
IGMP Snooping	Disabled	Disabled
RIP	Disabled	Disabled
NAT	Disabled	Disabled
PPPoE Client	Not Applicable	Disabled in SU Mode Not Applicable in End Point B
HTTP Management Interface	Enabled	Enabled
Telnet Management Interface	Enabled	Enabled
SNMP Management Interface	Enabled with SNMPv1-v2c	Enabled with SNMPv1-v2c
Simple Network Time Protocol (SNTP)	Disabled	Disabled
Management Access Control	Disabled	Disabled
Event Log Priority	Notice	Notice
SysLog Status	Enabled	Enabled
SysLog Priority	Critical	Critical

## Basic Configuration

The **BASIC CONFIGURATION** tab provides a one-place access to a minimum set of configuration parameters to quickly set up a Point-to-point or Point-to-multipoint network.

To configure basic parameters of the device, click **BASIC CONFIGURATION** tab. The following screen appears:

**Basic Configuration**

System Name: System-Name (0-64) characters

Frequency Domain: World S GHz \*

Radio Mode: BSU \*

Channel Bandwidth: 20 MHz \*

Auto Channel Selection: Disable

Preferred Channel: 160 | 5.8GHz

Active Channel: 160 | 5.8GHz

DDRS Status: Enabled

Network Name: MY\_NETWORK

Legacy Mode: Disable

**IP Configuration\***

Interface	IP Address	Subnet Mask	Address Type
Ethernet 1	169.254.128.132	255.255.255.0	Static

**Default Gateway IP Address\***

IP Address: 169.254.128.132

**Notes :**

1. Channel Bandwidth change will reset the Tx Rate to default value.
2. Change in Channel Bandwidth and Frequency Domain will reset the Max EIRP to default value.
3. Radio Mode change will reset Wireless and WORP parameters to default values after reboot.
4. \* Reboot is required

OK

Figure 4-1 Basic Configuration (BSU)

### Basic Configuration

System Name	<input type="text" value="System-Name"/>	(0-64) characters
Frequency Domain	<input type="button" value="World 5 GHz"/>	*
Radio Mode	<input type="button" value="SU"/>	*
Channel Bandwidth	<input type="button" value="20"/>	MHz *
Auto Channel Selection	<input type="button" value="Enable"/>	
Active Channel	123 (5.615 GHz)	
DDRS Status	Enabled	
Network Name	<input type="text" value="MY_NETWORK"/>	
BSU Name	<input type="text" value="xyz"/>	

### IP Configuration\*

Interface	IP Address	Subnet Mask	Address Type
Ethernet 1	<input type="text" value="169.254.128.132"/>	<input type="text" value="255.255.255.0"/>	<input type="button" value="Static"/>

### Default Gateway IP Address\*

IP Address

**Notes :**

1. Channel Bandwidth change will reset the Tx Rate to default value.
2. Change in Channel Bandwidth and Frequency Domain will reset the Max EIRP to default value.
3. Radio Mode change will reset Wireless and WORP parameters to default values after reboot.
4. \* Reboot is required

Figure 4-2 Basic Configuration (SU)

**Basic Configuration**

System Name: System-Name (0-64 characters)

Frequency Domain: World 5 GHz \*

Radio Mode: End Point B \*

Channel Bandwidth: 20 MHz \*

Auto Channel Selection: Enable

Active Channel: 120 (5.6 GHz)

DDRS Status: Enabled

Network Name: MY\_NETWORK

End Point A Name: End A

**IP Configuration\***

Interface	IP Address	Subnet Mask	Address Type
Ethernet 1	169.254.128.132	255.255.255.0	Static

**Default Gateway IP Address\***

IP Address: 169.254.128.132

**Notes :**



1. Channel Bandwidth change will reset the Tx Rate to default value.
2. Change in Channel Bandwidth and Frequency Domain will reset the Max EIRP to default value.
3. Radio Mode change will reset Wireless and WORP parameters to default values after reboot.
4. \* Reboot is required

OK



Figure 4-3 Basic Configuration (End Point B)

Tabulated below is the table which explains Basic parameters and the method to configure the configurable parameter(s):

Parameter	Description
System Name	Represents the system name of the device. By default, the system name is <b>System-Name</b> . You can change the system name to the desired one. Please note that the length of the name is limited to 64 characters.

Parameter	Description
Frequency Domain	<p>This parameter specifies the country of operation, permitted frequency bands and regulatory rules for that particular country or domain. When you choose 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 <b>Frequency domain</b> selection pre-selects and displays only the allowed frequencies for the selected country or domain.</p>  : <ul style="list-style-type: none"> <li>• Devices sold only in United States are pre-configured to scan and display only the outdoor frequencies permitted by the Federal Communications Commission (FCC). No other countries, channels, or frequencies can be configured. Devices sold outside United States support the selection of a country by the professional installer. Any change in the Frequency Domain, requires device reboot.</li> <li>• If World 5 GHz is selected from the Frequency Domain drop-down menu, channels only in the 5 GHz range are displayed for manual selection.</li> </ul> <p>For a non US device, the default Frequency Domain selected is <b>World 5GHz</b>. For more details on frequency domains, refer to <a href="#">Frequency Domains and Channels</a>.</p>
Radio Mode	<p>Represents the radio mode of the device. Based on the SKU, the radio mode is set to either BSU, SU, End Point A or End Point B.</p> <p>In case of a BSU device, you can toggle between BSU and SU modes. Similarly in case of End Point A device, you can toggle between End Point A and End Point B. But note that a change in radio mode will reset wireless and WOPR parameters of the device after reboot.</p>
Channel Bandwidth	<p>Represents the width of the frequency band that is used to transmit data on the wireless interface. By default, it is set to 20 MHz. 40 MHz can be selected for higher throughputs depending on the distance and signal quality. 5 and 10 MHz can be selected for greater flexibility in spectrum selection.</p>
Auto Channel Selection (ACS)	<p>Enables a device to select the best channel for data transmission on the wireless medium, with less interference. By default, ACS is disabled on a BSU/End Point A and enabled on a SU/End Point B device. When ACS is enabled on a BSU/End Point A, it scans all the channels and selects the best channel during the start up. If ACS is enabled on the SU/End Point B, it continuously scans all the channels till it connects to a BSU or End Point A respectively.</p>  : Irrespective of the ACS status, the BSU/Endpoint A will automatically select a new channel upon radar detection.
Preferred Channel	<p>Applicable only when the Auto Channel Selection (ACS) is disabled. This parameter enables you to select a specific channel (in the specified frequency domain) for the device to operate.</p>
Active Channel	<p>Displays the current active channel on which wireless interface is operating. When the Auto Channel Selection parameter is enabled or when the device moves to a different channel because of radar detection, this parameter enables you to view the current operating channel.</p>



Parameter	Description
DDRS Status	Applicable only when Dynamic Data Rate Selection (DDRS) is enabled on the device. It indicates that DDRS is enabled on the device. See <a href="#">DDRS</a> .
Tx Rate	Applicable only when Dynamic Data Rate Selection (DDRS) is disabled on the device. This parameter represents the data transmission rate of the device. You can configure the appropriate data rate based on the signal level.   : A change in Channel Bandwidth will reset the Tx Rate to default value.
Network Name	Network name to identify a wireless network. The network name can be of minimum 2 or maximum 32 characters. The default network name is <b>MY_NETWORK</b> .   : For a BSU and SU to establish a wireless link, both should in the same network. The same applies to End Point A and End Point B as well.
Legacy Mode	Applicable only to Tsunami® MP-8100-BSU device.  When enabled, allows the device to operate with the legacy products of the Tsunami® MP.11 family such as: MP.11 5054 series, 5012 series, 2454 series and so on. By default, this parameter is disabled.
BSU / End Point A Name	Applicable only to a SU/End Point B device.  Represents the BSU/End Point A name to which SU/End Point B is connected.
IP Configuration, and Default Gateway IP Address	See <a href="#">Network</a> .

After configuring the required parameters, click **OK** and then **COMMIT**.



: Reboot the device, if you have configured any of the parameters with an asterisk symbol marked against them.

## Advanced Configuration

The **ADVANCED CONFIGURATION** tab provides a means to configure the following advanced features of the device:

- [System](#)
- [Network](#)
- [Ethernet](#)
- [Wireless](#)
- [Security](#)
- [Quality of Service \(QoS\)](#)
- [RADIUS Based SU QoS Configuration](#)
- [VLAN \(Bridge Mode Only\)](#)
- [RADIUS Based SU VLAN Configuration](#)
- [Filtering \(Bridge Only\)](#)
- [DHCP](#)
- [IGMP Snooping](#)
- [Routing Mode Features](#)

### 5.1 System


The **System** tab enables you to configure system specific information.

To configure system specific parameters, navigate to **ADVANCED CONFIGURATION > System**. The **System** screen appears:

**Figure 5-1 System Configuration**

Tabulated below is the table which explains System parameters and the method to configure the configurable parameter(s):

Parameter	Description
Radio Mode	Represents the radio mode of the device. Based on the device, the radio mode is set to either BSU, SU, End Point A or End Point B. In case of a BSU device, you can toggle between BSU and SU modes. Similarly in case of End Point A or End Point B device, you can toggle between End Point A and End Point B. But note that a change in radio mode will reset wireless and WORP parameters of the device after reboot.

Parameter	Description
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. See <a href="#">Frequency Domain</a> .
Network Mode	The device can be configured in two network modes: <b>Bridge</b> and <b>Routing</b> . By default, the network mode is <b>Bridge</b> mode.
Active Network Mode	A change in the network mode (either Bridge or Routing mode) is applied on the device only when the device is rebooted.  So, when the network mode is changed and the device is not rebooted, this parameter displays the current operating network mode of the device.
Maximum MTU (Maximum Transmission Unit)	Largest size of the data packet that can be sent to/from the Ethernet interface of the device. By default, the MTU size is 1500 bytes. It can be configured with any value ranging from 1500 to 2048 bytes. The MTU size excludes Ethernet Header(14 bytes) + Frame Check Sequence (4 bytes) + VLAN Tag(4 bytes).   : <ul style="list-style-type: none"> <li>Not all devices support this parameter.</li> <li>MTU is configurable only in Tsunami® MP-8150-CPE, Tsunami® MP-8160-CPE and Tsunami® QB-8150-EPR-12/50 devices.</li> <li>For optimal performance, MTU should be configured same on both local and remote devices.</li> <li>By default, Maximum MTU for Tsunami® MP-8100-BSU, Tsunami® MP-8100-SUA, MP-8150-SUR, Tsunami® MP-8160-BSU, Tsunami® MP-8160-SUA, Tsunami® QB-8100-EPA, Tsunami® QB-8150-EPR is not configurable and set to 1500 excluding Ethernet Header(14 bytes) + Frame Check Sequence (4 bytes) + VLAN Tag(4 bytes).</li> </ul>
Frequency Filter Lower Edge, and Frequency Filter Upper Edge	These parameters enable you to define the lower and upper frequency band edges, which helps to limit the available frequency band, for a given frequency domain, to a smaller band. By limiting the frequency band, the time taken by a device to scan and connect to any other device in the network is reduced.  You can enter frequencies ranging from 0 to 10000 MHz. By default the lower frequency is set to 0 MHz and higher frequency is set to 10000 MHz.

After configuring the required parameters, click **OK**, **COMMIT** and then **REBOOT**.

## 5.2 Network

The **Network** tab allows you to view and configure the network specific information of the device.

To view the current operating network mode of the device, navigate to **ADVANCED CONFIGURATION > Network**. If the network mode of the device is configured in **Bridge** mode, then following screen appears:



Figure 5-2 Bridge Mode

If the network mode of the device is configured in **Routing** mode, then the following screen appears:



Figure 5-3 Routing Mode

### 5.2.1 IP Configuration (Bridge Mode)


To configure the IP parameters of the device when operating in Bridge mode, navigate to **ADVANCED CONFIGURATION > Network > IP Configuration**. The following **IP Configuration** screen appears:



Figure 5-4 IP Configuration (Bridge Mode)

Tabulated below is the table which explains the method to configure IP parameters in Bridge mode:

Parameter	Description
<b>Ethernet</b>	
Please note that the number of Ethernet interfaces depend on your device.	

Parameter	Description
Address Type	<p>Specifies whether the Ethernet interface parameters are to be configured through Dynamic Host Configuration Protocol (DHCP) or to be assigned statically.</p> <p>By default, the address type is set to <b>Static</b> meaning which the user can manually configure the network parameters. Select <b>Dynamic</b> to configure the device as a DHCP client. If <b>Dynamic</b> is selected, the device obtains the IP parameters 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 <b>Static</b>.</p> <p> : DHCP Client (IP Address Type Dynamic) is applicable in Bridge Mode, and is applicable on wireless interface in Routing mode only when PPPoE is enabled .</p>
IP Address	<p>Represents the IP address of the Ethernet interface.</p> <p>When the address type is set to <b>Static</b> (default address type), the static IP address by default is set to 169.254.128.132. When set to static, you can manually change the IP address.</p> <p>When the address type is set to <b>Dynamic</b>, this parameter is read-only and displays the device IP address obtained from the DHCP server. The device will fallback to 169.254.128.132, if it cannot obtain the IP address from the DHCP server.</p>
Subnet Mask	<p>Represents the subnet mask of the Ethernet interface.</p> <p>When the address type is set to <b>Static</b> (default address type), the subnet mask by default is set to 255.255.255.0. When set to static, you can manually change the subnet mask.</p> <p>When the address type is set to <b>Dynamic</b>, this parameter is read-only and displays the device current subnet mask obtained from the DHCP server. The subnet mask will fallback to 255.255.255.0, if the device cannot obtain the subnet mask from the DHCP server.</p>
<b>Default Gateway IP Address</b>	
IP Address	<p>Represents the gateway IP address of the device.</p> <p>When the address type is set to <b>Static</b> (default address type), the gateway IP address by default is set to 169.254.128.132. When set to static, you can manually change the gateway IP address.</p> <p>When the address type is set to <b>Dynamic</b>, this parameter is read-only and displays the device's current gateway IP address that is obtained from the DHCP server. The gateway IP address will fallback to 169.254.128.132, if it cannot obtain the gateway IP address from a DHCP server.</p>
<b>DNS</b>	
Primary IP Address	<p>Represents the IP address of the Primary DNS Server.</p> <p>When the address type is set to <b>Dynamic</b>, this parameter is read-only and displays the DNS Primary IP Address obtained from the DHCP server. If the address type is set to <b>Static</b>, then you will have to manually enter the primary IP Address.</p>

Parameter	Description
Secondary IP Address	Represents the IP address of the Secondary DNS Server.  When the address type is set to <b>Dynamic</b> , this parameter is read-only and displays the DNS Secondary IP Address obtained from the DHCP server. If the address type is set to <b>Static</b> then you will have to manually enter the secondary IP Address.

After configuring the required parameters, click **OK**, **COMMIT** and then **REBOOT**.

### 5.2.2 IP Configuration (Routing Mode)

To configure the IP parameters of the device when operating in Routing mode, navigate to **ADVANCED CONFIGURATION > Network**. The **IP Configuration** screen appears:

Figure 5-5 IP Configuration (Routing Mode)

Tabulated below is the table which explains the method to configure IP parameters in Routing mode:

Parameter	Description
<b>Ethernet</b>	
Please note that the number of Ethernet interfaces depend on your device.	

Parameter	Description
IP Address	<p>Represents the IP address of the Ethernet interface.</p> <p>By default, the static IP address for Ethernet1 is set to 169.254.128.132 and for Ethernet2 it is set to 169.254.129.132.</p> <p>You can manually change the IP address.</p>
Subnet Mask	<p>Represents the subnet mask of the Ethernet interface.</p> <p>By default, the static subnet mask is set to 255.255.255.0. You can manually change the subnet mask.</p>
<b>Wireless</b>	
IP Address	<p>Represents the IP address of the wireless interface.</p> <p>By default, the static IP address is set to 169.254.130.132. You can manually change the IP address.</p>
Subnet Mask	<p>Represents the subnet mask of the wireless interface.</p> <p>By default, the static subnet mask is set to 255.255.255.0. You can manually change the subnet mask.</p>
<b>Default Gateway IP Address</b>	
IP Address	<p>Represents the gateway IP address of the device.</p> <p>By default, the Gateway IP address is set to 169.254.128.132. You can manually change the gateway IP address.</p>
<b>DNS</b>	
Primary IP Address	Represents the IP Address of the Primary DNS Server.
Secondary IP Address	Represents the IP Address of the Secondary DNS Server.

After configuring the required parameters, click **OK**, **COMMIT** and then **REBOOT**.



- To obtain dynamic IP address of the SU over WARP,
  - **Scenario 1:** When BSU and SU are in Bridge Mode with DHCP Client enabled in SU, and if DHCP server is behind BSU, SU will get the IP Address over WARP.
  - **Scenario 2:** When BSU is in Routing Mode and SU is in Bridge mode and DHCP server is in a different network than SU, then we need to configure DHCP relay in BSU to get the IP for SU over WARP.
  - **Scenario 3:** When BSU is in Routing mode and SU in Bridge mode with DHCP server running on wireless interface of BSU, then SU will get the IP address from BSU.

## 5.2.3 IP Configuration (Routing Mode with PPPoE Client Enabled)

 : **IP Configuration in Routing mode with PPPoE client enabled is applicable only in SU mode. See PPPoE End Point (SU Only)**

To configure the IP parameters of the device when configured in Routing mode with PPPoE client enabled, navigate to **ADVANCED CONFIGURATION > Network**. The **IP Configuration** screen appears:



**IP Configuration**

**Ethernet \***

S.No.	IP Address	Subnet Mask
1	169.254.128.132	255.255.255.0
2	169.254.129.132	255.255.255.0

**Wireless\* (pppoe)**

S.No.	IP Address	Subnet Mask	Address Type
1	169.254.130.132	255.255.255.0	Static

**Default Gateway IP Address\***

IP Address: 169.254.128.132

**DNS\***

Primary IP Address: 00.00

Secondary IP Address: 00.00

**Notes:** 1.\* Reboot is required.  
2.DHCP Server must be disabled before changing the network configurations like IPAddress, Subnet Mask, Address Type.  
3.Only Wireless interface Address Type is Configurable. and that too only when PPPoE status is enabled.

OK

**Figure 5-6 IP Configuration (Routing Mode with PPPoE Client Enabled)**

Tabulated below is the table which explains the method to configure IP parameters in Routing mode with PPPoE client enabled:

Parameter	Description
<b>Ethernet</b>	
Please note that the number of Ethernet interfaces depend on your device.	
IP Address	Represents the IP address of the Ethernet interface.  By default, the static IP address for Ethernet1 is set to 169.254.128.132 and 169.254.129.132 for Ethernet2. You can manually change the IP address.
Subnet Mask	Represents the subnet mask of the Ethernet interface.  By default, the static subnet mask is set to 255.255.255.0. You can manually change the subnet mask.



Parameter	Description
<b>Wireless (PPPoE)</b>	
Address Type	<p>This parameter specifies whether the wireless interface parameters are to be configured through PPPoE server or to be assigned statically.</p> <p>By default, the address type is set to <b>PPPoE-iccp</b> meaning which the PPPoE client obtains the IP parameters from a network PPPoE server automatically during the bootup. To manually configure the PPPoE Client's IP settings, select <b>Static</b>.</p>
IP Address	<p>Represents the IP address of the wireless interface.</p> <p>When the address type is set to <b>PPPoE-iccp</b>, this parameter is read-only and displays the PPPoE client's IP address obtained from the PPPoE server. The client will fallback to 169.254.130.132, if it cannot obtain the IP address from the PPPoE server.</p> <p>When the address type is set to <b>Static</b>, the IP address by default is set to 169.254.130.132. You can manually change the IP address.</p>
Subnet Mask	<p>Represents the subnet mask of the wireless interface.</p> <p>When the address type is set to <b>PPPoE-iccp</b>, this parameter is read-only and is set to Host Mask as it is a point-to-point interface. The client will fallback to 255.255.255.0, if it cannot obtain the IP address from the PPPoE server.</p> <p>When the address type is set to <b>Static</b>, the subnet mask by default is set to 255.255.255.0. You can manually change the subnet mask.</p>
<b>Default Gateway IP Address</b>	
IP Address	<p>Represents the gateway IP address of the device.</p> <p>When the address type is set to <b>PPPoE-iccp</b>, this parameter is read-only and displays the PPPoE client's gateway IP address (which is nothing but the IP address of the PPPoE server). If it cannot obtain the IP address from a PPPoE server, then there will be no gateway for the device.</p> <p>When the address type is set to <b>Static</b>, the gateway IP address by default is set to 169.254.128.132. You can manually change the gateway IP address.</p>
<b>DNS</b>	
Primary IP Address	Represents the IP Address of the Primary DNS Server.
Secondary IP Address	Represents the IP Address of the Secondary DNS Server.

After configuring the required parameters, click **OK**, **COMMIT** and then **REBOOT**.

## 5.3 Ethernet

The **Ethernet** tab allows you to view and configure the Ethernet interface properties of the device.

### 5.3.1 Basic Ethernet Configuration


To view and perform basic Ethernet configuration, navigate to **ADVANCED CONFIGURATION > Ethernet**. The **Ethernet Interface Properties** screen appears:



**Figure 5-7 Basic Ethernet Configuration**

Tabulated below is the table which explains Basic Ethernet parameters and the method to configure the configurable parameter(s):

Parameter	Description						
MAC Address	Displays the MAC address of the Ethernet interface.						
Operational Speed	<p>Displays the current operational speed of the Ethernet interface.</p> <p>Tabulated below is the maximum operational speed of the Ethernet interface product wise:</p> <table border="1"> <thead> <tr> <th>Product</th> <th>Maximum Speed</th> </tr> </thead> <tbody> <tr> <td> <ul style="list-style-type: none"> <li>• Tsunami® MP-8100-BSU</li> <li>• Tsunami® MP-8100-SUA</li> <li>• Tsunami® MP-8150-SUR</li> <li>• Tsunami® MP-8160-BSU</li> <li>• Tsunami® MP-8160-SUA</li> <li>• Tsunami® QB-8100-EPA</li> <li>• Tsunami® QB-8100-LNK</li> <li>• Tsunami® QB-8150-EPR</li> <li>• Tsunami® QB-8150-LNK</li> </ul> </td> <td>1 Gbps</td> </tr> <tr> <td> <ul style="list-style-type: none"> <li>• Tsunami® MP-8150-CPE</li> <li>• Tsunami® MP-8160-CPE</li> <li>• Tsunami® QB-8150-EPR-12/50</li> </ul> </td> <td>100 Mbps</td> </tr> </tbody> </table>	Product	Maximum Speed	<ul style="list-style-type: none"> <li>• Tsunami® MP-8100-BSU</li> <li>• Tsunami® MP-8100-SUA</li> <li>• Tsunami® MP-8150-SUR</li> <li>• Tsunami® MP-8160-BSU</li> <li>• Tsunami® MP-8160-SUA</li> <li>• Tsunami® QB-8100-EPA</li> <li>• Tsunami® QB-8100-LNK</li> <li>• Tsunami® QB-8150-EPR</li> <li>• Tsunami® QB-8150-LNK</li> </ul>	1 Gbps	<ul style="list-style-type: none"> <li>• Tsunami® MP-8150-CPE</li> <li>• Tsunami® MP-8160-CPE</li> <li>• Tsunami® QB-8150-EPR-12/50</li> </ul>	100 Mbps
Product	Maximum Speed						
<ul style="list-style-type: none"> <li>• Tsunami® MP-8100-BSU</li> <li>• Tsunami® MP-8100-SUA</li> <li>• Tsunami® MP-8150-SUR</li> <li>• Tsunami® MP-8160-BSU</li> <li>• Tsunami® MP-8160-SUA</li> <li>• Tsunami® QB-8100-EPA</li> <li>• Tsunami® QB-8100-LNK</li> <li>• Tsunami® QB-8150-EPR</li> <li>• Tsunami® QB-8150-LNK</li> </ul>	1 Gbps						
<ul style="list-style-type: none"> <li>• Tsunami® MP-8150-CPE</li> <li>• Tsunami® MP-8160-CPE</li> <li>• Tsunami® QB-8150-EPR-12/50</li> </ul>	100 Mbps						

Parameter	Description
Operational Tx Mode	Displays the current operational transmission mode of the Ethernet interface. It supports two types of transmission modes: <ul style="list-style-type: none"> <li>• <b>Half Duplex:</b> Allows one-way data transmission at a time.</li> <li>• <b>Full Duplex:</b> Allows two-way transmission simultaneously.</li> </ul>
Speed And TxMode	Enables the user to select the speed and transmission mode of the Ethernet interface. By default, it is set to <b>Auto</b> . When set to Auto (recommended to set), both the transmitter and the receiver negotiate and derive at the best transmission mode.   : Please ensure the same transmission modes are configured on the transmitter and the receiver device.
Admin Status	This parameter is applicable only when the device support more than one Ethernet interface. By default, both the Ethernet interfaces of the device are enabled. The first Ethernet interface is always enabled; whereas the second Ethernet interface can be either enabled or disabled as desired.

After configuring the required parameters, click **OK** and then **COMMIT**.

Reboot the device, if you have changed the **Admin Status** configuration.

### 5.3.2 Advanced Configuration

The Advanced Configuration feature enables you to achieve high availability and link aggregation in wireless medium by using two parallel links and additional Link Aggregation Control Protocol (LACP) capable switches.




**Applicable only to Tsunami® QB-8100-EPA, Tsunami® QB-8100-LNK, Tsunami® QB-8150-EPR, and Tsunami® QB-8150-LNK.**

To view and perform advanced Ethernet configuration, click **Advanced** in the **Ethernet Interface Properties** screen. The following screen appears:



Figure 5-8 Advanced Ethernet Configuration

Tabulated below is the table which explains Advanced Ethernet parameters and the method to configure the configurable parameter(s):

Parameter	Description
Auto Shutdown	<p>This parameter facilitates LACP capable Ethernet switches to use two Quick Bridge links to achieve higher throughput and redundancy. By default, it is <b>Disabled</b>.</p> <p>If <b>Auto Shutdown</b> is enabled on the Ethernet Interface, then the Ethernet port will be automatically disabled, when the wireless link goes down. It will be automatically enabled once the wireless link is up again.</p> <p> : This feature works only if <b>STP/LACP Frames</b> is set to passthru (See <b>ADVANCED CONFIGURATION &gt; Filtering</b>)</p> <p>Tsunami® Quick Bridge devices that are part of LACP link cannot be managed through the switches, so it is recommended to use the second ethernet port for management.</p>

After configuring the required parameters, click **OK** and then **COMMIT**.

## 5.4 Wireless

The **Wireless** tab allows you to configure the wireless properties for the radio interface of the device.

### 5.4.1 Wireless Outdoor Router Protocol (WORP)

WORP is protocol, designed by Proxim that protects the network from packet collisions and solves the hidden node problem to transmit the data in an optimal way.

To configure the WORP properties, navigate to **ADVANCED CONFIGURATION > Wireless > Interface1 > WORP**. The **WORP Configuration** screen appears:

### WORP Configuration




Mode	BSU		
Network Name	<input type="text" value="MY_NETWORK"/>	(2-32) characters	
Max SUs	<input type="text" value="100"/>	(1-100)	
WORP MTU	<input type="text" value="3808"/>	(350-3808) Bytes	
Super Framing	Enable <span style="float: right;">▼</span>		
Sleep Mode	Disable <span style="float: right;">▼</span>		
Multi Frame Bursting	Enable <span style="float: right;">▼</span>		
Auto Multi Frame Bursting	Enable <span style="float: right;">▼</span>		
Registration Timeout	<input type="text" value="10"/>	(1-10) Seconds	
Retry Count	<input type="text" value="3"/>	(0-10)	
DDRS Status	Enabled		
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	Shaping <span style="float: right;">▼</span>		
Security Profile Name	WORP Security <span style="float: right;">▼</span>		
Radius Profile Name	Default Radius <span style="float: right;">▼</span>		
MAC ACL Status	Disable <span style="float: right;">▼</span>		
RADIUS MAC ACL Status	Disable <span style="float: right;">▼</span>		
Poll BackOff on Timeout	Disable <span style="float: right;">▼</span>		





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




Figure 5-9 WORP Configuration

Tabulated below is the table which explains WORP parameters and the method to configure the configurable parameter(s):

Parameter	Description
Mode	Represents the device type (BSU, SU, End Point A or End Point B)
BSU Name	Applicable only to SU. It specifies the name of the BSU to which a SU can establish wireless connection. If this parameter is left blank, SU can establish a link with any BSU.
End Point A Name	Applicable only in End Point B mode. It specifies the name of the End Point A to which End Point B can establish wireless connection. If this parameter is left blank, End Point B can establish a link with any End Point A.
Network Name	It is a unique name given to a logical network. Devices only within this logical network can establish wireless connection.  The Network Name can be of 2 to 32 characters in length. By default it is <b>MY_NETWORK</b> .

Parameter	Description
Max SUs	<p>Represents the maximum number of SUs that can register with a BSU. The maximum SUs are limited to the licensed number of SUs.</p> <p> : Applicable only in BSU mode.</p>
WORP MTU	<p>WORP MTU (Maximum Transmission Unit) is the largest size of the data payload in wireless frame that can be transmitted. The MTU size can range from <b>350 to 3808</b> bytes for High throughput modes and <b>350 to 2304</b> bytes for legacy mode. The default and maximum value of the WORP MTU is <b>3808</b> bytes for higher throughput and <b>2304</b> bytes for legacy mode.</p>
Super Framing	<p>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. By default it is <b>Enabled</b>.</p>
Sleep Mode	<p>A BSU can put SUs in sleep mode when there is no data transmission during the past 15 seconds. This reduces the traffic congestion in the wireless medium and preserves the wireless bandwidth for other SUs in the network. BSU polls sleeping SUs once in every 4 seconds to maintain the wireless connection. By default, it is <b>Disabled</b>.</p> <p> : Applicable only in BSU mode.</p>
Multi Frame Bursting	<p>To achieve higher throughput, WORP protocol allows the transmitter or receiver to send multiple data frames in sequence without waiting for acknowledgment for every data frame and treats it as a single burst. During the burst transmission, the receiver is not allowed to interrupt the transmitter. After completion of the burst, the receiver response by sending the acknowledgement.</p> <p>By default, the Multi Frame Bursting feature is <b>Enabled</b> on the device. When Multi Frame Bursting is enabled, the maximum data frames that can be transmitted for each burst can be configured as part of <a href="#">Quality of Service (QoS)</a>.</p> <p> : Though Multi Frame Bursting configuration is not applicable from SU/End Point B, the SU/End Point B does Multi Frame Bursting under the control of BSU/End Point A respectively.</p>

Parameter	Description
Auto Multi Frame Bursting	<p>Auto Multi Frame Bursting feature takes effect only when Multi Frame Bursting feature is Enabled.</p> <p>When this feature is enabled, the device monitors all active QoS Service Flow Classes and determines the highest priority QoS Service Flow Class for every wireless connection. The device enables the burst transmission for the active highest priority QoS Service Flow Class and disables the burst transmission for other active lower priority QoS Service Flow Classes. By default, Auto Multi Frame Bursting is <b>Enabled</b> on the device.</p>  : <ul style="list-style-type: none"> <li>• When using Software Version 2.4.0, it is recommended to disable Auto Multi Frame Bursting.</li> <li>• Though Auto Multi Frame Bursting configuration is not applicable from SU/End Point B, the SU/End Point B does Auto Multi Frame Bursting under the control of BSU/End Point A respectively.</li> </ul>
Registration Timeout	<p>Represents the maximum time for a SU to register with a BSU or vice versa, or an End Point B to register with an End Point A or vice versa. The registration timeout value can be set in the range 1 to 10 seconds. The default registration timeout value is <b>10 seconds</b>.</p>
Retry Count	<p>Represents the maximum number of times the data is retransmitted by the transmitter over the wireless medium, if acknowledgement from the peer is not received. The Retry Count parameter can be configured in the range 0 to 10 seconds. By default, it is set to <b>3</b>.</p>
DDRS Status	 : Applicable only when DDRS is enabled. <p>It is a read-only parameter that displays the status of the DDRS feature. For more details refer to <a href="#">DDRS</a>.</p>
Tx Rate	<p>Represents the modulation rate at which the packets are transmitted from the wireless device. Please note that the a change in Channel Bandwidth, Guard Interval and Number of Data Streams will reset Tx rate to default values.</p>  : Applicable only when the DDRS is disabled on the device. See <a href="#">DDRS</a> .
Input or Output Bandwidth Limit	<p>This parameter limits the data received or transmitted to the wireless interface. It limits the data from a minimum of 64 Kbps to the maximum value specified in the License File.</p>  : Input/Output Bandwidth throttling does not throttle broadcast/multicast traffic. These traffic can be trottled by the Maximum Information Rate (MIR) / Committed Information Rate (CIR) configured for <b>DL-L2 Broadcast BE</b> in QoS Service Flow. See <a href="#">QoS Service Flow Configuration (SFC)</a>

Parameter	Description
Bandwidth Limit Type	<p>Specifies the action performed when the traffic utilization exceeds the configured input or output limits. By default it is set to <b>Shaping</b>.</p> <ul style="list-style-type: none"> <li>• <b>Policing</b>: When the traffic utilization reaches the configured limit, the excess traffic will be discarded.</li> <li>• <b>Shaping</b>: 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.</li> </ul>
Security Profile Name	The Security Profile Name represents the encryption method used to encrypt the data over the wireless medium. The default configured Security Profile Name is <b>WORP Security</b> . See <a href="#">Security</a> .
Radius Profile Name	<p>The Radius Profile Name, containing the IP address of the RADIUS server, is used to authenticate a SU or an End Point B. See <a href="#">RADIUS</a>.</p> <p> : Not applicable in SU mode and End Point B mode.</p>
MAC ACL Status	<p>When enabled, based on the configured ACL list, the BSU/End Point A decides if SU/End Point B can register with them respectively.</p> <p> : Not applicable in SU mode and End Point B mode.</p>
Radius MAC ACL Status	<p>This parameter is used to enable authentication using RADIUS server. When enabled, the BSU or End Point A contacts the RADIUS server for authenticating the SU or End Point B during the registration process.</p> <p> : Not applicable in SU mode and End Point B mode.</p>
Poll BackOff on Timeout	<p>When enabled, the BSU will back-off polling the SUs that timeout (due to interference or low SNR etc).</p> <p>When multiple SUs are connected, it is possible that some SUs are performing well without much retransmissions and other SUs are timing out. In such as scenario to make sure that the good SUs do not suffer due to under performing SUs it is recommended to enable this parameter.</p> <p>By default this parameter is disabled. It is recommended that this parameter should be enabled only when there is a mix of good and bad SUs and when good SUs are really suffering.</p>

After configuring the required parameters, click **OK** and then **COMMIT**.



- Modifying any of the WORP parameters result in temporary loss of connectivity between transmitter and receiver.



- MAC ACL Status and Radius MAC ACL Status parameters cannot be enabled simultaneously.
- When you modify WORP parameters and click **COMMIT**, it may result in brief interruption.

### 5.4.2 Wireless Interface Properties

To configure the wireless interface properties, navigate to **ADVANCED CONFIGURATION > Wireless > Interface 1 > Properties**. The **Wireless Interface Properties** screen appears depending on your device:

Parameter	Value	Unit/Range
Channel Bandwidth	20	MHz
Channel Offset	0	
Auto Channel Selection	Disable	
Preferred Channel	260 (6.3 GHz)	
Active Channel	260 (6.3 GHz)	
Satellite Density	Micro	
ATPC Status	Enable	
Max EIRP	100	(0-100) dBm
Active TPC	10.0	dBm
Active EIRP	27	dBm
Active Power	12	dBm
Antenna Gain	15	(0-40) dBi
Wireless Inactivity Timer	10	(0.5-600) Seconds

**Notes :**

1. Channel Bandwidth change will reset the Tx Rate to default value.
2. Channel Bandwidth change will reset the Max EIRP to default value.
3. Reboot is required





OK



Figure 5-10 Wireless Interface Properties


The Wireless Interface Properties screen is classified under two categories: **Basic** and **Advanced**.

## Basic Configuration



Under **Basic Configuration** screen, you can configure and view the following parameters.


Parameter	Descriptions
Channel Bandwidth	<p>By default, the channel bandwidth is set to <b>20 MHz</b>. 40 MHz can be selected for higher throughputs depending on the distance and signal quality. 5 and 10 MHz can be selected for greater flexibility in spectrum selection.</p> <p> : A change in Channel Bandwidth will reset the Tx Rate and Maximum EIRP to default.</p>
Channel Offset	<p> : Applicable only to Tsunami® MP-8160-BSU; Tsunami® MP-8160-SUA; Tsunami® MP-8150-CPE; Tsunami® MP-8160-CPE; Tsunami® QB-8150-EPR-12/50 devices.</p> <p>The Channel Offset parameter helps to change the operating channel center frequency. If the predefined center frequencies are not desirable, user can shift the center frequency to suit the requirements by configuring the Channel Offset. By default, the Channel Offset is set to 0. You can configure the Channel Offset in the range -2 to +2 MHz.</p> <p>For example, consider a channel number 100 with center channel frequency set to 5500 MHz. If the Channel Offset is set to 0 MHz, the center channel frequency remains at 5500 MHz. If you configure the Channel Offset to 2MHz then the center channel frequency will change to 5502MHz. Similarly for a Channel Offset of -2MHz, the center channel frequency is changed to 5498 MHz.</p> <p> : Even though the center channel frequency is changed, the channel number still remains same, in this case 100.</p>
Auto Channel Selection (ACS)	<p>Auto Channel Selection (ACS) enables the device to determine the best channel for wireless data transmission with less interference.</p> <p>If ACS is enabled on the BSU/End Point A, it scans all the channels and selects the best channel at the startup. If ACS is enabled on the SU/End Point B, it continuously scans all the channels till it finds a suitable BSU/End Point A and connects to it. By default, ACS is <b>disabled</b> on BSU/End Point A and <b>enabled</b> on SU/End Point B.</p> <p> : On BSU/End Point A, ACS is performed only during startup.</p>
Preferred Channel	<p>Allows the user to select and operate in the preferred channel.</p> <p>Preferred channel can be configured only when ACS is disabled. If Dynamic Frequency Selection (DFS) is active, the device will automatically pick a new channel when radar interference is detected.</p>


Parameter	Descriptions																		
Active Channel	<p>A read-only parameter that displays the current operating channel on which the wireless interface is operating.</p>  : Active Channel can be different from Preferred Channel if radar interface is detected.																		
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. 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 set to <b>Large</b>. The Medium, Small, Mini, and Micro settings are appropriate for higher noise environments; whereas, Large is appropriate for a lower noise environment. A long distance link can have difficulty in 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 link, the BSU or End Point A should have a density setting suitable for an SU or End Point B, 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>Tabulated below are the Sensitivity Threshold Values corresponding to various Satellite Density values:</p> <table border="1" data-bbox="528 1355 1358 1702"> <thead> <tr> <th>Satellite Density</th> <th>Receive Sensitivity Threshold</th> <th>Defer Threshold</th> </tr> </thead> <tbody> <tr> <td>Large</td> <td>-96 dbm</td> <td>-62 dbm</td> </tr> <tr> <td>Medium</td> <td>-86 dbm</td> <td>-62 dbm</td> </tr> <tr> <td>Small</td> <td>-78 dbm</td> <td>-52 dbm</td> </tr> <tr> <td>Mini</td> <td>-70 dbm</td> <td>-42 dbm</td> </tr> <tr> <td>Micro</td> <td>-62 dbm</td> <td>-36 dbm</td> </tr> </tbody> </table>  : 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 restore the communication link. 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.	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
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																	

Parameter	Descriptions
ATPC Status	<p>If Adaptive Transmit Power Control (ATPC) is enabled, then the device automatically adjusts the transmit power to avoid saturation of remote receiver, which could cause data errors leading to lower throughput and link outage. If disabled, user can manually adjust the transmit power. By default, ATPC is enabled on the device.</p> <p>Transmit Power Control (TPC) is calculated based on two factors:</p> <ul style="list-style-type: none"> <li>• Equivalent Isotropically Radiated Power (EIRP)</li> <li>• Maximum Optimal SNR</li> <li>• Antenna Gain</li> </ul> <p> : In BSU, the ATPC considers the EIRP only; where as in SU, End Point A and End Point B both EIRP and Maximum SNR are considered.</p>

Parameter	Descriptions																																																																							
Max EIRP  The maximum effective power that a radio antenna is allowed to radiate as per the regulatory standard. By default, the maximum EIRP is set as per the regulatory requirements for each frequency domain.  Tabulated below are the default maximum EIRP values that are set according to regulatory domain:																																																																								
	<table border="1"> <thead> <tr> <th rowspan="2">Regulatory Domain</th> <th rowspan="2">Frequency (MHz)</th> <th colspan="2">Max EIRP (dBm)</th> </tr> <tr> <th>PTP Mode (QB)</th> <th>PTMP Mode (MP)</th> </tr> </thead> <tbody> <tr> <td>World</td> <td>All</td> <td>Unlimited (100)</td> <td>Unlimited (100)</td> </tr> <tr> <td rowspan="4">United States</td> <td>2402-2472</td> <td>32 + 2/3(antenna gain)</td> <td>BSU: 36 SU/CPE: 32 + 2/3 (antenna gain)</td> </tr> <tr> <td>4940 - 4990</td> <td>33 (20 MHz) 30 (10 MHz) 27 (5 MHz)</td> <td>33 (20 MHz) 30 (10 MHz) 27 (5 MHz)</td> </tr> <tr> <td>5250 - 5330</td> <td>30</td> <td>30</td> </tr> <tr> <td>5735 - 5835</td> <td>53</td> <td>36</td> </tr> <tr> <td rowspan="5">Canada</td> <td>4940 - 4990</td> <td>33 (20 MHz) 30 (10 MHz) 27 (5 MHz)</td> <td>33 (20 MHz) 30 (10 MHz) 27 (5 MHz)</td> </tr> <tr> <td>5250 - 5330</td> <td>30</td> <td>30</td> </tr> <tr> <td>5490 - 5590</td> <td>30</td> <td>30</td> </tr> <tr> <td>5650 - 5710</td> <td>30</td> <td>30</td> </tr> <tr> <td>5730 - 5860</td> <td>53</td> <td>36</td> </tr> <tr> <td rowspan="4">Europe (including UK)</td> <td>2402 - 2472</td> <td>20</td> <td>20</td> </tr> <tr> <td>5490 - 5590</td> <td>30</td> <td>30</td> </tr> <tr> <td>5650 - 5710</td> <td>30</td> <td>30</td> </tr> <tr> <td>5735 - 5875</td> <td>36</td> <td>36</td> </tr> <tr> <td rowspan="3">Russia</td> <td>5150 - 5350</td> <td>33</td> <td>33</td> </tr> <tr> <td>5350 - 5650</td> <td>Unlimited (100)</td> <td>Unlimited (100)</td> </tr> <tr> <td>5650 - 6425</td> <td>53</td> <td>53</td> </tr> <tr> <td rowspan="2">Taiwan</td> <td>5490 - 5710</td> <td>30</td> <td>30</td> </tr> <tr> <td>5735 - 5835</td> <td>36</td> <td>36</td> </tr> </tbody> </table>			Regulatory Domain	Frequency (MHz)	Max EIRP (dBm)		PTP Mode (QB)	PTMP Mode (MP)	World	All	Unlimited (100)	Unlimited (100)	United States	2402-2472	32 + 2/3(antenna gain)	BSU: 36 SU/CPE: 32 + 2/3 (antenna gain)	4940 - 4990	33 (20 MHz) 30 (10 MHz) 27 (5 MHz)	33 (20 MHz) 30 (10 MHz) 27 (5 MHz)	5250 - 5330	30	30	5735 - 5835	53	36	Canada	4940 - 4990	33 (20 MHz) 30 (10 MHz) 27 (5 MHz)	33 (20 MHz) 30 (10 MHz) 27 (5 MHz)	5250 - 5330	30	30	5490 - 5590	30	30	5650 - 5710	30	30	5730 - 5860	53	36	Europe (including UK)	2402 - 2472	20	20	5490 - 5590	30	30	5650 - 5710	30	30	5735 - 5875	36	36	Russia	5150 - 5350	33	33	5350 - 5650	Unlimited (100)	Unlimited (100)	5650 - 6425	53	53	Taiwan	5490 - 5710	30	30	5735 - 5835	36	36
	Regulatory Domain	Frequency (MHz)	Max EIRP (dBm)																																																																					
			PTP Mode (QB)	PTMP Mode (MP)																																																																				
	World	All	Unlimited (100)	Unlimited (100)																																																																				
	United States	2402-2472	32 + 2/3(antenna gain)	BSU: 36 SU/CPE: 32 + 2/3 (antenna gain)																																																																				
		4940 - 4990	33 (20 MHz) 30 (10 MHz) 27 (5 MHz)	33 (20 MHz) 30 (10 MHz) 27 (5 MHz)																																																																				
		5250 - 5330	30	30																																																																				
		5735 - 5835	53	36																																																																				
	Canada	4940 - 4990	33 (20 MHz) 30 (10 MHz) 27 (5 MHz)	33 (20 MHz) 30 (10 MHz) 27 (5 MHz)																																																																				
		5250 - 5330	30	30																																																																				
		5490 - 5590	30	30																																																																				
		5650 - 5710	30	30																																																																				
		5730 - 5860	53	36																																																																				
	Europe (including UK)	2402 - 2472	20	20																																																																				
5490 - 5590		30	30																																																																					
5650 - 5710		30	30																																																																					
5735 - 5875		36	36																																																																					
Russia	5150 - 5350	33	33																																																																					
	5350 - 5650	Unlimited (100)	Unlimited (100)																																																																					
	5650 - 6425	53	53																																																																					
Taiwan	5490 - 5710	30	30																																																																					
	5735 - 5835	36	36																																																																					

Parameter	Descriptions																											
	<table border="1" data-bbox="480 421 1385 1003"> <thead> <tr> <th data-bbox="480 421 671 524" rowspan="2">Regulatory Domain</th> <th data-bbox="676 421 868 524" rowspan="2">Frequency (MHz)</th> <th colspan="2" data-bbox="873 421 1385 472">Max EIRP (dBm)</th> </tr> <tr> <th data-bbox="873 479 1123 524">PTP Mode</th> <th data-bbox="1128 479 1385 524">PTMP Mode</th> </tr> </thead> <tbody> <tr> <td data-bbox="480 530 671 575">India</td> <td data-bbox="676 530 868 575">5825 - 5875</td> <td data-bbox="873 530 1123 575">36</td> <td data-bbox="1128 530 1385 575">36</td> </tr> <tr> <td data-bbox="480 582 671 712" rowspan="2">Brazil</td> <td data-bbox="676 582 868 627">5470 - 5725</td> <td data-bbox="873 582 1123 627">30</td> <td data-bbox="1128 582 1385 627">30</td> </tr> <tr> <td data-bbox="676 633 868 712">5725 - 5850</td> <td data-bbox="873 633 1123 712">Unlimited (100)</td> <td data-bbox="1128 633 1385 712">32 + 2/3(antenna gain)</td> </tr> <tr> <td data-bbox="480 719 671 1003" rowspan="3">Australia</td> <td data-bbox="676 719 868 828">5470 - 5600</td> <td data-bbox="873 719 1123 828">30 (20 and 40 MHz) 27 (10 MHz) 24 (5 MHz)</td> <td data-bbox="1128 719 1385 828">30 (20 and 40 MHz) 27 (10 MHz) 24 (5 MHz)</td> </tr> <tr> <td data-bbox="676 835 868 945">5650 - 5725</td> <td data-bbox="873 835 1123 945">30 (20 and 40 MHz) 27 (10 MHz) 24 (5 MHz)</td> <td data-bbox="1128 835 1385 945">30 (20 and 40 MHz) 27 (10 MHz) 24 (5 MHz)</td> </tr> <tr> <td data-bbox="676 952 868 1003">5725 - 5850</td> <td data-bbox="873 952 1123 1003">36</td> <td data-bbox="1128 952 1385 1003">36</td> </tr> </tbody> </table> <p data-bbox="475 1016 544 1093"> :</p> <ul data-bbox="507 1111 1334 1211" style="list-style-type: none"> <li>• The maximum EIRP is not defined in the above table then it is set to 100 (unlimited EIRP).</li> <li>• Maximum EIRP criterion is enforced only when ATPC is enabled.</li> </ul>	Regulatory Domain	Frequency (MHz)	Max EIRP (dBm)		PTP Mode	PTMP Mode	India	5825 - 5875	36	36	Brazil	5470 - 5725	30	30	5725 - 5850	Unlimited (100)	32 + 2/3(antenna gain)	Australia	5470 - 5600	30 (20 and 40 MHz) 27 (10 MHz) 24 (5 MHz)	30 (20 and 40 MHz) 27 (10 MHz) 24 (5 MHz)	5650 - 5725	30 (20 and 40 MHz) 27 (10 MHz) 24 (5 MHz)	30 (20 and 40 MHz) 27 (10 MHz) 24 (5 MHz)	5725 - 5850	36	36
Regulatory Domain	Frequency (MHz)			Max EIRP (dBm)																								
		PTP Mode	PTMP Mode																									
India	5825 - 5875	36	36																									
Brazil	5470 - 5725	30	30																									
	5725 - 5850	Unlimited (100)	32 + 2/3(antenna gain)																									
Australia	5470 - 5600	30 (20 and 40 MHz) 27 (10 MHz) 24 (5 MHz)	30 (20 and 40 MHz) 27 (10 MHz) 24 (5 MHz)																									
	5650 - 5725	30 (20 and 40 MHz) 27 (10 MHz) 24 (5 MHz)	30 (20 and 40 MHz) 27 (10 MHz) 24 (5 MHz)																									
	5725 - 5850	36	36																									
Active TPC	<p data-bbox="440 1234 1417 1290">A read-only parameter which displays the TPC applied by the device to adjust the transmit power, when ATPC is enabled.</p> <p data-bbox="475 1317 1353 1435"> : In case of BSU, the Active TPC refers to the TPC applied to the broadcast packets. To view Active TPC of each link, refer to <a href="#">SU / End Point B Link Statistics</a>.</p>																											
Active EIRP	A read-only parameter which displays the current EIRP that a radio antenna radiates.																											
Active Power	A read-only parameter which displays the current power radiated by the radio.																											

Parameter	Descriptions												
TPC	<p>This parameter enables you to manually set the Transmit Power Control (TPC) value when ATPC is disabled. You can manually set TPC ranging from 0 to 25 dBm.</p> <p>With 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. By default, it is set to <b>0 dBm</b>.</p>  <ul style="list-style-type: none"> <li>• TPC 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.</li> <li>• TPC can be configured in the steps of 0.5 dB</li> </ul>												
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 dBi. For devices with connectorized antenna, the Antenna Gain by default is set to zero dBi.</p> <p>Tabulated below are the default Antenna Gain, for devices with integrated antenna:</p> <table border="1" data-bbox="592 1279 1299 1626"> <thead> <tr> <th>Product (s)</th> <th>Antenna Gain</th> </tr> </thead> <tbody> <tr> <td>Tsunami® MP-8150-SUR</td> <td>23 dBi</td> </tr> <tr> <td>Tsunami® MP-8150-CPE</td> <td>16 dBi</td> </tr> <tr> <td>Tsunami® MP-8160-CPE</td> <td>15 dBi</td> </tr> <tr> <td>Tsunami® QB-8150-EPR/ Tsunami® QB-8150-LNK</td> <td>23 dBi</td> </tr> <tr> <td>Tsunami® QB-8150-EPR-12/50</td> <td>16 dBi</td> </tr> </tbody> </table>	Product (s)	Antenna Gain	Tsunami® MP-8150-SUR	23 dBi	Tsunami® MP-8150-CPE	16 dBi	Tsunami® MP-8160-CPE	15 dBi	Tsunami® QB-8150-EPR/ Tsunami® QB-8150-LNK	23 dBi	Tsunami® QB-8150-EPR-12/50	16 dBi
Product (s)	Antenna Gain												
Tsunami® MP-8150-SUR	23 dBi												
Tsunami® MP-8150-CPE	16 dBi												
Tsunami® MP-8160-CPE	15 dBi												
Tsunami® QB-8150-EPR/ Tsunami® QB-8150-LNK	23 dBi												
Tsunami® QB-8150-EPR-12/50	16 dBi												
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 <b>10 seconds</b> (disabled if set to 0 seconds) and can be configured between 5 to 600 seconds.</p>												

Parameter	Descriptions
Legacy Mode	<p>When Legacy Mode is enabled, the BSU can interoperate with the legacy products of the Tsunami MP.11 family: MP.11 5054 series, 5012 series, 2454 series and so on.</p> <p>By default, it is <b>disabled</b>.</p> <p> : Applicable only to Tsunami® MP-8100-BSU.</p>

After configuring the required parameters, click **OK** and then **COMMIT**.

Reboot the device, if you have changed any of the Wireless Interface parameters with asterisk (\*) symbol marked against them.

### Advanced

To view **Advanced** parameters, click **Advanced** tab in the **Wireless Interface Properties** screen. The following screen appears:



Figure 5-11 Advanced Wireless Properties

The following table lists the **Advanced** Wireless properties parameters and their description. Note that these parameters are read-only and can be configured only through CLI or SNMP.

Parameter	Description
ATPC Lower Margin and ATPC Upper Margin	<p>SNR Upper Limit = Maximum Optimal SNR            SNR Initial = SNR Upper Limit - ATPC Upper Margin            SNR Lower Limit = SNR Initial - ATPC Lower Margin</p> <p>ATPC Algorithm, after reducing the power to honor the Maximum EIPR limit, adjusts the power based on Maximum Optimal SNR, ATPC Upper Margin and ATPC Lower Margin. To begin with, ATPC will adjust the power to bring the SNR to <b>SNR Initial</b> and adjusts power only when the current SNR goes beyond the <b>SNR Upper Limit</b> and <b>SNR Lower Limit</b>.</p>

Click **Local SNR-Table**, to view the optimal SNR values that are exchanged with the peer for optimal throughput.



### 5.4.3 MIMO Properties

The **MIMO Properties** tab allows you to configure the Multiple-Input-Multiple-Output (MIMO) parameters that enable to achieve high throughput and longer range.

To configure MIMO properties, navigate to **ADVANCED CONFIGURATION > Wireless > Interface1 > MIMO Properties**. The **MIMO Properties** screen appears:

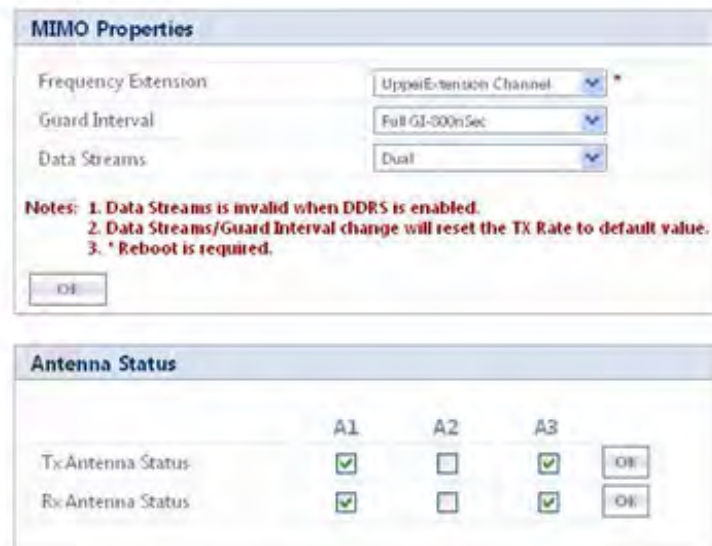


Figure 5-12 3x3 MIMO Properties

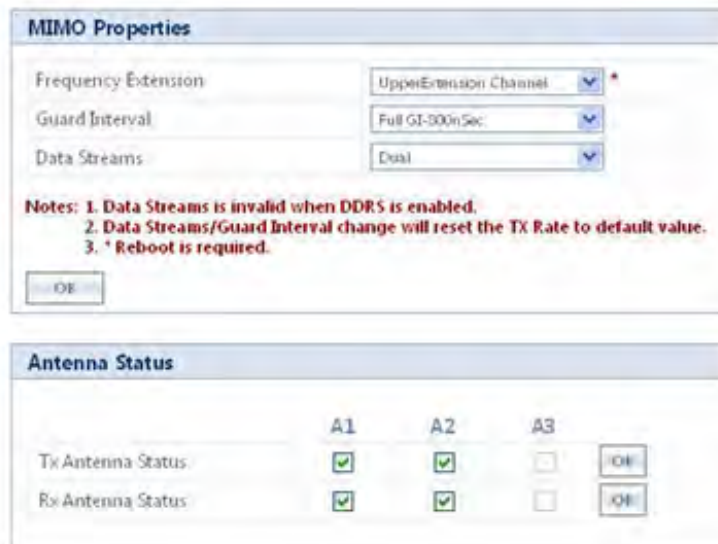







Figure 5-13 2x2 MIMO Properties

Tabulated below is the table which explains MIMO parameters and the method to configure the configurable parameters:

Parameter	Description
<b>MIMO Properties</b>	

Parameter	Description
Frequency Extension	<p>Frequency Extension is applicable only when the Channel Bandwidth is set to 40 MHz.</p> <p>While choosing 40MHz bandwidth, you can select either 40 PLUS (Upper Extension Channel) or 40 MINUS (Lower Extension Channel). 40 PLUS means the center frequency calculation is done for 20MHz and add another 20MHz to the top edge of 20MHz. 40 MINUS means the center frequency calculation is done for 20MHz and add another 20MHz to the bottom edge of 20MHz.</p>
Guard Interval	<p>Guard Interval determines the space between symbols being transmitted. The guard interval can be configured as either Short GI - 400n seconds or Full GI-800n seconds.</p> <p>In 802.11 standards, when 40 MHz Channel Bandwidth is configured then Short GI can be used to improve the overall performance and throughout.</p> <p>By default, Full GI is enabled for 5 MHz, 10 MHz and 20 MHz channels.</p> <p> : Short GI-400 nSec is valid only for 40 MHz channel bandwidth.</p>
Data Streams	<p>MIMO radio uses multiple antennas for transmitting and receiving the data.</p> <p>The data streams supported by the device are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Single:</b> In single data stream, the data frames are transmitted in parallel over all the antennas. This stream is recommended for longer range.</li> <li>• <b>Dual:</b> In dual data stream, the data frames are distributed across the antennas and transmitted. This stream is recommended for higher throughput.</li> </ul> <p> : Data streams is not applicable when DDRS is enabled.</p>
<b>Antenna Status</b>	
Tx Antenna Status	<p>Allows the user to select the antenna(s) for data transmission. Select the checkbox against each antenna(s) for data transmission and click Ok.</p> <p> : Atleast two Tx antenna ports should be enabled when Data Stream is dual, or DDRS Stream Mode is set to auto or dual.</p>
Rx Antennas Status	<p>Allows the user to select the antenna(s) for receiving data. Select the checkbox against each antenna(s) for receiving data and click Ok.</p> <p> : Atleast two Rx antenna ports should be enabled when Data Stream is dual, or DDRS Stream Mode is set to auto or dual.</p>
<p> : Modifying the Guard Interval and Data Stream configuration values, will reset the Tx Rate to default value.</p>	

After configuring the required parameters, click **OK** and then **COMMIT**.

Reboot the device, if you have changed any of the MIMO parameters with asterisk (\*) symbol marked against them.

#### 5.4.4 Dynamic Frequency Selection (DFS)

The Tsunami® products support 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 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.



**DFS is not applicable in case of Tsunami® MP-8160-BSU, Tsunami® MP-8160-SUA and Tsunami® MP-8160-CPE devices.**

##### 5.4.4.1 DFS in BSU or End Point A mode

Explained below is the DFS functionality and the way it operates on a BSU or in End Point A devices.

1. Based on the selected frequency (regulatory) domain, DFS is automatically enabled on the device.
2. During bootup,
  - if ACS is disabled on the device, the device chooses the Preferred Channel to be the operational channel.



: By default, Automatic Channel Selection (ACS) is disabled on the BSU or a device in End Point A mode.

- if ACS is enabled, then the device scans all the channels and selects the channel with the best RSSI to be the operational channel.
3. Once the operating channel is selected, the device scans the channel for the presence of the RADAR for a duration of the configured Channel Wait Time (by default configured to 60 seconds). During this time, no transmission of data occurs.
  4. If no RADAR is detected, the device starts operating in that channel.
  5. If RADAR is detected, the channel is blacklisted for 30 minutes. Now, ACS will scan all the non-blacklisted channels and select the channel with best RSSI. Upon choosing the best channel, the device again scans the selected channel for the presence of the RADAR for a duration of the configured Channel Wait Time. Again, during this time no transmission of data occurs.
  6. If no RADAR is detected, it operates in that channel else repeats step 5.
  7. While operating in a channel, the device continuously monitors for potential interference from a RADAR source (this is referred to as in-service monitoring). If RADAR is detected, then the device stops transmitting in that channel. The channel is added to the blacklisted channel list.
  8. A channel in the blacklisted listed can be purged once the Non Occupancy Period (NOP) has elapsed for that channel.



- When a channel is blacklisted, all its sub-channels that are part of the current channel bandwidth are also blacklisted.
- For Europe 5.8 GHz channel, once the device finds a RADAR free channel (after 60 seconds RADAR scan), it does not perform scan for the next 24 hours. This is not applicable when device is rebooted or a particular channel got blacklisted earlier.
- Even if the preferred channel is configured with a DFS channel manually, the SU will scan for the BSU/End PointA's channel and associates automatically.

#### 5.4.4.2 DFS in SU or End Point B Mode

Explained below is the DFS functionality and the way it operates on SU or End Point B.

1. When SU/End Point B has no WOPR link, it scans continuously all the channels in the configured Frequency Domain for the presence of BSU/End Point A. If suitable BSU/End Point A is found in any scanned channel, the SU or End Point B tries to establish WOPR link.
2. After selecting the suitable BSU/End Point A's channel,
  - If SU/End Point B DFS is disabled, then SU/End Point B tries to connect to BSU/End Point A.
  - If SU/End Point B DFS is enabled, the SU/End Point B scans the selected channel for the presence of the RADAR for a duration of the configured Channel Wait Time (by default configured to 60 seconds). During this time, if the SU/End Point B detects radar, the channel is blacklisted and it starts scanning on non-blacklisted channels for a BSU/End Point A as given in step 1. If no radar is detected, a connection will be established.
3. While WOPR link is present, the SU/End Point B continuously monitors the current active channel for potential interference from a RADAR source (this is referred to as in-service monitoring).
  - If RADAR is detected, the SU/End Point B sends a message to the BSU or End Point A indicating the RADAR detection on the active channel and blacklists that channel for Non Occupancy Period (NOP). The default NOP is 30 Minutes.
  - On receiving the RADAR detection message from SU/End Point B, the BSU/ End Point A blacklists the active channel and ACS starts scanning for an interference free channel.



: The BSU blacklist the channel only when the number of SUs reporting the RADAR equals or exceeds the configured **SUs Reporting RADAR** parameter.

4. A blacklisted channel can be purged once the Non Occupancy Period (NOP) has elapsed.



- On the SU/End Point B, if the preferred channel is configured with a DFS channel then SU will scan all the channels even if ACS is disabled.
- When a channel is blacklisted, all its sub-channels that are part of that channel bandwidth are also blacklisted.

For detailed information on DFS enabled countries, see [Frequency Domains and Channels](#).

To configure DFS parameters, navigate to **ADVANCED CONFIGURATION > Wireless > Interface 1 > DFS**. The **Dynamic Frequency Selection (DFS)** screen appears.

### Dynamic Frequency Selection ( DFS )

**DFS Configuration**
Manual Blacklist

Channel Wait Time  (0-3 0) Seconds

SUs Reporting RADAR  (0-250)

#### Blacklist Information

Note: Blacklist Table will not be updated with Manual Blacklist changes made after modification to rebootable parameters.

Channel Number	Reason	Time Elapsed (Seconds)
100 ( 5.5 GHz )	Remote Radar	0
101 ( 5.505 GHz )	Remote Radar	0
102 ( 5.51 GHz )	Unusable	0
103 ( 5.515 GHz )	Unusable	0
108 ( 5.54 GHz )	Unusable	0
109 ( 5.545 GHz )	Unusable	0
110 ( 5.55 GHz )	Manual	0
111 ( 5.555 GHz )	Manual	0
112 ( 5.56 GHz )	Manual	0
113 ( 5.565 GHz )	Manual	0
114 ( 5.57 GHz )	Manual	0
115 ( 5.575 GHz )	Unusable	0
116 ( 5.58 GHz )	Unusable	0

Figure 5-14 DFS Configuration (BSU Mode)

**Dynamic Frequency Selection ( DFS )**

**DFS Configuration**    Manual Blacklist

Channel Wait Time:  (0-3600) Seconds

DFS Status:

**Blacklist Information**

**Note: Blacklist Table will not be updated with Manual Blacklist changes made after modification to rebootable parameters.**

Channel Number	Reason	Time Elapsed (Seconds)
100 ( 5.5 GHz )	Local Radar	1
101 ( 5.505 GHz )	Local Radar	1
102 ( 5.51 GHz )	Unusable	1
103 ( 5.515 GHz )	Unusable	1

**Figure 5-15 DFS Configuration (SU/End Point B Mode)**

Tabulated below is the table which explains DFS parameters and the method to configure the configurable parameter(s):

Parameter	Description
Channel Wait Time	One the device selects the best channel, it scans that channel for the presence of RADAR for a period of set Channel Wait Time. The wait time can be configured in the range 0 to 3600 sec. By default, the wait time is set to <b>60 seconds</b> .
SUs Reporting RADAR	Applicable only to BSU.  When a SU detects a RADAR, it reports to BSU. The BSU will take a decision on whether to blacklist this channel based on <b>SUs Reporting RADAR</b> parameter. If the number of SU reporting RADAR equals or exceed the configured SUs Reporting RADAR parameter then BSU blacklists that channel. If SUs reporting the RADAR is less than this configured value then BSU continues to operate in the same channel. The range varies depending on the product license. By default, it is set to <b>0</b> .
DFS Status	Applicable only to SU or End Point B devices.  A SU or End Point B devices have the option to either enable or disable DFS. By default, DFS is disabled.

After configuring the required parameters, click **OK** and then **COMMIT**.

### 5.4.4.3 Blacklist Information

The blacklisted table displays all the channels that are blacklisted.

Parameter	Description
Channel Number	Indicates the channel that is blacklisted.
Reason	<p>Specifies the reason for blacklisting a channel.</p> <p>Following are the reasons for blacklisting a channel:</p> <ol style="list-style-type: none"> <li>1. <b>Remote Radar:</b> A SU/End Point B detects a RADAR and informs BSU/End Point A accordingly.</li> <li>2. <b>Local Radar:</b> The device detects the RADAR on its own.</li> <li>3. <b>Unusable:</b> For bandwidths more than 5 MHz, channels that are not usable because they fall in the frequency range of other radar/manual blacklisted channels. For example, if channel 110 is blacklisted, then channels 108, 109, 111, 112 will become unusable for 20 MHz bandwidth.</li> <li>4. <b>Manual:</b> A channel is manually blacklisted by the administrator.</li> </ol>
Time Elapsed	<p>The time elapsed since the channel was blacklisted due to radar. When the channel is blacklisted due to the presence of a radar, it will be de-blacklisted after 30 Minutes.</p> <p>This parameter is applicable for radar blacklisted channels only.</p>

Click **Refresh**, to view updated/refreshed blacklisted channels.

### 5.4.4.4 Manual Blacklist

This tab enables you to manually blacklist a channel.

However, there are few conditions to be followed while blacklisting channels:

- When ACS is disabled, the preferred channel and its sub-channels that are part of the current channel bandwidth cannot be manual blacklisted.
- When WOP link is UP, the active channel and its sub-channels that are part of the current channel bandwidth cannot be manual blacklisted.
- When DFS/ACS is enabled, atleast one channel and its sub-channels that are part of the current channel bandwidth should be available for operation. That is, all channels cannot be blacklisted.

To manual blacklist channels, click **Manual Blacklist** under **Dynamic Frequency Selection (DFS)** screen. The following screen appears:

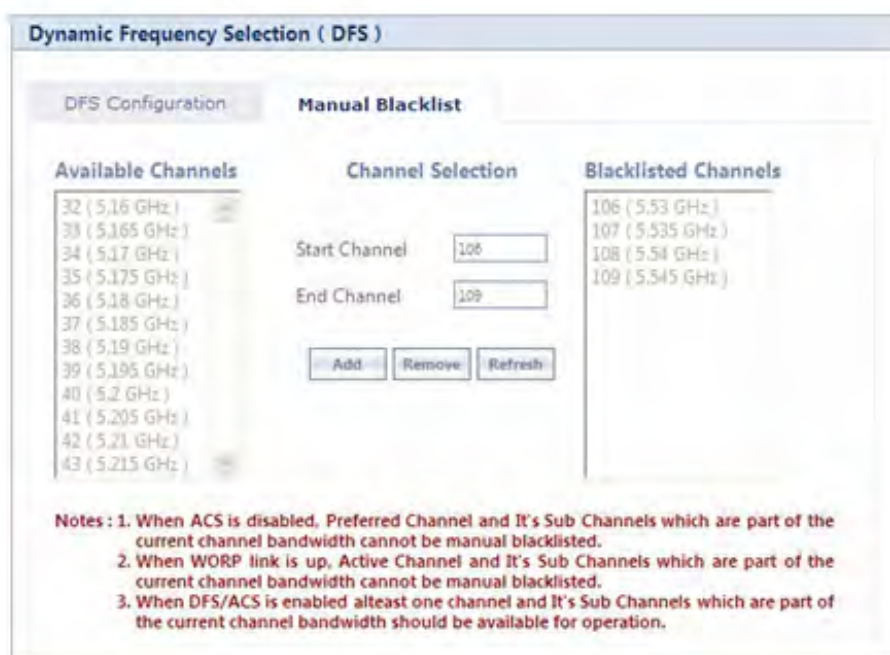


Figure 5-16 Manual Blacklist

Select the channels that you want to blacklist by entering the start and end channels in the Start Channel and End Channel boxes respectively.

Next, click **Add**. All the selected channels are added to the **Blacklisted Channels** table.

To remove any blacklisted channel, enter the Start and End Channel of the blacklisted channels and then click **Remove** button.

To refresh channel entries, click **Refresh**.

#### 5.4.5 DDRS

Dynamic Data Rate Selection (DDRS) feature adjusts the transmission data rate to an optimal value to provide the best possible throughput according to the current communication conditions and link quality.

The factors for adjusting the transmission data rate are,

1. Remote average Signal-to-noise (SNR) ratio
2. Number of retransmissions

DDRS can be configured separately on each device (BSU mode/ SU mode /End Point A mode/ End Point B mode).

##### 5.4.5.1 DDRS Configuration

To configure **DDRS** on the device, navigate to **ADVANCED CONFIGURATION > Wireless > Interface 1 > DDRS**. The **DDRS Configuration** screen appears:







Figure 5-17 Basic DDRS Configuration

The DDRS Configuration is classified under two categories, namely, **Basic** and **Advanced**.

### Basic Configuration

Under **Basic Configuration** screen, you can configure the following parameters.

Parameter	Description
DDRS Status	Enables the user the either enable or disabled DDRS feature on the device. By default, it is enabled on the device.
Stream Mode	<p>Select the stream mode as either <b>Auto</b>, <b>Single</b> or <b>Dual</b>. By default, the <b>Auto</b> mode is selected. Based on the selected stream modes, DDRS dynamically chooses the data rate.</p> <ul style="list-style-type: none"> <li>• <b>Dual</b>: Select <b>Dual</b>, for higher throughput.</li> <li>• <b>Single</b>: Select <b>Single</b>, for reliability and longer range.</li> <li>• <b>Auto</b>: When configured to <b>Auto</b>, DDRS decides on the stream modes based on the environment conditions.</li> </ul> <p> : Stream Mode is not valid in legacy mode.</p>
Maximum Rate	<p>Represents the maximum data rate that DDRS can dynamically choose to provide the best possible throughput. The default value depends on the channel bandwidth and the number of streams.</p> <p> : A change in Frequency Domain, Channel Bandwidth, Guard Interval and Data Stream will reset maximum data rate to defaults.</p>

After configuring the required parameters, click **OK** and then **COMMIT**.

### Advanced Configuration

To view **Advanced Configuration** parameters, click **Advanced** tab in the **DDRS Configuration** screen. The following screen appears depending on your device:

### DDRS Configuration

Basic
**Advanced**

Minimum Rate	6.5 Mbps
Maximum Rate	130 Mbps
Lower SNR Correction	0 dB
Upper SNR Correction	3 dB
Rate Increment RTX Threshold	25 %
Rate Decrement RTX Threshold	30 %
Chain Balance Threshold	15 dB
Rate BackOff Interval	300 secs


Click here to view the [Local SNR-Table](#)

Note: DDRS algorithm considers minimum required SNR configured, lower/upper SNR corrections and Tx power for computing actual minimum required SNR

Figure 5-18 Advanced DDRS Configuration

The following table lists the **Advanced Configuration** parameters and their description. Note that these parameters are read-only and can be configured only through CLI or SNMP.

Parameter	Description
Minimum Rate and Maximum Rate	Represents the minimum and maximum data rate between which the DDRS dynamically selects the transmission data rate. These varies depending on the configured Data Streams, Channel Bandwidth and Guard Interval.
Lower SNR Correction	Represents the margin value to be added to the Minimum Required SNR, for the purpose of removing the data rate from the valid data rate table. Doing so, avoids Hysteresis in the dynamic data rate.  By default, it is configured to <b>10 dB</b> .
Upper SNR Correction	Represents the margin value to be added to the Minimum Required SNR, for the purpose of adding the data rate to the valid data rate table. Doing so, avoids Hysteresis in the dynamic data rate.  By default, it is set to <b>3 dB</b> .
Rate Increment RTX Threshold	Represents a threshold for the percentage of retransmissions, below which the rate can be increased. By default, it is set to <b>25%</b> .  <div style="display: flex; align-items: flex-start;"> <div style="font-size: small;">: If the percentage of retransmissions is between “Rate Increment RTX Threshold” and “Rate Decrement RTX Threshold” then the current operation rate is maintained.</div> </div>

Rate Decrement RTX Threshold	Represents a threshold for percentage of retransmissions, above which the rate can be decreased. By default, it is set to <b>30%</b> . Please note that if the percentage of retransmissions is between “Rate Increment RTX Threshold” and “Rate Decrement RTX Threshold” then the current operation rate is maintained.
Chain Balance Threshold	<p>In the case of MIMO, the difference in SNR between two chains must be less than or equal to this threshold for the chains to be considered as “Balanced”. By default, it is set to <b>15 dB</b>.</p>  <ul style="list-style-type: none"> <li>• This parameter is applicable only for “Auto” stream mode.</li> <li>• When “Auto” stream mode is configured and if chains are not balanced, then Single Stream rates are considered.</li> </ul>
Rate Back Off Interval	The DDRS algorithm constantly attempts higher data rates, when the current rate is stable. If not successful, it goes back to older stable rate. Before the next attempt, it waits for a minimum duration. This duration starts with 10 seconds and increases exponentially up to <b>Rate Back Off Interval</b> and remains at this value. By default, it is set to <b>300 seconds</b> .

Click **Local SNR-Table**, to view the optimal SNR values that are exchanged with the peer for optimal throughput.

Local SNR Information								
Wireless 1								
S.No.	MCS Index	Modulation	Number of Streams	Data Rate (Mbps)	Minimum Required SNR (dB)		Maximum Optimal SNR (dB)	
					Default	Configured	Default	Configured
1	MCS0	BPSK(1/2)	Single	6.5	6	6	86	86
2	MCS1	QPSK(1/2)	Single	13.0	9	9	86	86
3	MCS2	QPSK(3/4)	Single	19.5	11	11	84	84
4	MCS3	16QAM(1/2)	Single	26.0	14	14	82	82
5	MCS4	16QAM(3/4)	Single	39.0	18	18	80	80
6	MCS5	64QAM(2/3)	Single	52.0	22	22	78	78
7	MCS6	64QAM(3/4)	Single	58.5	25	25	77	77
8	MCS7	64QAM(5/6)	Single	65.0	28	28	77	77
9	MCS8	BPSK(1/2)	Dual	13.0	9	9	86	86
10	MCS9	QPSK(1/2)	Dual	26.0	12	12	84	84
11	MCS10	QPSK(3/4)	Dual	39.0	14	14	82	82
12	MCS11	16QAM(1/2)	Dual	52.0	16	16	80	80
13	MCS12	16QAM(3/4)	Dual	78.0	20	20	78	78
14	MCS13	64QAM(2/3)	Dual	104.0	26	26	78	78
15	MCS14	64QAM(3/4)	Dual	117.0	29	29	77	77
16	MCS15	64QAM(5/6)	Dual	130.0	30	30	76	76

Notes: 1. Remote device uses configured minimum required SNR values when it is enabled with DDRS feature.  
2. Remote device uses configured maximum optimal SNR values when it is enabled with ATPC feature.

Close

Figure 5-19 An Example - SNR Information

These SNR values vary depending on your device. For device specific SNR information, see [SNR Information](#).

## 5.5 Security

### 5.5.1 Wireless Security

The **Wireless Security** feature helps to configure security mechanisms to secure the communication link between a BSU and a SU, and a link between End Point A and End Point B. By default, a security profile (**WORP Security**) is preconfigured with the default configuration for WORP security. Altogether, device allows to create 8 security profiles as required. Even though 8 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. Refer to [Wireless Outdoor Router Protocol \(WORP\)](#) for more details.



: Configure the same security profile on the either ends to establish a connection.

To configure the Wireless security profile, navigate to **ADVANCED CONFIGURATION > Security > Wireless Security**. The **Wireless Security Configuration** screen appears:

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

OK Add

**Figure 5-20 Wireless Security Configuration**

Tabulated below is the table which explains Wireless Security parameters:

Parameter	Description
Profile Name	Specifies the security profile name. By default, it is <b>WDRP Security</b> .
Entry status	Enables a user to either <b>Enable</b> or <b>Disable</b> the security profile on the device. By default, it is enabled.
Edit	Enables you to edit the existing security profiles. Click <b>Edit</b> to modify any of the security profile parameters.

After configuring the required parameters, click **OK** and then **COMMIT**.

#### 5.5.1.1 Creating a New Security Profile

To create a new security profile, click **Add** in the **Wireless Security Configuration** screen. The following **Wireless Security Add Row** screen appears:

Profile Name: WDRP Security

Encryption Type: AES-CCM

Key: \*\*\*\*\*

Entry Status: Enable


Network Secret: \*\*\*\*\* (6-32)

Notes : 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. WEP and TKIP are applicable to legacy operational mode only.  
 4. For setting the Network Secret characters - = " ' ? \ / space are not allowed.

Add Back

**Figure 5-21 Creating a New Security Profile**

Tabulated below is the table which explains the method to create a new Security Profile:

Parameter	Description
Profile Name	A name to uniquely identify a security profile name.
Encryption Type	<p>Select encryption type as either <b>None</b>, <b>WEP</b>, <b>TKIP</b> or <b>AES-CCM</b>.</p> <ol style="list-style-type: none"> <li><b>None</b> - If the encryption type is selected as None, then there exist no security to the data frames transmitted over the wireless medium.</li> <li><b>WEP (Wired Equivalent Privacy)</b> - Represents the <b>WEP</b> 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. <ul style="list-style-type: none"> <li><b>Key1 / Key 2 / Key 3 / key 4:</b> You can configure a maximum of four WEP keys. Enter 5/13/16 ASCII Characters or 10/26/32 Hexadecimal digits for WEP keys.</li> <li><b>Transmit Key:</b> Select one out of the four keys described above as the default transmit key, which is used for encrypting and transmitting the data.</li> </ul> </li> <li><b>TKIP</b> - Represents the <b>TKIP</b> 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. <ul style="list-style-type: none"> <li><b>Key1 / Key 2 / Key 3 / key 4:</b> You can configure a maximum of four TKIP keys. Enter 16 ASCII Characters or 32 Hexadecimal digits.</li> <li><b>Transmit Key:</b> Select one out of the four keys described above as the default transmit key, which is used for encrypting and transmitting the data.</li> </ul> </li> <li><b>AES-CCM</b> - Represents CCM Protocol with AES Cipher restricted to 128 bits. <ul style="list-style-type: none"> <li><b>Key:</b> Enter 16 ASCII Characters or 32 Hex Digits for AES-CCM encryption keys.</li> </ul> </li> </ol>
Entry status	Enables a user to either <b>Enable</b> or <b>Disable</b> the security profile on the device. By default, it is enabled.
Network Secret	Enter the WOPR Protocol Secret Key, ranging from 6 to 32 characters, used for authenticating a SU with a BSU, and an End Point B with End Point A. The network secret should be same for a BSU and SU. Similarly, the network secret should be same for an End Point A and an End Point B.
	 <ul style="list-style-type: none"> <li>A maximum of 8 security profiles can be created.</li> <li>A Quick Bridge support <b>AES-CCM</b> encryption type only.</li> <li>Special characters like - = \ " ' ? / space are not allowed while configuring the keys.</li> <li>All four Keys (Key1, Key2, Key3, Key4) must be of same length and same type, that is, all four Keys must be either ASCII Characters or Hexadecimal digits.</li> <li>Transmit Key can be any one of the four keys, provided all the four keys are same in a SU and BSU, or End Point devices.</li> <li>WEP and TKIP Encryption Types are supported only in legacy Modes.</li> <li>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.</li> </ul>

After configuring the required parameters, click **Add** and then **COMMIT**.

## Sample Security Profile Configuration

	End Point A	End Point B
<b>Profile Name</b>	WORP Security	WORP Security
<b>Encryption Type</b>	AES-CCM	AES-CCM
<b>Key</b>	1234567890abcdef1234567890abcdef (32 Hexadecimal digits) or publicpublic1234 (16 ASCII Characters)	1234567890abcdef1234567890abcdef (32 Hexadecimal digits) or publicpublic1234 (16 ASCII Characters)
<b>Entry Status</b>	Enable	Enable
<b>Network Secret</b>	public	public

## 5.5.1.2 Editing an existing Security Profile

To edit the parameters of the existing security profiles, click **Edit**  icon in the **Wireless Security Configuration** screen. The **Wireless Security Edit Row** screen appears:



**Wireless Security Edit Row**

Profile Name:

Encryption Type:

Key:

Entry Status:

Network Secret:  (6-32)

Notes : 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. WEP and TKIP are applicable to legacy operational mode only.  
 4. For setting the Network Secret characters - = " ' ? \ / space are not allowed.

Figure 5-22 Wireless Security Edit Row

Edit the required parameters and click **OK** and then **COMMIT**.

## 5.5.2 RADIUS



:Applicable only to a BSU and End Point A devices.

The **RADIUS** tab allows you to configure a RADIUS authentication server on a BSU/End Point A that remotely authenticates a SU or an End Point B while registering with a BSU or an End Point A respectively. These servers are also used to configure few features (VLAN and QoS) on a SU.

A RADIUS server profile consists of a Primary and a Secondary RADIUS server that can act as Authentication servers. Configuration of Secondary Authentication Server is optional. The RADIUS server is applicable only when it is enabled in the **WORP Configuration** page.

To configure the RADIUS Server profile, navigate to **ADVANCED CONFIGURATION > Security > RADIUS**. The following **RADIUS Server Profile** screen appears:

**Figure 5-23 Configuring RADIUS Server Profile**

Tabulated below is the table which explains RADIUS Server parameters and the method to configure the configurable parameter(s):

Parameter	Description
Profile Name	A name that represents the Radius Server profile. By default, it is <b>Default Radius</b> .
Max Retransmissions	Represents the maximum number of times an authentication request may be retransmitted to the configured RADIUS server. The range is 0 to 3. By default, it is set to 3.
Message Response Time	Represents the response time (in seconds) for which that the BSU/End Point A should wait for the RADIUS server to respond to a request. The range is 3 to 9 seconds. By default, it is set to 3 seconds.
Re Authentication Period	Represents the time period after which the RADIUS server should re-authenticate a SU or an End Point B. The re-authenticate period ranges from 900 to 65535 seconds. By default, the re-authentication period is set to 0.
Entry status	A read-only parameter which displays the status of the RADIUS server profile as <b>Enabled</b> . The Entry status cannot be disabled or edited.
Server Type	For better accessibility and reliability, you can configure two RADIUS servers: <ol style="list-style-type: none"> <li>1. Primary RADIUS Server</li> <li>2. Secondary RADIUS Server</li> </ol> <p>The secondary RADIUS server serves as backup when the primary RADIUS server is down or not reachable.</p>
IP Address	Represents the IP address of the primary and secondary RADIUS servers.



Parameter	Description
Server Port	Specifies the port number that is used by the BSU/End Point A and the RADIUS server to communicate. By default, RADIUS Authentication Server communicates on port <b>1812</b> .
Shared Secret	Specifies the password shared by the BSU/End Point A and the RADIUS server to communicate. The default password is <b>public</b> .  Care should be taken to configure same Shared Secret on both BSU/End Point A and RADIUS Server, otherwise no communication is possible between BSU/End Point A and RADIUS server.
Entry Status	You can either enable or disable the configured RADIUS servers. By default, the Primary RADIUS server is enabled and the secondary RADIUS server is disabled.

After configuring the required parameters, click **OK** and then **COMMIT**.

Listed below are the points to be noted before configuring the Radius Server Profile,

1. **Message Response Time** should always be less than **WORP Registration Timeout**.
2. If **Max Retransmissions** is configured as **Zero**, then retransmissions does not occur.
3. The value of **Max Retransmissions** multiplied by **Message Response Time** should be less than **WORP Registration Timeout** value.

### 5.5.3 MAC ACL



:Applicable only to a BSU and End Point A mode.

The **MAC ACL** feature allows only the authenticated SUs/End Point Bs to access the wireless network. Please note that MAC Authentication is supported only on the wireless interface. The MAC ACL feature is applicable only when it is enabled in the **WORP Configuration** page.

To configure the MAC Access Control List, navigate to **ADVANCED CONFIGURATION > Security > MAC ACL**. The **MAC Access Control** screen appears:

S.No.	MAC Address	Comment	Entry Status
1	00-11-22-33-44-55	MAC ACL	Enable

**Figure 5-24 MAC Access Control Configuration**

Select the Operation Type as either **Allow** or **Deny**.

- **Allow**: Allows only the SUs/End Point Bs configured in the MAC Access Control Table to access the wireless network.

- **Deny:** Does not allow the SUs/End Point B devices configured in the MAC Access Control Table to access the wireless network.

Click **OK**, if you have changed the Operation Type parameters.

### 5.5.3.1 Add SUs/End Point B to MAC Access Control Table

To add entries to **MAC Access Control** table, click **Add** in the **MAC Access Control** screen. The **MAC ACL Add Row** screen appears:

Figure 5-25 MAC ACL Add Row

1. Type the **MAC Address** of the SU/End Point B.
2. Add comments, if any.
3. Select the Entry Status as either **Enable** or **Disable**.
4. Next, click **Add**.



- The maximum number of SUs/End Point Bs that can be added to the MAC ACL table is 250.
- Either RADIUS MAC or Local MAC can be enabled at one time.

### 5.5.3.2 Edit the existing SUs/End Point B from MAC Access Control Table

To edit the existing SUs/End Point B from MAC Access Control Table, edit parameters from the MAC Access Control Table in **MAC Access Control** screen and click **OK**.

## 5.6 Quality of Service (QoS)

The Quality of Service (QoS) feature is based on the 802.16 standard and defines the classes, service flows, and packet identification rules for specific types of traffic. The main priority of QoS is to guarantee a reliable and adequate transmission quality for all types of traffic under conditions of high congestion and bandwidth over-subscription.

There are already several pre-defined QoS classes, SFCs and PIRs available that you may choose from which cover the most common types of traffic. If you want to configure something else, you start building the hierarchy of a QoS class by defining PIRs; you define the QoS class by associating those PIRs to relevant SFCs with priorities to each PIR within each SFC. QoS can be applied on standard 802.3 ethernet frames as well as PPPoE encapsulated frames.

### 5.6.1 QoS Concepts and Definitions

QoS feature is applicable for BSU or End Point A only. You may define different classes of service on a BSU or End Point A that can then be assigned to the SU or End Point B that is associated, or that may get associated, with that BSU or End Point A.

You can create, edit, and delete classes of service that are specified below in the following hierarchy of parameters:

- **Packet Identification Rule (PIR)** - up to 64 rules, including 18 predefined rules
- **Service Flow class (SFC)** - up to 32 SFCs, including 8 predefined SFCs; up to 8 PIRs may be associated per SFC
- **Class List** - Priority for each rule within each SF class - 0 to 255, with 0 being lowest priority
- **QoS class** - up to 8 QoS classes, including 5 predefined classes; up to 8 SFCs may be associated per QoS class

### 5.6.1.1 Packet Identification Rule (PIR)

A Packet Identification Rule is a combination of parameters that specifies what type of traffic is allowed or not allowed. You can create a maximum of 64 different PIRs, including 18 predefined PIRs. Also, you can create, edit, and delete PIRs that contain none, one, or more of the following classification fields:

- Rule Name
- IP ToS (Layer 3 QoS identification)
- 802.1p tag (layer 2 QoS identification)
- IP Protocol List containing up to 4 IP protocols
- VLAN ID
- PPPoE Encapsulation
- Ether Type (Ethernet Protocol identification)
- Up to 4 TCP/UDP Source port ranges
- Up to 4 TCP/UDP Destination port ranges
- Up to 4 pairs of Source IP address + Mask
- Up to 4 pairs of Destination IP address + Mask
- Up to 4 source MAC addresses + Mask
- Up to 4 destination MAC addresses + Mask



: IP Address, TCP/UDP Port, MAC Address need to be configured separately and associate those classification in PIR details if required.

A good example is provided by the 18 predefined PIRs. Note that these rules help identify specific traffic types:

1. All - No classification fields, all traffic matches
2. L2 Multicast
  - a. Ethernet Destination (dest = 0x010000000000, mask = 0x010000000000)
3. L2 Broadcast
  - a. Ethernet Destination (dest = 0xffffffff, mask = 0xffffffff)
4. Cisco VoIP UL
  - a. TCP/UDP Source Port Range (16,000-33,000)
  - b. IP Protocol List (17 = UDP)
5. Vonage VoIP UL
  - a. TCP/UDP Source Port Range (5060-5061, 10000-20000)
  - b. IP Protocol List (17 = UDP)
6. Cisco VoIP DL
  - a. TCP/UDP Destination Port Range (16,000-33,000)
  - b. IP Protocol List (17 = UDP)
7. Vonage VoIP DL
  - a. TCP/UDP Destination Port Range (5060-5061, 10000-20000)

- b. IP Protocol List (17 = UDP)
- 8. TCP
  - a. IP Protocol List (6)
- 9. UDP
  - a. IP Protocol List (17)
- 10. PPPoE Control
  - a. Ether Type Rule (Ether Type = DIX-Snap, Ether Value = 0x8863)
- 11. PPPoE Data
  - a. Ether Type Rule (Ether Type = DIX-Snap, Ether Value = 0x8864)
- 12. IP
  - a. Ether Type Rule (Ether Type = DIX-Snap, Ether Value = 0x0800)
- 13. ARP
  - a. Ether Type Rule (Ether Type = DIX-Snap, Ether Value = 0x0806)
- 14. Expedited Forwarding
  - a. IP TOS/DSCP (ToS low=45(0x2D), ToS high=45(0x2D), ToS mask = 63(0x3F))
- 15. Streaming Video (IP/TV)
  - a. IP TOS/DSCP (ToS low=13(0x0D), ToS high=13(0x0D), ToS mask = 63(0x3F))
- 16. 802.1p BE
  - a. Ethernet Priority (low=0, high=0) (this is the equivalent of the User Priority value in the TCI (Tag Control Information) field of a VLAN tag)
- 17. 802.1p Voice
  - a. Ethernet Priority (ToS low=6, ToS high=6) (this is the equivalent of the User Priority value in the TCI (Tag Control Information) field of a VLAN tag)
- 18. 802.1p Video
  - a. Ethernet Priority (ToS low=5, ToS high=5) (this is the equivalent of the User Priority value in the TCI (Tag Control Information) field of a VLAN tag)



: Two different VoIP rule names have been defined for each direction of traffic, Uplink (UL) and Downlink (DL), (index numbers 4 to 7). This has been done to distinguish the proprietary nature of the Cisco VoIP implementation as opposed to the more standard Session Initiation Protocol (SIP) signaling found, for example, in the Vonage-type VoIP service.

### 5.6.1.2 Service Flow Class (SFC)

A Service Flow class defines a set of parameters that determines how a stream of application data that matches a certain classification profile will be handled. You can create up to 32 different SFCs, including 8 predefined SFCs. Also, you can create, edit, and delete SFCs that contain the following parameters and values:

- Service flow name
- Scheduling type - Best Effort (BE); Real-Time Polling Service (RTPS)
- Service Flow Direction - Downlink (DL: traffic from End Point ABSU to End Point BSU); Uplink (UL: traffic from SU/End Point B to BSU/End Point A)
- Maximum sustained data rate (or Maximum Information Rate (MIR) - specified in units of 1 Kbps from 8 Kbps up to the maximum rate specified in the license.
- Minimum reserved traffic rate (or Committed Information Rate (CIR) - specified in units of 1 Kbps from 0 Kbps up to the maximum rate specified in the license.
- Maximum Latency - specified in increments of 1 ms steps from a minimum of 5 ms up to a maximum of 100 ms

- Tolerable Jitter - specified in increments of 1 ms steps from a minimum of 0 ms up to the Maximum Latency (in ms)
- Traffic priority - zero (0) to seven (7), 0 being the lowest, 7 being the highest
- Maximum number of data messages in a burst - one (1) to sixteen (16), which affects the percentage of the maximum throughput of the system
- Entry Status - Enable, Disable, and Delete



: Note that traffic priority refers to the prioritization of this specific Service Flow.

The device tries to deliver the packets within the specified latency and jitter requirements, relative to the moment of receiving the packets in the device. For delay-sensitive traffic, the jitter must be equal to or less than the latency. A packet is buffered until an interval of time equal to the difference between Latency and jitter (Latency - Jitter) has elapsed. The device will attempt to deliver the packet within a time window starting at (Latency - Jitter) until the maximum Latency time is reached. If the SFC's scheduling type is real-time polling (RTPS), and the packet is not delivered by that time, it will be discarded. This can lead to loss of packets without reaching the maximum throughput of the wireless link. For example, when the packets arrive in bursts on the Ethernet interface and the wireless interface is momentarily maxed out, then the packets at the "end" of the burst may be timed out before they can be sent.

Users can set up their own traffic characteristics (MIR, CIR, latency, jitter, etc.) per service flow class to meet their unique requirements. A good example is provided by the 8 predefined SFCs:

1. UL-Unlimited BE
  - a. Scheduling Type = Best Effort
  - b. Service Flow Direction = Uplink
  - c. Entry Status = Enable
  - d. Maximum Sustained Data Rate = 102400 Mbps e. Traffic Priority = 0
2. DL-Unlimited BE (same as UL-Unlimited BE, except Service Flow Direction = Downlink)
3. DL-L2 Broadcast BE (same as UL-Unlimited BE, except Service Flow Direction = Downlink)
4. UL-G711 20 ms VoIP RTPS
  - a. Schedule type = RTPS (Real time Polling Service)
  - b. Service Flow Direction = Uplink
  - c. Entry Status = Enable
  - d. Maximum Sustained Data Rate = 88 Kbps
  - e. Minimum Reserved Traffic Rate = 88 Kbps
  - f. Maximum Latency = 20 milliseconds g. Traffic Priority = 1
5. DL-G711 20 ms VoIP rtPS (same as UL-G711 20ms VoIP rtPS, except Service Flow Direction = Downlink)
6. UL-G729 20 ms VoIP rtPS (same as UL-G711 20ms VoIP rtPS, except Maximum Sustained Data Rate and Committed Information rate = 66 Kbps)
7. DL-G729 20 ms VoIP rtPS (same as UL-G729 20ms VoIP rtPS, except Service Flow Direction = Downlink)
8. DL-2Mbps Video
  - a. Schedule type = Real time Polling
  - b. Service Flow Direction = Downlink
  - c. Initialization State = Active
  - d. Maximum Sustained Data Rate = 2 Mbps
  - e. Minimum Reserved Traffic Rate = 2 Mbps
  - f. Maximum Latency = 20 milliseconds
  - g. Traffic Priority = 1

Note that two different VoIP Service Flow classes for each direction of traffic have been defined (index numbers 4 to 7) which follow the ITU-T standard nomenclatures: G.711 refers to a type of audio companding and encoding that produces a 64 Kbps bitstream, suitable for all types of audio signals. G.729 is appropriate for voice and VoIP applications, but cannot transport music or fax tones reliably. This type of companding and encoding produces a bitstream between 6.4 and 11.8 Kbps (typically 8 Kbps) according to the quality of voice transport that is desired.

### 5.6.1.3 QoS Class

A QoS class is defined by a set of parameters that includes the PIRs and SFCs that were previously configured. You can create up to eight different QoS classes, including five predefined QoS classes. Up to eight SF classes can be associated to each QoS class, and up to eight PIRs can be associated to each SF class. For example, a QoS class called “G711 VoIP” may include the following SFCs: “UL-G711 20 ms VoIP rtPS” and “DL-G711 20 ms VoIP rtPS”.

In turn, the SFC named “UL-G711 20 ms VoIP rtPS” may include the following rules: “Cisco VoIP UL” and “Vonage VoIP UL”. You can create, edit, and delete QoS classes that contain the following parameters:

- QoS class name
- Service Flow (SF) class name list per QoS class (up to eight SF classes can be associated to each QoS class)
- Packet Identification Rule (PIR) list per SF class (up to eight PIRs can be associated to each SF class)
- Priority per rule which defines the order of execution of PIRs during packet identification process. The PIR priority is a number in the range 0-255, with priority 255 being executed first, and priority 0 being executed last. The PIR priority is defined within a QoS class and can be different for the same PIR in some other QoS class. If all PIRs within one QoS class have the same priority, the order of execution of PIR rules will be defined by the order of definition of SFCs, and by the order of definition of PIRs in each SFC, within that QoS class.

A good example of this hierarchy is provided by the five predefined QoS classes:

1. Unlimited Best Effort
  - a. SF class: UL-Unlimited BE
    - PIR: All; PIR Priority: 0
  - b. SF class: DL-Unlimited BE
    - PIR: All; PIR Priority: 0
2. L2 Broadcast Best Effort
  - a. SF class: DL-L2 Broadcast BE
    - PIR: L2 Broadcast; PIR Priority: 0
3. G711 VoIP
  - a. SF class: UL-G711 20 ms VoIP rtPS
    - PIR: Vonage VoIP UL; PIR Priority: 1
    - PIR: Cisco VoIP UL; PIR Priority: 1
  - b. SF class: DL-G711 20 ms VoIP rtPS
    - PIR: Vonage VoIP DL; PIR Priority: 1
    - PIR: Cisco VoIP DL; PIR Priority: 1
4. G729 VoIP
  - a. SF class: UL-G729 20 ms VoIP rtPS
    - PIR: Vonage VoIP UL; PIR Priority: 1
    - PIR: Cisco VoIP UL; PIR Priority: 1
  - b. SF class: DL-G729 20 ms VoIP rtPS
    - PIR: Vonage VoIP DL; PIR Priority: 1
    - PIR: Cisco VoIP DL; PIR Priority: 1
5. 2Mbps Video

- a. SF class: DL-2Mbps Video
  - PIR: Streaming Video (IP/TV); PIR Priority: 1

## 5.6.2 QoS Configuration

There are several pre-defined QoS classes, SFCs, and PIRs available that cover the most common types of traffic. If you want to configure something else, build the hierarchy of a QoS class as follows:

1. Define PIR MAC Address, IP Address and TCP/UDP Port Entries.
2. Define PIRs and specify packet classification rules, associate MAC Address/IP Address/TCP-UDP Port Entries if required.
3. Define SFCs
4. Define QoS Class by associating PIRs with relevant SFC.
5. Assign priorities to each PIR within each SFC.

For detailed instructions on configuring a management station (a single station used for managing an entire network), refer to [QoS Configuration for a Management Station](#).

### QoS PIR MAC Address Configuration

1. Navigate to **ADVANCED CONFIGURATION > QoS > PIR List > MAC Address Entries**, the **QoS PIR MAC Address Entries screen** appears:
2. Three predefined MAC Address entries are displayed in this page. You can configure a maximum of 256 entries. MAC Address and Mask combination should be unique. This MAC Address entry can be referred in the PIR Rule's Source or Destination MAC Address Classification. MAC Entry referred by any PIR rule cannot be deleted.

S.No.	MAC Address	Mask	Comment	Entry Status
1	00:00:00:00:00:00	00:00:00:00:00:00	All	Enable
2	01:00:00:00:00:00	01:00:00:00:00:00	L2 Multicast	Enable
3	ff:ff:ff:ff:ff:ff	ff:ff:ff:ff:ff:ff	L2 Broadcast	Enable

**Notes :**

1. Maximum 256 Entries are allowed.
2. MAC Address & Mask combination should be unique
3. MAC Address Entry referred by any PIR rule can not be deleted.

OK Add

Figure 5-26 QoS PIR MAC Address Entries

3. Click **OK**.

To Add a New PIR MAC Address Entry,

- a. Navigate to **ADVANCED CONFIGURATION > QoS > PIR List > MAC Address Entries**, the **QoS PIR MAC Address Entries screen** appears.
- b. Click **Add** on the **QoS PIR MAC Address Entries screen** to add a new entry. The following screen appears for configuring the MAC Entry Details.

Figure 5-27 QoS PIR MAC Address Add Entry

- c. Provide the MAC Address, Mask, Comment, Entry Status details and click **Add**. Comment field can be used to identify when this particular entry is referred in PIR Rule/QoS Class.

The bit that is enabled in the “MAC Mask” configuration, the corresponding bit’s value in the “MAC Address” configuration should match with the same bit of the incoming traffic’s MAC Address (other bits of the incoming traffic are ignored). Then it is considered as matching traffic and the rest are unmatched traffic. The following is explained with the help of an example:

#### 1. Creating Matching profile for single MAC address

To apply QoS classification for traffic which is originated / destined from / to a Device only. **MAC**

**Address:** 00:20:A6:00:00:01

**MAC Mask:** FF:FF:FF:FF:FF:FF

In this example, all bits in the MAC Mask are enabled, so incoming traffic’s MAC address should exactly match with specified configured MAC Address (that is, 00:20:A6:00:00:01). Other traffics are considered as non-matching traffic.

#### 2. Creating Matching profile for all MAC Address

MAC Address: 00:00:00:00:00:00

MAC Mask: 00:00:00:00:00:00

In this example, all bits in the MAC Mask are disabled, so any traffic is considered as matching traffic.

#### 3. Creating Matching Profile for Broadcast MAC Address

MAC Address: FF:FF:FF:FF:FF:FF

MAC Mask: FF:FF:FF:FF:FF:FF

#### 4. Creating Matching Profile for all Multicast MAC Address

MAC Address: 01:00:00:00:00:00

MAC Mask: 01:00:00:00:00:00

#### 5. Creating Matching Profile for range of MAC Address (00:20:A6:00:00:01 to 00:20:A6:00:00:FF)

MAC Address: 00:20:A6:00:00:00

MAC Mask: FF:FF:FF:FF:FF:00

### QoS PIR IP Address Configuration

1. Navigate to **ADVANCED CONFIGURATION > QoS > PIR List > IP Address Entries**, the **QoS PIR IP Address Entries** screen appears. A single predefined IP Address entry is displayed. You can configure a maximum of 256 entries. IP Address, Subnet Mask combination should be unique. This IP Address entry can be referred in the PIR Rule’s Source or Destination IP Address Classification. IP Address Entry referred by any PIR rule cannot be deleted.
2. Click **OK**.



S.No.	IP Address	Subnet Mask	Comment	Entry Status
1	0.0.0.0	0.0.0.0	All	Enable

Notes : 1. Maximum 256 Entries are allowed.  
 2. IP Address & Subnet Mask combination should be unique.  
 3. IP Address Entry referred by any PIR rule can not be deleted.

OK Add

Figure 5-28 QoS PIR IP Address Entries

To Add a New PIR IP Address Entry,

- Navigate to **ADVANCED CONFIGURATION > QoS > PIR List > IP Address Entries**. The **QoS PIR IP Address Entries** screen appears
- Click **Add** on the **QoS PIR IP Address Entries** screen to add a new entry. The following screen appears for configuring the IP Address Entry Details.

QoS PIR IP Address Add Entry

IP Address: 10.0.0.3  
 Subnet Mask: 255.255.255.0  
 Comment: TEST\_CASE  
 Entry Status: Enable

Add Back

Figure 5-29 QoS PIR IP Address Add Entry

- Provide the IP Address, Subnet Mask, Comment, Entry Status details and click **Add**. Comment field can be used by the user to identify when this particular entry is referred in PIR Rule or QoS Class.

### QoS PIR TCP/UDP Port Configuration

- Navigate to **ADVANCED CONFIGURATION > QoS > PIR List > TCP/UDP Port Entries**. The **QoS PIR TCP/UDP Port Entries** screen appears. Three predefined TCP/UDP Port Entries are displayed. You can configure a maximum of 256 entries. Start Port, End Port combination should be unique. This TCP/UDP Port entry can be referred in the PIR Rule's Source or Destination TCP/UDP Port Classification. TCP/UDP Port Entry referred by any PIR rule can not be deleted.
- Click **OK**.

S.No.	Start Port	End Port	Comment	Entry Status
1	18000	33000	Cisco VOIP	Enable
2	5060	5061	Vonage VOIP-1	Enable
3	10000	20000	Vonage VOIP-2	Enable

Notes : 1. Maximum 256 Entries are allowed.  
 2. Start Port & End Port combination should be unique  
 3. TCP/UDP Port Entry referred by any PIR rule can not be deleted.

OK Add

Figure 5-30 QoS PIR TCP/UDP Port Entries

To Add a New PIR TCP/UDP Port Entry,

- Navigate to **ADVANCED CONFIGURATION > QoS > PIR List > TCP/UDP Port Entries**. The **QoS PIR TCP/UDP Port Entries** screen appears.
- Click **Add** on the **QoS PIR TCP/UDP Port Entries** screen to add a new entry. The following screen appears for configuring the IP Address entry details.

QoS PIR TCP/UDP Port Add Entry

Start Port: 50000  
 End Port: 60000  
 Comment: TEST\_CASE  
 Entry Status: Enable

Add Back

Figure 5-31 QoS PIR TCP/UDP Port Add Entry

- Provide the Start Port, End Port, Entry Status details and click **Add**. Comment field can be used to identify when this particular entry is referred in PIR Rule or QoS Class.

### 5.6.2.1 QoS PIR Configuration

- Navigate to **ADVANCED CONFIGURATION > QoS > PIR List**. The **QoS PIR Entries** screen appears. 18 predefined PIR Rules are displayed in this page. You can configure a maximum of 64 entries. PIR Rule Name should be unique. This PIR Rule can be referred in the QoS Class's Service Flow Details. PIR rule referred by any QoS Class cannot be deleted.
- Click **OK**.

QoS PIR Entries			
S.No.	PIR Name	Entry Status	Details
1	All	Enable	Details
2	L2 Multicast	Enable	Details
3	L2 Broadcast	Enable	Details
4	Cisco VoIP UL	Enable	Details
5	Vonage VoIP UL	Enable	Details
6	Cisco VoIP DL	Enable	Details
7	Vonage VoIP DL	Enable	Details
8	TCP	Enable	Details
9	UDP	Enable	Details
10	PPPoE Control	Enable	Details
11	PPPoE Data	Enable	Details
12	IP	Enable	Details
13	ARP	Enable	Details
14	Expedited Forwarding	Enable	Details
15	Streaming Video	Enable	Details
16	802.1p BE	Enable	Details
17	802.1p Voice	Enable	Details
18	802.1p Video	Enable	Details

**Notes :** 1. Maximum 64 Entries are allowed.  
 2. PIR Rule Name Should be Unique.  
 3. New PIR rule will be created without any PIR classification rules applied by default.  
 4. PIR Rule referred by any QoS Class can not be deleted.

OK Add

Figure 5-32 QoS PIR Entries

To Add a New PIR Rule,

- a. Navigate to **ADVANCED CONFIGURATION > QoS > PIR List**. The **QoS PIR Entries** screen appears.
- b. Click **Add** on the **QoS PIR Entries** screen to add a new entry. The following screen appears for configuring the New PIR Entry.

**QoS PIR Add Entry**

PIR Name

Entry Status

**Note: PIR Name should be unique.**

Add Back

Figure 5-33 QoS PIR Add Entry

c. Provide the PIR Name, Entry Status details and click **Add**.

### **PIR Rule Clarification Details**

1. Navigate to **ADVANCED CONFIGURATION > QoS > PIR List** and click **Details** for editing a particular PIR Rule.

**QoS PIR Edit Entry** [Back](#)

**PIR Entry Details**

Rule Name:

**Enable ToS Rule**

ToS Low:  (0-255)

ToS High:  (0-255)

ToS Mask:  (0-255)

**Enable Ether Priority Rule**

Priority Low:  (0-7)

Priority High:  (0-7)

**Enable VLAN Rule**

VLAN Id:  (1 - 4094)

PPPoE Encapsulation:

**Enable Ether Type Rule**

Ether Type:

PPPoE Protocol Id:

Ether Value:

Notes : 1. Ether Value is not valid when PPPoE Encapsulation is enabled.  
Similarly PPPoE Protocol ID is not valid when PPPoE Encapsulation is disabled.

**Protocol Id Entries**

S.No.	Protocol Id	Delete
1	17	<input type="button" value="Delete"/>

**TCP/UDP Source Port Entries**

S.No.	Start Port	End Port	Comment	Delete
1	16000	33000	Cisco VOIP	<input type="button" value="Delete"/>

**TCP/UDP Destination Port Entries**

S.No.	Start Port	End Port	Comment	Delete
-------	------------	----------	---------	--------

**Source IP Address Entries**

S.No.	IP Address	Sub Mask	Comment	Delete
-------	------------	----------	---------	--------

**Destination IP Address Entries**

S.No.	IP Address	Sub Mask	Comment	Delete
-------	------------	----------	---------	--------



**Source MAC Address Entries**

S.No.	MAC Address	Mask	Comment	Delete
-------	-------------	------	---------	--------

**Destination MAC Address Entries**

S.No.	MAC Address	Mask	Comment	Delete
-------	-------------	------	---------	--------

Figure 5-34 QoS PIR Edit Entry

Parameter	Description
Rule Name	This parameter specifies the Name of the Packet Identification Rule (PIR) and can have a length of 1-32 characters.
ToS Rule	This parameter is used to enable or disable a TOS rule. Enter the values for the following to specify the ToS-related configuration: <ul style="list-style-type: none"> <li>ToS Low</li> <li>ToS High</li> <li>ToS Mask</li> </ul>
Ether Priority Rule	This parameters is used to enable or disable 802.1p priority rule. Enter the values for the following to specify 802.1p priority configuration: <ul style="list-style-type: none"> <li>Priority Low</li> <li>Priority High</li> </ul>
VLAN Rule	This parameters allows to enable or disable VLAN rule. Enter the VLAN ID when the VLAN rule is enabled.
PPPoE Encapsulation	This parameter is used to classify PPPoE traffic.  <ul style="list-style-type: none"> <li>If you Enable/disable the PPPoE Configuration, it will automatically disable the Ether Type Rule. User can configure it again by enabling Ether Type Rule.</li> <li>When PPPoE Encapsulation is enabled, incoming packet will be checked again Ether value "0x8864" and look for PPPoE Protocol Id value "0x0021"(IP Protocol) by default. User can modify the PPPoE Protocol Id. All other classification rules which are specified in the PIR rule will work only if the PPPoE Protocol Id is "0021".</li> <li>Ether Value is not valid when PPPoE Encapsulation is enabled.</li> </ul>
Ether Type Rule	This parameters is used to enable or disable Ether Type rule. Enter the values for the following to specify the Ether Type rule related configuration: <ul style="list-style-type: none"> <li>Ether Type</li> <li>PPPoE Protocol Id</li> <li>Ether Value</li> </ul>  <ul style="list-style-type: none"> <li>PPPoE Protocol Id is not valid if PPPoE Encapsulation is disabled.</li> <li>Ether Value is not valid if PPPoE Encapsulation is enabled.</li> </ul>

### Adding Protocol ID

- Navigate to **ADVANCED CONFIGURATION > QoS > PIR List**. Click **Details**. The **Qos PIR Edit Entry** screen appears.
- Navigate to **Protocol Id Entries** tab and then click **Add** to add a new Protocol entry. The following screen appears.

Figure 5-35 QoS PIR Protocol ID

- c. Enter the details and click **Add**. For deleting an entry, click **Delete** for the corresponding entry in **PIR Details** screen.

### Adding TCP/UDP Source Port Numbers

- a. Navigate to **ADVANCED CONFIGURATION > QoS > PIR List**. Click **Details**. The **Qos PIR Edit Entry** screen appears.
- b. Navigate to **TCP/UDP Source Port Entries** tab and then click **Add** to add a new entry. The following screen appears.

Figure 5-36 QoS PIR TCP/UDP Source Port Add Entry

- c. All the Entries present in the **PIR TCP/UDP Port Entries** are displayed in the TCP/UDP Port Entry Table. Select the appropriate radio button and click **Add**. When an entry is added for the specific PIR, the entry gets displayed in the existing TCP/UDP Port Entries table. For deleting an entry, click **Delete** for the corresponding entry in the PIR Details page.

### Adding TCP/UDP Destination Port Numbers

- a. Navigate to **ADVANCED CONFIGURATION > QoS > PIR List**. Click **Details**. The **Qos PIR Edit Entry** screen appears.
- b. Navigate to **TCP/UDP Destination Port Entries** tab and then click **Add** to add a new entry. The following screen appears.

**QoS PIR TCP/UDP Destination Port Add Entry**

Note: Maximum 4 entries are allowed

New TCP/UDP Port Entry

S.No.	Start Port	End Port	Comment	Select
1	16000	33000	Cisco VOIP	<input type="radio"/>
2	5060	5061	Vonage VOIP-1	<input type="radio"/>
3	10000	20000	Vonage VOIP-2	<input type="radio"/>

Existing TCP/UDP Port Entries

S.No.	Start Port	End Port	Comment	Delete
2	5060	5061	Vonage VOIP-1	Delete

Figure 5-37 QoS PIR TCP/UDP Destination Port Add Entry

- c. All the entries present in the PIR TCP/UDP Port Entries are displayed in the TCP/UDP Port Entry Table. Select the appropriate radio button and click **Add**. When an entry is added for a specific PIR, it gets displayed in the existing TCP/UDP Port Entries table. For deleting an entry, click **Delete** for the corresponding entry in the PIR Details page.

#### Adding Source IP Address

- a. Navigate to **ADVANCED CONFIGURATION > QoS > PIR List**. Click **Details**. The **Qos PIR Edit Entry** screen appears.
- b. Navigate to **Source IP Address Entries** tab and then click **Add** to add a new entry. The following screen appears:

**QoS PIR Source IP Address Add Entry**

Note: Maximum 4 entries are allowed

New IP Address Entry

S.No.	IP Address	Subnet Mask	Comment	Select
1	0.0.0.0	0.0.0.0	All	<input type="radio"/>

Existing IP Address Entries

S.No.	IP Address	Subnet Mask	Comment	Delete
1	0.0.0.0	0.0.0.0	All	Delete

Figure 5-38 QoS PIR Source IP Address Add Entry

- c. All the entries present in the PIR IP Address Entries are displayed in the IP Address Entry Table. Select the appropriate radio button and click **Add**. After adding the entry for this specific PIR, it is displayed in the Existing IP Address Entries table. For deleting an entry, click **Delete** for the corresponding entry in the PIR Details page.

#### Adding Destination IP Address

- a. Navigate to **ADVANCED CONFIGURATION > QoS > PIR List**. Click **Details**. The **Qos PIR Edit Entry** screen appears.



- b. Navigate to **Destination IP Address Entries** tab and then click **Add** to add a new entry. The following screen appears.

S.No.	IP Address	Subnet Mask	Comment	Select
1	0.0.0.0	0.0.0.0	All	<input type="radio"/>

S.No.	IP Address	Subnet Mask	Comment	Delete
1	0.0.0.0	0.0.0.0	All	Delete

Figure 5-39 QoS PIR Destination IP Address Add Entry

- c. All the entries present in the PIR IP Address Entries are displayed in the IP Address Entry Table. Select the appropriate radio button and click **Add**. After adding the entry for this specific PIR, it is displayed in the Existing IP Address Entries table. For deleting an entry, click **Delete** for the corresponding entry in the PIR Details page.

### Adding Source MAC Address

- a. Click **Add** to add a new entry. The following screen appears.

S.No.	MAC Address	Mask	Comment	Select
1	00:00:00:00:00:00	00:00:00:00:00:00	All	<input type="radio"/>
2	01:00:00:00:00:00	01:00:00:00:00:00	L2 Multicast	<input type="radio"/>
3	XXXXXXXXXX	XXXXXXXXXX	L2 Broadcast	<input type="radio"/>

S.No.	MAC Address	Mask	Comment	Delete
2	01:00:00:00:00:00	01:00:00:00:00:00	L2 Multicast	Delete

Figure 5-40 QoS PIR Source MAC address Add Entry

- b. All the entries present in the PIR MAC Address Entries are displayed in the MAC Address Entry Table. Select the appropriate radio button and click **Add**. After adding the entry for this specific PIR, it is displayed in the Existing MAC Address Entries table. For deleting an entry, click **Delete** for the corresponding entry in the PIR Details page.

### Adding Destination MAC Address

- a. Click **Add** to add a new entry. The following screen appears.

**QoS PIR Destination MAC Address Add Entry**

Note: Maximum 4 entries are allowed

New MAC Address Entry ADD Back

S.No.	MAC Address	Mask	Comment	Select
1	00:00:00:00:00:00	00:00:00:00:00:00	All	<input type="radio"/>
2	01:00:00:00:00:00	01:00:00:00:00:00	L2 Multicast	<input type="radio"/>
3	#####	#####	L2 Broadcast	<input type="radio"/>

Existing MAC Address Entries

S.No.	MAC Address	Mask	Comment	Delete
2	01:00:00:00:00:00	01:00:00:00:00:00	L2 Multicast	Delete

Figure 5-41 QoS PIR Destination MAC address Add Entry

- b. All the entries present in the PIR MAC Address Entries are displayed in the MAC Address Entry Table. Select the appropriate radio button and click **Add**. After adding the entry for this specific PIR, it is displayed in the Existing MAC Address Entries table. For deleting an entry, click **Delete** for the corresponding entry in the PIR Details page.

### 5.6.2.2 QoS Service Flow Configuration (SFC)

1. Click **ADVANCED CONFIGURATION > QoS > SFC List**. Eight predefined SFCs are displayed in this page. This table allows the user to configure maximum of 32 entries. Service Flow Name should be unique. This SFC can be referred in the QoS Class' Details. SFC referred by any QoS Class cannot be deleted.

**QoS Service Flow Entries**

S.No.	Service Flow Name	Scheduler Type	Traffic Direction	MIR (Kbps)	CIR (Kbps)	Max Latency (ms)	Tolerable Jitter (ms)	Traffic Priority	Max Msgs. In Burst	Entry Status
1	UL-Unlimited BE	BE	Uplink	307200	0	5	5	0	16	Enable
2	DL-Unlimited BE	BE	Down	307200	0	5	5	0	16	Enable
3	DL-L2 Broadcast BE	BE	Down	307200	0	5	5	0	16	Enable
4	UL-G711 20ms VoIP rti	RTPS	Uplink	88	88	20	20	1	16	Enable
5	DL-G711 20ms VoIP rti	RTPS	Down	88	88	20	20	1	16	Enable
6	UL-G729 20ms VoIP rti	RTPS	Uplink	66	66	20	20	1	16	Enable
7	DL-G729 20ms VoIP rti	RTPS	Down	66	66	20	20	1	16	Enable
8	DL 2 Mbps Video	RTPS	Down	2048	2048	20	20	1	16	Enable

Notes: 1. Maximum 32 Entries are allowed.  
 2. Service Flow Name should be unique  
 3. Service Flow referred by any QoS Class can not be deleted.  
 4. For setting the Service Flow Name characters - = \ \ ' ' ? \ \ / space are not allowed.

OK Add


Figure 5-42 QoS Service Flow Entries


**Adding a New Service Flow (SFC):**

- a. Click **Add** to add new entry. The following screen appears for configuring the New PIR Entry.

**Figure 5-43 QoS Service Flow Add Entry**

2. Specify details for the Service Flow Name, Scheduler Type, Traffic Direction, MIR, CIR, Max Latency, Tolerable Jitter, Traffic Priority, Max Messages in Burst and Entry Status.
3. Click **Add**.

Parameter	Description
Service Flow Name	Specifies the Name of the Service Flow. It can be of length 1-32 characters. T  : Special characters - = \\ \" ' ? \\/ <b>space</b> are not allowed.
Scheduler Type	Specifies the Scheduler methods to be used. Scheduler type supports BE (Best Effort), RTPS (Real-Time Polling Service).
Traffic Direction	Specifies the Direction (Downlink or Uplink) of the traffic in which the configuration has to be matched.
MIR (Maximum Information Rate)	Specifies the maximum bandwidth allowed for this Service Flow. This value ranges from 8 kbps to maximum value specified in the license file.
CIR (Committed Information Rate)	Specifies the reserved bandwidth allowed for this Service Flow. This value ranges from 0 to maximum value specified in the license file.
Max Latency	Specifies the Latency value. This value ranges from 5 to 100 ms.
Tolerable Jitter	Specifies the Jitter value. This value ranges from 0 to 100 ms.
Traffic Priority	Specifies the priority of the Service flow when multiple Service flows are assigned to single QoS Class. This value ranges from 0 to 7.

Parameter	Description
Max Messages in Burst	Specifies the maximum number of messages that can be sent in a burst. This value ranges from 1 to 16.   : Reducing the number of messages impacts the throughput.
Entry Status	Specifies the Service Flow status.

### 5.6.2.3 QoS Class Configuration

1. Click **ADVANCED CONFIGURATION > QoS > Class List**. Five predefined QoS Classes are displayed in this page. You can configure maximum 8 entries. QoS Class Name should be unique. This QoS Class can be referred in the Default QoS Class or L2 Broadcast QoS Class. Any QoS Class referred cannot be deleted.
2. Click **OK**.




Figure 5-44 QoS Class Details

Parameter	Description
Default QoS Class	This parameter specifies the QoS Class profile that needs to be associated with an SU or End Point B which is not listed in the QoS SU or End Point B List but connected.
L2 Broadcast QoS Class	This parameter specifies WORP to use this particular class for WORP broadcast facility. L2 Broadcast QoS Class is valid only for Downlink Direction. QoS Class assigned to this profile should have at least one Downlink SFC.

4. Add a New QoS Class:
  - a. Click **Add** to add new entry. The following screen appears for configuring the New Class Entry.

Figure 5-45 QoS Class Add Entry

b. Specify the QoS Class Name, Service Flow Name PIR Rule Name Priority and Entry Status and click **Add**.

Parameter	Description
Class Name	Specifies the Name of the QoS Class. This name length can range from 1 to 32 characters.  : Special characters - = \\ \" ' ? \\/ <b>space</b> are not allowed.
Service Flow Name	Specifies the Service Flow to be associated with the QoS Class. Select one of the possible SFCs that have been previously configured in the SFC List.
PIR Rule Name	Specifies the PIR Rule need to be associated with this Service Flow. Select one of the possible PIRs that have been previously configured in the PIR List.
Priority	Specifies priority or order of execution of PIRs during packet identification process. The PIR priority is a number that can range from 0-255, with priority 255 being executed first, and priority 0 being executed last. The PIR priority is defined within a QoS class, and can be different for the same PIR in some other QoS class. If all PIRs within one QoS class have the same priority, the order of execution of PIR rules will be defined by the order of definition of SFCs, and by the order of definition of PIRs in each SFC, within that QoS class.
Entry Status	Specifies the status of the QoS Class as enable/disable.

### Adding Service Flows in QoS Class

1. Click on the corresponding Details of the QoS Class for adding more Service Flows. Each QoS Class can have maximum 8 Service Flows. At least there should be one service flow per QoS Class. The following screen is displayed to configure the new SFC entry inside the QoS Class.
2. Click **OK**.

S.No.	SFC Name	Entry Status	Details
1	UL-Unlimited BE	Enable	Details
2	DL-Unlimited BE	Enable	Details
3	DL-L2 Broadcast BE	Enable	Details
4	UL-G711 20ms VoIP rPS	Enable	Details
5	DL-G711 20ms VoIP rPS	Enable	Details
6	UL-G729 20ms VoIP rPS	Enable	Details
7	DL-G729 20ms VoIP rPS	Enable	Details

Notes: 1. Maximum 8 Service Flows are allowed.  
2. QoS class should have atleast one Service Flow entry.

OK Add Back

Figure 5-46 QoS Class Service Flow Details

- Click **Add**. The following screen appears for association of the new SFC in this QoS Class.

Service Flow Name: UL-Unlimited BE

PIR Rule Name: All

Priority: 0 (0-255)

Entry Status: Enable

Note : Same Service Flow cannot exists more than once in a QoS Class

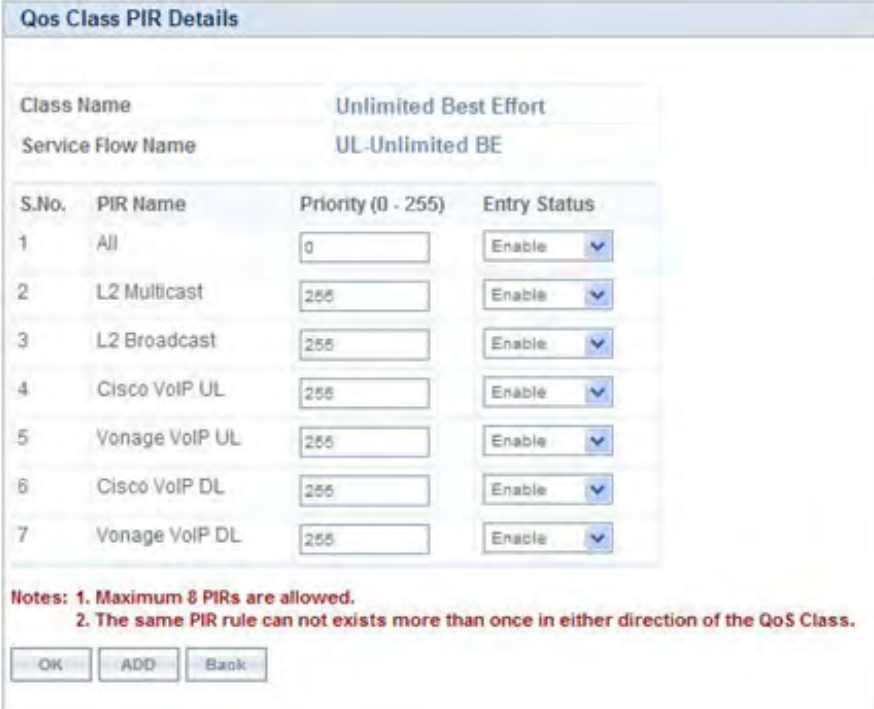
Add Back

Figure 5-47 QoS Class Service Flow Add Entry

- Specify the Service Flow Name, PIR Rule Name, Priority and Entry Status and click **Add** to add a new entry.

#### Adding PIR in QoS Class

- Click on the corresponding Details provided in the Service Flow of a particular QoS Class. Maximum 8 PIR rules can be associated per SFC of an QoS Class. At least there should be one PIR per SFC of an QoS Class. The following screen appears to associate the new PIR entry inside an SFC of an QoS Class.
- Click **OK**.



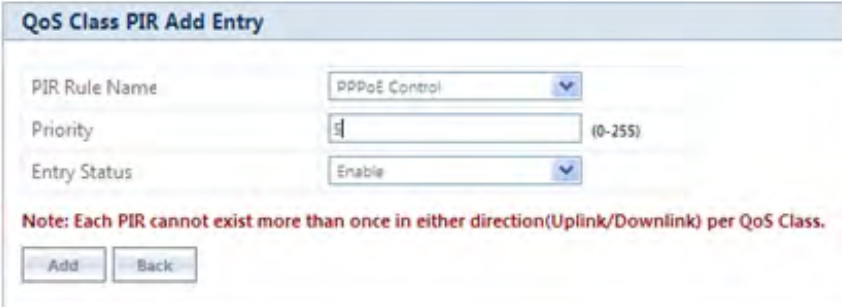
S.No.	PIR Name	Priority (0 - 255)	Entry Status
1	All	0	Enable
2	L2 Multicast	255	Enable
3	L2 Broadcast	255	Enable
4	Cisco VoIP UL	255	Enable
5	Vonage VoIP UL	255	Enable
6	Cisco VoIP DL	255	Enable
7	Vonage VoIP DL	255	Enable

**Notes:** 1. Maximum 8 PIRs are allowed.  
2. The same PIR rule can not exists more than once in either direction of the QoS Class.

OK ADD Back

Figure 5-48 QoS Class PIR Details

- Click **Add**. The following screen appears for association of the new PIR rule in an SFC already associated in an QoS Class.



PIR Rule Name: PPPoE Control

Priority: 5 (0-255)

Entry Status: Enable

**Note:** Each PIR cannot exist more than once in either direction(Uplink/Downlink) per QoS Class.

Add Back

Figure 5-49 QoS Class PIR Add Entry

- Specify the PIR Rule Name, Priority and Entry Status and click **Add** to add a new entry.

#### 5.6.2.4 QoS SU or End Point B List Configuration

- Navigate to **ADVANCED CONFIGURATION > QoS > SU or End Point B List**. By default, the table does not have any entry. User can configure the Wireless MAC Address of the SU or End Point B here and associate the QoS Class that is to be used for that particular SU or End Point B.

S.No.	MAC Address	Class Name	Comment	Entry Status
1	10.20.30.40.50.60	Unlimited Best Effort	Test_Case	Enable

Notes : 1. Maximum 250 SUs allowed.  
2. SU MAC Address should be unique.

Add Edit

Figure 5-50 QoS SU or End Point B List Entries

- If an SU or End Point B is not in the list and is associated, the default QoS class configuration is applied.

### Adding a New SU or End Point B

- Navigate to **ADVANCED CONFIGURATION > QoS > SU or End Point B List**. The **QoS SU or End Point B Entries** screen appears.
- Click **Add** to add a new entry. The following **QoS SU or End Point B Table Add Row** screen appears.

QoS SU Table Add Row	
Wireless MAC Address	10.20.30.40.50.60
Class Name	Unlimited Best Effort
Comment	TEST_CASE
Entry Status	Enable
Add Back	

Figure 5-51 QoS SU or End Point B Table Add Row

- Specify the Wireless Mac Address of the SU or End Point B, Class Name, Comment and Entry Status and click **Add**. Previously defined Class Name can be viewed in the **Class Name** drop-down box.



- QoS SU Entries configuration can be done locally or through a RADIUS Server.
- Local configuration takes priority over RADIUS Based QoS configuration.
- RADIUS Configuration is applicable only when the **RADIUS MAC ACL Status** is enabled on the BSU.
- When the link is down, the RADIUS configuration is lost.

### 5.6.3 QoS Configuration for a Management Station

As stated previously, the QoS feature enables prioritization of traffic and allocation of the available bandwidth based on that prioritization. The system is designed in such a way that higher priority traffic preempts lower priority traffic, keeping lower priority traffic on hold until higher priority traffic finishes. This mechanism ensures that the available bandwidth is always given first to the higher priority traffic; if all the bandwidth is not consumed, the remaining bandwidth is given to the lower priority traffic.

If QoS is not properly configured, the system becomes difficult to access in heavily loaded networks. One of the side effects of this misconfiguration is ping time-out, which is usually interpreted as a disconnection of the pinged node. However, with the correct QoS configuration, every node in the network can be reached at any point of time.



The following configuration instructions explain how to configure the system so that configuration parameters can always be changed, and ping requests and responses get higher priority in order to show the actual connectivity of the pinged node.

The configuration suggested here assumes that the whole network is managed from a single work station, called the management station. This station can be connected anywhere in the network, and can be recognized by either its IP address, or by its MAC Ethernet address if the network uses DHCP.

In this configuration, any traffic coming from or going to the management station is treated as management traffic. Therefore, the management station should be used only for configuration of the Quick Bridge nodes in the network and to check connectivity of the nodes, but it should not be used for any throughput measurements.



*: While this QoS configuration is used, the TCP or UDP throughput should not be measured from the management station.*

### Step 1: Add Packet Identification Rules

To recognize management traffic, the system needs to recognize ARP requests or responses and any traffic coming from or going to the management station.

#### A. Confirm the Attributes of the Existing ARP PIR

The default QoS configuration contains the PIR called “ARP,” which recognizes ARP requests or responses by the protocol number 0x0806 in the Ethernet Type field of the Ethernet packet. Confirm that the ARP PIR parameters are correct, as follows:

1. Navigate to **ADVANCED CONFIGURATION > QoS > PIR list**.
2. Click **Details** corresponding to the ARP PIR.
3. Confirm the following attributes:
  - Rule Name: ARP
  - Status: Enable
  - Enable Ether Type Rule: Yes (checkbox is selected)
    - Ether Type: DIX-Snap
    - Ether Value: 08:06(hex)

#### B. Create New PIRs to Recognize Management Traffic

To recognize the traffic coming from or going to the management station, the system must contain two additional PIRs: one with either the destination IP address or the destination MAC address equal to the management station’s IP or MAC address, and another with either the source IP address or the source MAC address equal to the management station’s IP or MAC address. The following examples explain PIR rules based on the IP Address of the Management Station.

1. Navigate to **ADVANCED CONFIGURATION > QoS > PIR list > IP Address Entries**.
2. Click **Add**. The screen for adding the Management Station’s IP Address appears. Enter proper IP Address, Subnet mask as 255.255.255.255, Entry status as **Enable** and then click **Add**. This adds the Management Station’s IP details in the IP Address Entries of the PIR List.
3. Navigate to **ADVANCED CONFIGURATION > QoS > PIR list**.
4. Add PIR Rule for Source IP Address.
  - a. Click **Add**. The screen for adding the New PIR Rule appears. Enter the PIR Rule Name as “Management Station SRC IP”, Entry status as **Enable** and click **Add**. This adds the new PIR rule in the PIR List. By default, no classification rules are applied.
  - b. Navigate to **ADVANCED CONFIGURATION > QoS > PIR list**. Click **Details** for “Management Station SRC IP” PIR rule. This displays all the classification rule details for this particular rule.

- c. Click **Add** that corresponds to Source IP Address Entries. This displays a screen for referring the Management Station's IP Address. New Entry Table displays all the IP Address Entries of the PIR List. Select the option button corresponding to the Management Station and then click **Add**. This adds the IP Address of the Management Station to the Existing Entries. Click **Back** and the new entry appears in the Source IP Address Entries Table.
5. Add PIR Rule for Destination IP Address.
    - a. Click **Add**. This displays a screen for adding the New PIR Rule. Enter the PIR Rule Name as "Management Station DST IP", Entry status as **Enable** and then click **Add**. This adds the new PIR rule in the PIR List. By default, no classification rules are applied.
    - b. Navigate to **ADVANCED CONFIGURATION > QoS > PIR list**. Click **Details** corresponding to the "Management Station DST IP" PIR rule. This displays the classification rule details for this particular rule.
    - c. Click **Add** corresponding to Destination IP Address Entries. This displays a screen for referring the Management Station's IP Address. New Entry Table displays all the Entries of the IP Address Entries of the PIR List. Select the option button corresponding to the Management Station and click **Add**. This adds the IP Address of the Management Station to the Existing Entries. Click **Back** and the new entry appears in the Destination IP Address Entries Table.

## Step 2: Add Service Flow Classes

To handle management traffic, the system needs two Service Flow Classes: one for uplink traffic and one for downlink traffic.

1. Configure the Downlink Service Flow.
  - a. Navigate to **ADVANCED CONFIGURATION > QoS > SFC list**.
  - b. Click **Add**.
  - c. Enter the following parameters:
    - Service Flow Name: DL-Management
    - Scheduler Type: RtPS
    - Traffic Direction: Downlink
    - MIR: 1000
    - CIR: 1000
    - Max Latency: 20
    - Tolerable Jitter: 10
    - Priority: 7
    - Max Messages in Burst: 16
    - Entry Status: Enable
  - d. Click **Add**. The DL-Management Service Flow is added to the QoS SFC List.
2. Configure the Uplink Service Flow.
  - a. Navigate to **ADVANCED CONFIGURATION > QoS > SFC list**.
  - b. Click **Add**.
  - c. Enter the following parameters:
    - Service Flow Name: UL-Management
    - Scheduler Type: RtPS
    - Traffic Direction: Uplink
    - MIR: 1000
    - CIR: 1000
    - Max Latency: 20
    - Tolerable Jitter: 10
    - Priority: 7

- Max Messages in Burst: 16
  - Entry Status: Enable
- d. Click **Add**. The UL-Management SF is added to the QoS SFC List.

**NOTE:** The input and output bandwidth limits set on the End Point A or BSU or on the End Point B or SU are used for limiting aggregate bandwidth used by the SU or End Point B. These limits override any limit imposed by MIR in the SFC. Therefore, these limits should be set to at least 1000 kbps (MIR values in UL-Management and DL-Management SFCs).

### Step 3: Configure QoS Classes

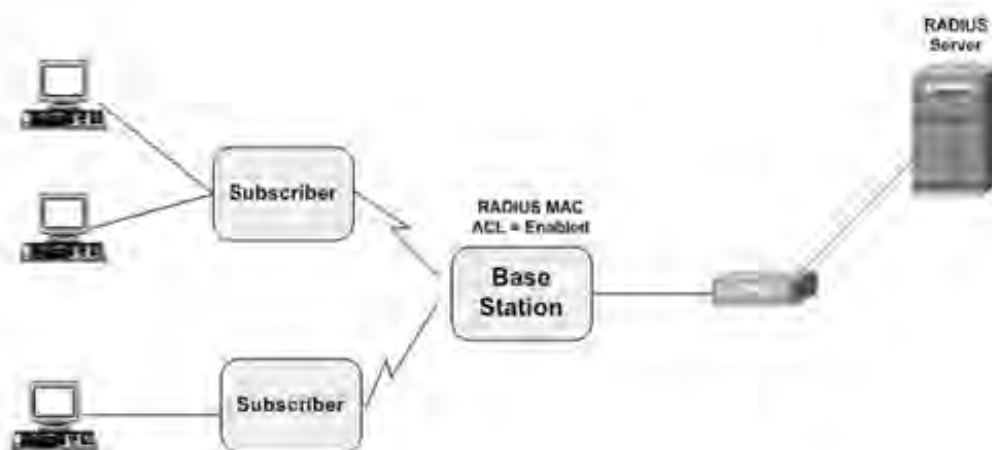
Finally, the DL-Management SFC and UL-Management SFCs created in Step 2 must be added to each QoS Class used by the Quick Bridge network. Additionally, within the QoS class, these SFC must have the three PIRs mentioned in Step 1 associated with them.

1. Add SFCs to QoS Class.
  - a. Navigate to **ADVANCED CONFIGURATION > QoS > Class list**.
  - b. Click **Details** corresponding to the first class (Unlimited Best Effort) you wish to modify.
  - c. Under the QoS Class Service Flow, click **Add**.
  - d. Configure the following parameters, and click **Add**. This adds the New SFC & PIR relation to the QoS Class.
    - Service Flow Name: DL-Management
    - PIR Rule Name: ARP
    - PIR Priority: 63
    - Entry Status: Enable.
  - e. Again click **Add** under the QoS Class Service Flow Details.
  - f. Configure the following parameters and click **Add**. This adds the New SFC & PIR relation to the QoS Class.
    - Service Flow Name: UL-Management
    - PIR Rule Name: ARP
    - PIR Priority: 63
    - Entry Status: Enable
2. Add PIRs to SFCs within the QoS Class.
  - a. Navigate to **ADVANCED CONFIGURATION > QoS > Class list**.
  - b. Click **Details** corresponding to the first class (Unlimited Best Effort) you wish to modify.
  - c. Under the QoS Class Service Flow Details, click **Details** corresponding to the DL-Management Service Flow.
  - d. Under the QoS Class PIR Details heading, click **Add**.
  - e. Add the Management Station DST IP PIR to this Service Flow by configuring the following parameters:
    - PIR Rule Name: Management Station DST IP
    - PIR Priority: 63
    - Entry Status: Enable
  - f. Click **Add**. This PIR is added to the first QoS Class (Unlimited Best Effort) Service Flow's (DL-Management) list.
  - g. Add the Management Station SRC IP PIR to this Service Flow by configuring the following parameters:
    - PIR Rule Name: Management Station SRC IP
    - PIR Priority: 63
    - Entry Status: Enable
  - h. Return to the Class List and repeat steps 2 - 7 for the UL-Management Service Flow in this class.

## 5.7 RADIUS Based SU QoS Configuration

RADIUS based QoS configuration enables you to configure QoS parameters on a SU through RADIUS Server. This way of configuring QoS parameters, reduces the task of manually configuring QoS parameters on each SU available on the network.

Explained below is the process followed to configure QoS parameters on a SU from a RADIUS Server.



**Figure 5-52 RADIUS Based QoS Configuration**

To establish a connection with the BSU, the SU sends a registration request to BSU. On receiving the registration request, the BSU sends an Access request along with the SU MAC address, to the RADIUS Server. The RADIUS Server then checks the authentication of the user. If it is an authenticated user, it sends an Access-Accept response along with Vendor assigned QoS parameter's value to the BSU. On receiving the response, the BSU sends the response to the SU. The received QoS parameters are then applied on the SU.

Tabulated below are the vendor specific attributes:

Name of the attribute	Vendor Assigned Attribute Number	Attribute Format	Attribute Value
QoS Class Index	34	Decimal	1 - 8
QoS Class SU Table Status	35	Decimal	1 - Enable / 2 - Disable



- RADIUS Based QoS configuration takes priority over Local QoS configuration.
- When the link is down, the configuration received from the RADIUS is lost.

## 5.8 VLAN (Bridge Mode Only)

The Virtual Local Area Network (VLAN) feature helps in logical grouping of network host on different physical LAN segments, which can communicate with each other as if they are all on the same physical LAN segment.

With VLANs, you can 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

The SUs and End Point devices support QinQ VLAN feature that enables service providers to use a single VLAN ID to support multiple customer VLANs by encapsulating the 802.1Q VLAN tag within another 802.1Q frame. The benefits with QinQ are,

- Increases the VLAN space in a provider network or enterprise backbone
- Reduce the number of VLANs that a provider needs to support within the provider network for the same number of customers
- Enables customers to plan their own VLAN IDs, without running into conflicts with service provider VLAN IDs
- Provides a simple Layer 2 VPN solution for small-sized MANs (Metropolitan Area Networks) or intranets
- Provides customer traffic isolation at Layer 2 within a service provider network



**: VLAN can be configured in Bridge Mode only.**

### 5.8.1 System-Level VLAN Configuration

To configure system-level VLAN parameters, navigate to **ADVANCED CONFIGURATION > VLAN**. The **VLAN** configuration screen appears.

**Figure 5-53 System-Level VLAN Configuration**

1. **VLAN Status:** This parameter is used to either enable or disable VLAN feature on the device. By default, this parameter is disabled. To enable VLAN, select the **VLAN Status** box. If VLAN status is enabled, it indicates that locally configured VLAN parameters will be applied on the device. If VLAN status is disabled, it indicates that the device is open for remote VLAN configuration.
2. **Management VLAN Id:** This parameter enables the user to configure VLAN Id for management frames (SNMP, ICMP, Telnet and TFTP). The stations that manage the device must tag the management frames with the management VLAN Id. By default, the Management VLAN Id is set to -1 which indicates no tag is added to the management frame. To set VLAN tag to the management frame, enter a value ranging from 1 to 4094.



: Before setting the Management VLAN Id, make sure that the station that manages the device is a member of the same VLAN; else, your access to the device will be lost.

3. **Management VLAN Priority:** This parameter is used to set IEEE 802.1p priority for the management frames. By default, the priority is set to 0. To set the VLAN priority, enter a value ranging from 0 to 7.
4. **Double VLAN (Q in Q) Status:** Q in Q (also called as Double VLAN or Stacked VLAN) mechanism expands the VLAN space by tagging the tagged packets, thus producing a “double-tagged” frame. The expanded VLAN space allows the service provider to provide certain services, such as Internet access on specific VLANs for specific customers, and still allows the service provider to provide other types of services for their other customers on other VLANs.  
By default, Double VLAN is disabled on the device. To enable, select **Enable** from the **Double VLAN (Q in Q) Status** box and click **OK**.



- If **Double VLAN (Q in Q) Status** is enabled, device expects Double VLAN tagged packet in DownLink Direction. Management can be accessed with single VLAN/Double VLAN based on the management VLAN ID configured.
- Only SU, End Point A and End Point B support Double VLAN (Q in Q) feature.

5. **Service VLAN TPID:** The Tag Protocol Identifier (TPID) helps to identify the frame as VLAN tagged frame. By default the Service VLAN TPID is set to 0x8100. To interwork with few vendor devices that set the TPID to 0x9100, the device allows the user to configure Service VLAN TPID as 0x9100. In this case, when a QinQ packet goes out of the device, the Ether type of outer VLAN tag is changed to 0x9100.
6. **Service VLAN Id:** This parameter enables the user to configure outer/service provider VLAN ID for the data frames. By default, the Service VLAN ID is set to -1 which indicates no outer/service VLAN tag is added to the data frame. To set VLAN tag to the frame, enter a value ranging from 1 to 4094.



: When Double VLAN is enabled on the device, the Service VLAN ID should not be set to -1.

7. **Service VLAN Priority:** This parameter is used to set IEEE 802.1p priority in outer/service VLAN tag for the data frames. By default, the priority is set to 0. To set the VLAN priority, enter a value ranging from 0 to 7.

## 5.8.2 Ethernet VLAN Configuration

You can configure VLAN on the ethernet interface(s) by using any one of the following VLAN Modes:

1. Transparent Mode
2. Access Mode
3. Trunk Mode

### 5.8.2.1 Transparent Mode

Transparent mode can be configured in a BSU, SU and End Point devices. This mode is equivalent to NO VLAN support and is the default mode. It is used to connect VLAN aware or unaware networks. In this mode, the device transfers both tagged and untagged frames received on the Ethernet or WORM interface.

To configure the Ethernet interface of the device in VLAN Transparent Mode, navigate to **ADVANCED CONFIGURATION > VLAN > Ethernet**. The **VLAN Ethernet Configuration** screen appears:

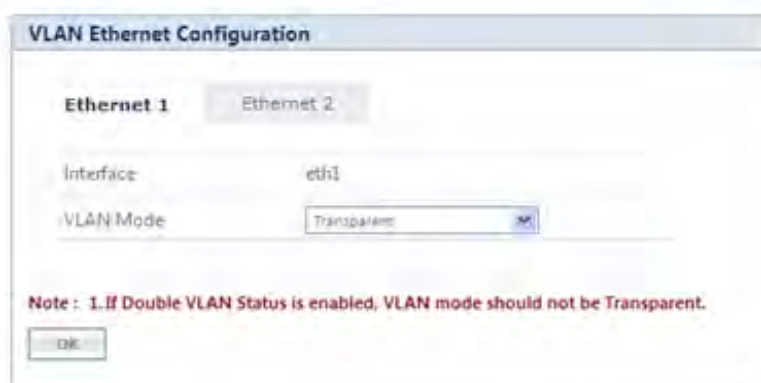



Figure 5-54 Transparent Mode

Tabulated below is the table which explains the method to configure the device in Transparent mode:

Parameters	Description
Interface	Displays the name of the Ethernet interface.
VLAN Mode	Select the <b>VLAN mode</b> as <b>Transparent</b> .   : When the device is configured in Double VLAN mode, do not configure the Ethernet interface of the device in Transparent Mode.

Click **OK** and then **COMMIT**.



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

### 5.8.2.2 Access Mode

Access Mode can be configured in a SU, End Point A and End Point B. This mode is used to connect VLAN aware networks with VLAN unaware networks.

The ingress untagged traffic received on the Ethernet interface are tagged with the configured Access VLAN Id and Access VLAN priority before forwarding to the WORM interface. Similarly all egress tagged frames with specified VLAN Id are untagged at the Ethernet interface and then forwarded. Based on the Management VLAN ID configuration, both tagged and untagged management frames can access the device from the WORM interface. However, only untagged management frames can access the device from the Ethernet Interface; the tagged frames are dropped.

To configure the Ethernet interface of the device in Access Mode, navigate to **ADVANCED CONFIGURATION > VLAN > Ethernet**. The **VLAN Ethernet Configuration** screen appears:

**VLAN Ethernet Configuration**

**Ethernet 1**    Ethernet 2

Interface: eth1

VLAN Mode: Access

Access VLAN Id: -1 (1-1-4094)


Access VLAN Priority: 0 (0-7)

Notes: 1. If Double VLAN Status is enabled, VLAN mode should not be Transparent.  
2. If Double VLAN Status is enabled, Access VLAN id should not be -1.

OK

Figure 5-55 Access Mode

Tabulated below is the table which explains the method to configure the device in Access Mode:

Parameter	Description
Interface	Displays the name of the Ethernet interface.
VLAN Mode	Select the <b>VLAN mode</b> as <b>Access</b> and click <b>OK</b> .
Access VLAN Id	Enter the Access VLAN Id in the <b>Access VLAN Id</b> box. The untagged data frames received at the Ethernet interface are tagged with this configured VLAN Id and then forwarded to the WORP interface. By default, the Access VLAN Id is set to -1 which indicates no tag is added to the data frame. To set Access VLAN tag to the data frame, enter a value ranging from 1 to 4094.   : When Double VLAN is enabled on the device, the Access VLAN ID should not be set to -1.
Access VLAN Priority	This parameter is used to set IEEE 802.1p priority for the data frames. By default, the priority is set to 0. To set the Access VLAN priority, enter a value ranging from 0 to 7.

Click **OK** and then **COMMIT**.

### 5.8.2.3 Trunk Mode

Trunk Mode can be configured in a BSU, SU, End Point A and End Point B. This mode is used to connect VLAN aware networks with VLAN aware networks. In the Trunk mode, the Ethernet interface of the device forwards only those tagged frames whose VLAN Id matches with a VLAN Id present in the trunk table.

If the device receives untagged frames and the **Allow Untagged Frames** functionality is disabled, then the untagged packets are dropped.

If the **Allow Untagged Frames** functionality is enabled, then functionality varies based on the device:

- In case of a BSU, the untagged packets are forwarded to the destination.
- In case of a SU, End Point A and End Point B, the device behaves as in Access Mode for untagged traffic. The untagged frames are tagged with the configured Port VLAN ID and forwarded to the destination.





: Mixed VLAN Mode = Trunk Mode + Allow Untagged Frames + Port VLAN ID

To configure the Ethernet interface of the device in Trunk mode, navigate to **ADVANCED CONFIGURATION > VLAN > Ethernet**. The **VLAN Ethernet Configuration** screen appears:

**VLAN Ethernet Configuration**

**Ethernet 1** | Ethernet 2

Interface: eth1

VLAN Mode: Trunk

Allow untagged frames: Enable

S.No.	Trunk Id	Entry Status
1.1	8	Enable

Buttons: OK, Add

Figure 5-56 Trunk Mode (BSU)

**VLAN Ethernet Configuration**

**Ethernet 1** | Ethernet 2

Interface: eth1

VLAN Mode: Trunk

Allow untagged frames: Enable

Port VLAN Id: -1 (-1, 1-4094)

Port VLAN Priority: 0 (0-7)

S.No.	Trunk Id	Entry Status
1.1	8	Enable

Notes:



1. If Double VLAN Status is enabled, VLAN mode should not be Transparent.
2. If Double VLAN Status is enabled, Port VLAN id should not be -1.
3. Port VLAN id should not exist in Trunk Table.

Buttons: OK, Add

Figure 5-57 Trunk Mode (SU/End Point A/End Point B)

Tabulated below is the table which explains the method to configure the device in Trunk Mode:

Parameter	Description
Interface	Displays the name of the Ethernet interface.
VLAN Mode	Select the <b>VLAN Mode</b> as <b>Trunk</b> .

Parameter	Description
Allow Untagged Frames	<p>Select <b>Enable</b> or <b>Disable</b>. By default, it is disabled.</p> <ul style="list-style-type: none"> <li>• <b>Disable:</b> If this option is selected, the Ethernet interface forwards only tagged frames whose VLAN Id matches with a VLAN ID present in trunk table.</li> <li>• <b>Enable:</b> <ul style="list-style-type: none"> <li>- In case of a BSU, when <b>Allow Untagged Frames</b> is enabled, the Ethernet interface of the device forwards the data packets as-is.</li> <li>- In case of a SU/End Point A/End Point B, when <b>Allow Untagged Frames</b> is enabled, the device behaves as in Access mode. Click <b>OK</b>.</li> </ul> </li> </ul>
Port VLAN ID	<p>Enter the Port VLAN ID in the <b>Port VLAN ID</b> box. The untagged data frames received at the Ethernet interface are tagged with this port VLAN Id and then forwarded to the destination interface. By default, the Port VLAN Id is set to -1 which indicates no tag is added to the data frame. To set Port VLAN tag to the data frame, enter a value ranging from 1 to 4094.</p>  <ul style="list-style-type: none"> <li>• Applicable only on a SU, End Point A and End Point B.</li> <li>• When Double VLAN is enabled on the device, the Port VLAN ID should not be set to -1.</li> <li>• The configured Port VLAN Id should not exist in the Trunk table.</li> </ul>
Port VLAN Priority	<p>This parameter is used to set IEEE 802.1p priority for the data frames. By default, the priority is set to 0. To set the Port VLAN priority, enter a value ranging from 0 to 7.</p>  <p>: Applicable only to SU and End Point devices.</p>

After configuring the required parameters, click **OK** and then **COMMIT. Add**

### VLAN IDs to Trunk Table

To add VLAN IDs to the trunk table,

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



Figure 5-58 Add VLAN IDs to Trunk Table

Tabulated below is the table which explains the method to add VLAN IDs to Trunk Table:

Parameter	Description
Trunk Id	Enter VLAN ID in the <b>Trunk Id</b> box.
Entry Status	This parameter indicates the status of each VLAN Trunk Id entry. By default, the Trunk Id is enabled. To disable, select <b>Disable</b> from the <b>Entry Status</b> box.

2. Click **Add**.
3. To save and apply the configured parameters on the device, click **COMMIT**.



: You can configure a maximum of 256 trunk VLAN Ids in a BSU and End Point A device, and 16 VLAN Ids in a SU and End Point B device.

## 5.9 RADIUS Based SU VLAN Configuration

RADIUS based VLAN configuration enables you to configure VLAN parameters on a SU through RADIUS Server. This way of configuring VLAN parameters,

- Reduces the task of manually configuring VLAN parameters on each SU available on the network
- Allows SU to remain on the same VLAN as it moves across the network

Explained below is the process followed to configure VLAN parameters on a SU from a RADIUS Server.

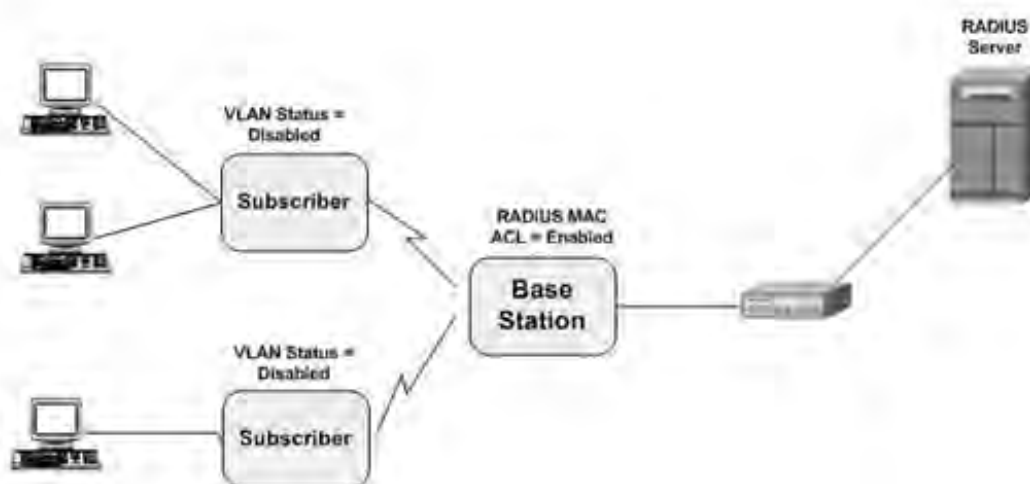


Figure 5-59 RADIUS Based VLAN Configuration

To establish a connection with the BSU, the SU sends a registration request to BSU. On receiving the registration request, the BSU sends an Access request along with the SU MAC address, to the RADIUS Server. The RADIUS Server then checks the authentication of the user. If it is an authenticated user, it sends an Access-Accept response along with Vendor assigned VLAN parameter's value to the BSU. On receiving the response, the BSU sends the response to the SU. The received VLAN parameters are then applied on the SU.

Tabulated below are the vendor specific attributes:

Name of the attribute	Vendor Assigned Attribute Number	Attribute Format	Attribute Value
SU_VLAN_MAC	3	MacAddr	SU Mac Address
VLAN_ETH1 Vlan Mode	4	Decimal	1 -Transparent Mode 2 - Trunk Mode / 3 - Access Mode
SU_VLAN_Name	5	String	SU VLAN Name
VLAN_ETH1 Access VLAN ID	6	Decimal	1 - 4095
VLAN_ETH1 Access Vlan Priority	7	Decimal	0 - 7
Management VLAN ID attribute	8	Decimal	1 - 4095
Management VLAN Priority	9	Decimal	0 - 7
VLAN_ETH1 TrunkID 1 ... 16	10 ... 25	Decimal	1 - 4095
SU_VLAN_Table_Status	26	Decimal	1 - enable / 2 - disable / 3 - delete
Service Vlan Id (Q-inQ)	32	Decimal	1 - 4095
Service Vlan Priority (Q-inQ)	33	Decimal	0 - 7
QoS Class Index	34	Decimal	1 - 8
QoS Class SU Table Status	35	Decimal	1 - Enable / 2 - Disable
VLAN_ETH2 Vlan Mode	40	Decimal	1 - Transparent Mode 2 - Trunk Mode / 3 - Access Mode
VLAN_ETH2 Access Vlan Id	41	Decimal	1 - 4095
VLAN_ETH2 Access Vlan Priority	42	Decimal	0 - 7
VLAN_ETH2 TrunkID 1 ... 16	43 ... 58	Decimal	1 - 4095
Double Vlan (Q-in-Q) Status	59	Decimal	1 - Enable / 2 - Disable
Service Vlan TPID (Q-inQ)	60	Decimal	1 - InnerTag / 2 - Outer Tag
VLAN_ETH1_Port_Vlan_Id	61	Decimal	1 - 4095
VLAN_ETH1_Port_Vlan_Pri	62	Decimal	0 - 7
VLAN_ETH1_Allow_Untag_Frames	63	Decimal	1 - Enable / 2 - Disable
VLAN_ETH2_Port_Vlan_Id	64	Decimal	1 - 4095
VLAN_ETH2_Port_Vlan_Pri	65	Decimal	0 - 7
VLAN_ETH2_Allow_Untag_Frames	66	Decimal	1 - Enable / 2 - Disable



- RADIUS Configuration is applicable only when the VLAN Status is disabled on the SU.
- Local VLAN configuration takes priority over RADIUS Based VLAN configuration.
- When the link is down, the configuration received from the RADIUS is lost.

## 5.10 Filtering (Bridge Only)

Filtering is useful in controlling the amount of traffic exchanged between the wired and wireless networks. By using filtering methods, we can restrict any unauthorized packets from accessing the network. Filtering is available only in bridge mode.

The various filtering mechanisms supported by the device are as follows:

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


Filters get activated only when they are globally enabled on the device. To apply/configure global filters on the device, navigate to **ADVANCED CONFIGURATION > Filtering**. The **Filtering** screen appears.



**Figure 5-60 Filtering**

Tabulated below is the table which explains Filtering parameters and the method to configure the configurable parameter(s):

Parameter	Description
Global Filter Flag	<p>By default, Global Filtering is disabled meaning which no filters are applied on the device. To apply filters on the device, enable the Global Filter Flag.</p> <p>Please note that if Global Filter Flag is not enabled on the device, then none of the filters can be applied on the device.</p>

Parameter	Description
STP/LACP Frames	<p>This parameter allows you to either <b>Block</b> or <b>Passthru</b> STP/LACP frames on the network.</p> <ul style="list-style-type: none"> <li>• <b>Passthru</b>: By allowing the STP/LACP frames, any loops that occurs within a network can be avoided. If configured to Passthru, the STP/LACP frames in the system are bridged.</li> <li>• <b>Block</b>: When blocked, the STP/LACP frames encountered on a network are terminated at bridge.</li> </ul> <p>By default, STP/LACP frames are allowed on the network.</p> <p> : STP or LACP Frame Status will block or passthru the frames destined to IEEE 802.1D and 802.1Q reserved MAC address (01:80:C2:00:00:00 to 01:80:C2:00:00:0F).</p>

After configuring the required parameters, click **OK** and then **COMMIT**.

### 5.10.1 Protocol Filter

The Protocol Filter blocks or forwards packets based on the protocols supported by the device.

To configure Protocol Filter on the device, navigate to **ADVANCED CONFIGURATION > Filtering > Protocol Filter**. The **Protocol Filter** screen appears:

**Protocol Filter**


Filtering Control:

Filtering Type:

S.No.	Protocol Name	Protocol Number	Filter Status	Entry Status
1	<input type="text" value="Apollo-Domain"/>	<input type="text" value="8019"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>
2	<input type="text" value="Apple-Talk-1-and-2"/>	<input type="text" value="809b"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>
3	<input type="text" value="Apple-Talk-ARP-1-and-2"/>	<input type="text" value="809f"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>
4	<input type="text" value="Banyan-VINES"/>	<input type="text" value="0bad"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>
5	<input type="text" value="Banyan-VINES-Echo"/>	<input type="text" value="0baf"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>
6	<input type="text" value="Decnet-Phase-IV"/>	<input type="text" value="8003"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>
7	<input type="text" value="DEC-Diagnostic"/>	<input type="text" value="8005"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>
8	<input type="text" value="DEC-LAT"/>	<input type="text" value="8004"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>
9	<input type="text" value="DEC-MOP-Dump/Load"/>	<input type="text" value="8001"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>
10	<input type="text" value="DEC-MOP-Rem-Cons"/>	<input type="text" value="8002"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>
11	<input type="text" value="DEC-NetBIOS"/>	<input type="text" value="8040"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>
12	<input type="text" value="HP-Probe-Control"/>	<input type="text" value="8005"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>
13	<input type="text" value="IBM-SNA-Services"/>	<input type="text" value="80d5"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>
14	<input type="text" value="IP-ARP"/>	<input type="text" value="0806"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>
15	<input type="text" value="Novell(ECONFIG-E)"/>	<input type="text" value="8137"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>
16	<input type="text" value="RARP-Reverse-ARP"/>	<input type="text" value="8035"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>
17	<input type="text" value="SNMP-Over-Ethernet"/>	<input type="text" value="814c"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>
18	<input type="text" value="Xyplex"/>	<input type="text" value="0888"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>
19	<input type="text" value="EAPOL-ether-type"/>	<input type="text" value="888e"/>	Block <input type="button" value="v"/>	Disable <input type="button" value="v"/>

Figure 5-61 Protocol Filter

Tabulated below is the table which explains Protocol Filter parameters and the method to configure the configurable parameter(s):

Parameter	Description
Filtering Control	<p>This parameter is used to configure the interface on which filtering has to be applied. The filtering can be applied on any of the following interfaces:</p> <ul style="list-style-type: none"> <li>• <b>Ethernet:</b> Packets are examined at the Ethernet interface.</li> <li>• <b>Wireless:</b> Packets are examined at the Wireless interface.</li> <li>• <b>All Interfaces:</b> Packets are examined at both Ethernet and Wireless interface. By default, the Filtering Control is set to <b>Disable</b>, meaning which Protocol Filters are disabled on all the interfaces.</li> </ul> <p> : In addition to enabling <b>Filtering Control</b>, the <b>Global Filter Flag</b> should also be enabled for the filter to take effect.</p>
Filtering Type	<p>This parameter specifies the action to be performed on the data packets whose protocol type is not defined in the protocol filter table (this table contains a list of default protocols supported by the device and the protocols defined by the user), or whose Entry Status is in Disable state. The available filtering types are:</p> <ul style="list-style-type: none"> <li>• <b>Block:</b> The protocols with entry status Disable or the protocols which do not exist in the protocol filtering table are blocked.</li> <li>• <b>Passthru:</b> The protocols with entry status Disable or the protocols which do not exist in the protocol filtering table are allowed through the configured interface.</li> </ul>


After configuring the required parameters, click **OK** and then **COMMIT**.

#### 5.10.1.1 Protocol Filter Table

The Protocol Filter table displays a list of default protocols supported by the device and the protocols created by the user. By default, the system generates 19 protocols entries. Each of the Protocol contains the following information:

Parameter	Description
Protocol Name	Represents the Protocol name. The system throws an error when you try to edit the name of a default protocol.
Protocol Number	Represents the Protocol number. The value is of 4 digit hexadecimal format. The system throws an error when you try to edit the Protocol number of a default protocol.
Filter Status	<p>The supported filter status are,</p> <ul style="list-style-type: none"> <li>• <b>Passthru:</b> When the filter status is set to <b>Passthru</b> and entry status is <b>Enable</b>, all packets whose protocol matches with the given protocol number are forwarded on the configured interface.</li> <li>• <b>Block:</b> When the filter status is set to <b>Block</b> and entry status is <b>Enable</b>, all packets whose protocol matches with the given protocol number are dropped on the configured interface.</li> </ul> <p>By default, the status is set to Block.</p>



Entry Status	Set the entry status as either Enable, Disable or Delete. <ul style="list-style-type: none"> <li>• <b>Enable:</b> Enables filter status on a protocol.</li> <li>• <b>Disable:</b> Disables filter status on a protocol.</li> <li>• <b>Delete:</b> Deletes a protocol entry from the Protocol Filter Table.</li> </ul>
 : System-defined default protocols cannot be deleted.	

### 5.10.1.2 Add User-defined Protocols to the Filter Table

To add user-defined protocols to the Protocol Filter Table, click **Add** in the **Protocol Filter** screen. The **Protocol Filter Add Row** screen appears.



Figure 5-62 Add User-defined Protocols

Enter details for all the required parameters and click **Add**.



: The maximum number of Protocol Filters that can be added to the table are 64, out of which 19 are default entries.

### 5.10.2 Static MAC Address Filter

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

Each MAC Address or Mask is comprised of 12 hexadecimal digits (0-9, 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 will look for when examining packets. The device uses Boolean logic to perform an “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 will examine 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 will only look for the specific MAC address (in this case, 00:20:A6:12:54:C3).

You can configure the Static MAC Address Filter parameters depending on the following scenarios:

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

### Static MAC Filter Examples

Consider a network that contains a wired PC and three wireless PCs. The MAC addresses for each PCs are as follows:

- **MAC Address of the wired PC:** 00:40:F4:1C:DB:6A
- **MAC Address of the wireless PC1:** 00:02:2D:51:94:E4
- **MAC Address of the wireless PC2:** 00:02:2D:51:32:12
- **MAC Address of the wireless PC3:** 00:20:A6:12:4E:38

#### **Prevent two specific PCs from communicating**

Configure the following settings to prevent the wired PC and wireless PC1 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 PC and wireless PC1 is blocked. wireless PC2 and PC3 can still communicate with the wired PC.

#### **Prevent multiple Wireless PCs from communicating with a single wired PC**

Configure the following settings to prevent wireless PC1 and PC2 from communicating with the wired PC:

- **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 PC1 and wireless PC2 share the same prefix (00:02:2D), traffic between the wired Server and wireless PC1 and PC2 is blocked. Wireless PC3 can still communicate with the wired PC since it has a different prefix (00:20:A6).

#### **Prevent all wireless PCs from communicating with a single wired PC**

Configure the following settings to prevent wired PC from communicating with all three wireless PCs:

- **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 device blocks all traffic between the wired PC and all wireless PCs.

#### Prevent a wireless PC from communicating with the wired network

Configure the following settings to prevent wireless PC 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 device blocks all traffic between wireless PC 3 and the Ethernet network.

#### 5.10.2.1 Static MAC Address Filter Configuration

To configure Static MAC Filter parameters, navigate to **ADVANCED CONFIGURATION > Filtering > Static MAC Address Filter**. The **Static MAC Address Filter** screen appears:

S.No.	Wired MAC Address	Wired MAC Mask	Wireless MAC Addr	Wireless MAC Mask	Comment	Entry Status
1	00:40:f4:1c:db:6a	ff:ff:ff:ff:ff:ff	00:02:2d:51:94:e4	ff:ff:ff:ff:ff:ff	Test	Enable
2	00:40:f4:1c:db:6a	ff:ff:ff:00:00:00	00:02:2d:51:94:e4	ff:ff:ff:00:00:00	Test	Enable

Figure 5-63 Static MAC Address Filter

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

Figure 5-64 Static MAC Address Filter Add Row

Tabulated below is the table which explains Static MAC Address Filter parameters and the method to configure the configurable parameter(s):

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 <b>Static MAC Filter</b> table entry.
Status	Specifies the status of the newly created filter.

Click **Add** and then **COMMIT**.



- A maximum of 200 MAC address filters can be added.
- The Wired MAC address and the Wireless MAC address should be a unicast MAC address.
- The MAC Address or Mask includes 12 hexadecimal digits (each hexadecimal equals to 4 bits containing 0 or 1) which is equivalent to 48 bit identifier.

### 5.10.3 Advanced Filtering

With Advanced Filtering, you can filter pre-defined IP Protocol traffic on the network.

By default, 5 IP protocols are pre-defined and based on the configuration they can be blocked or allowed to enter the network.

To apply filters on the IP protocols, navigate to **ADVANCED CONFIGURATION > Filtering > Advanced Filtering**. The **Advanced Filtering** screen appears:

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

There is an 'Edit' button at the bottom left of the table.

Figure 5-65 Advanced Filtering

The Advanced Filtering table contains a list of 5 pre-defined protocols on which Advanced Filtering is applied. The following table explains the Filtering table parameters:

Parameter	Description
Protocol Name	Represent the protocol name. By default, Advanced Filtering is supported on the following 5 default protocols: <ul style="list-style-type: none"> <li>• Deny IPX RIP</li> <li>• Deny IPX SAP</li> <li>• Deny IPX LSP</li> <li>• Deny IP Broadcasts</li> <li>• Deny IP Multicasts</li> </ul>
Direction	Represents the direction of an IP Protocol traffic that needs to be filtered. The directions that can be filtered are, <ul style="list-style-type: none"> <li>• Ethernet to wireless</li> <li>• Wireless to ethernet</li> <li>• Both</li> </ul>
Entry Status	If enabled, then filtering is applied on the IP protocol else not applied.



- The Advanced Filtering table contains a maximum of 5 pre-defined IP protocols.
- User-defined IP protocols cannot be added to the Advanced Filtering table.

#### 5.10.3.1 Edit Advanced Filtering Table Entries

To edit Advanced Filtering table protocols, click **Edit** in the **Advanced Filtering** screen. The **Advanced Filtering - Edit Entries** screen appears.

Name	Direction	Status
Deny IPX RIP	Both	Disable
Deny IPX SAP	Both	Disable
Deny IPX LSP	Both	Disable
Deny IP Broadcasts	Both	Disable
Deny IP Multicasts	Both	Disable

**Figure 5-66 Advance Filtering- Edit Entries**

Modify the IP protocol traffic direction that needs to be filtered, and the filtering status for the desired IP Protocol. Next click **OK** and then **COMMIT**.

#### 5.10.4 TCP/UDP Port Filter

TCP/UDP Port Filtering allows you to enable or disable Transmission Control Protocol (TCP) ports and User Datagram Port (UDP) ports on network devices. A user specifies a Protocol Name, Port Number, Port Type (TCP, UDP, or TCP/UDP), and filtering interfaces (Only Wireless, Only Ethernet or Both) in order to block access to services such as Telnet and FTP, and traffic such as NETBIOS and HTTP.

To apply filters on TCP/UDP Port, navigate to **ADVANCED CONFIGURATION > Filtering > TCP/UDP Port Filter**. The **TCP/UDP Port Filter** screen appears.

S.No.	Protocol Name	Port Number	Port Type	Filter Interface	Entry Status
1	NetBios Name S	137	Both	All Interface	Disable
2	NetBios Datagram	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 5-67 TCP/UDP Port Filter

The **Filter Control** parameters determines if filter has to be applied or not on a TCP/UDP Port. By default, it is disabled. To apply filters, select **Enable** and click **OK**.

#### 5.10.4.1 TCP/UDP Port Filter Table

The TCP/UDP Port Filter table displays a list of default TCP/UDP ports and user-defined ports which can be enabled or disabled as desired. By default, the device support 7 default TCP/UDP port filter entries.

Parameter	Description
Protocol Name	The name of the service/protocol. Please note that the system throws an error when an attempt is made to edit the default service/protocol name.
Port Number	Represents the destination port number. Please note that the system throws an error when an attempt is made to edit the port number.
Port Type	Represents the port type (TCP, UDP, Both).
Filter Interface	Represents the interface on which the filter is applied. The supported interfaces are, <ul style="list-style-type: none"> <li>• Only Ethernet</li> <li>• Only Wireless</li> <li>• All Interfaces</li> </ul>
Entry Status	Set the entry status as either Enable, Disable or Delete. <ul style="list-style-type: none"> <li>• <b>Enable</b>: Filter is applied and filters the packet based on the Port number and port type.</li> <li>• <b>Disable</b>: No filter is applied.</li> <li>• <b>Delete</b>: Allows to delete only user-defined TCP/UDP port filter entry. When you attempt to delete default entries, the device throws an error.</li> </ul>

If you have configured any user-defined protocols then click **OK** and then **COMMIT**.

For example, a device with the following configuration would discard frames received on its Ethernet interface with a UDP destination port number of 137, effectively blocking NETBIOS Name Service packets. Please note that even the Filtering Control should be enabled to apply the filter.

Protocol Name	Port Number	Port Type	Filter Interface	Entry Status (Enable/Disable)
NETBIOS Name Service	137	UDP	Ethernet	Enable

#### 5.10.4.2 Adding User-defined TCP/UDP Port Filter Entries

To add user-defined TCP/UDP port filter entries to the table, click **Add** in the **TCP / UDP Port Filter** screen. The **TCP/UDP Port Filter Add Row** screen appears:

The screenshot shows a configuration window titled "TCP / UDP Port Filter Add Row". It contains the following fields and values:

- Protocol Name: TEST\_PORT
- Port Number: 50000
- Port Type: TCP (dropdown menu)
- Filter Interface: Only Ethernet (dropdown menu)
- Table Status: Enable (dropdown menu)

At the bottom of the form, there are two buttons: "Add" and "Back".

Figure 5-68 Add User-defined TCP/UDP Protocols

Provide details for all the parameters and click **Add**.

To apply the configured parameters, click **COMMIT**.



- The TCP/UDP filtering operation is allowed only when the **Global Flag** and **Filter Control** options are enabled.
- A maximum of 64 TCP/UDP Port Filter entries can be added to the table, out of which 7 are default entries.

#### 5.10.5 Storm Threshold Filter

The Storm Threshold Filter restricts the excessive inbound multicast or broadcast traffic on layer two interfaces. This protects against broadcast storms resulting from spanning tree misconfiguration. A broadcast or multicast filtering mechanism needs to be enabled so that a large percentage of the wireless link remains available to the connected mobile terminals.

To configure Storm Threshold Filter, navigate to **ADVANCED CONFIGURATION > Filtering > Storm Threshold Filter**. The **Storm Threshold Filter** screen appears. This screen contains information about the threshold values per second of the multicast and broadcast packets that can be processed for the interface(s) present in the device.



Figure 5-69 Storm Threshold Filter

Tabulated below is the table which explains Storm Threshold Filter parameters and the method to configure the configurable parameter(s):

Parameter	Description
Interface	Allows to configure the type of interface on which filtering has to be applied. The Storm Threshold filter can be used to filter the traffic on two types of interfaces: Ethernet or Wireless. By default, Storm Threshold filtering is disabled on both Ethernet and Wireless interfaces.
Multicast Threshold	Allows to configure the threshold value of the multicast packets to be processed for the Ethernet or Wireless interface. Packets more than threshold value are dropped. If threshold value for multicast packets is set to '0', filtering is disabled. The default <b>Multicast Threshold</b> value is 0 per second.
Broadcast Threshold	Allows to configure the threshold value of the broadcast packets to be processed for the Ethernet or Wireless interface. Packets more than threshold value are dropped. If threshold value for broadcast packets is set to '0', filtering is disabled. The default <b>Broadcast Threshold</b> value is 0 per second.

After configuring the required parameters, click **OK** and then **COMMIT**.

### 5.10.6 WORP Intra Cell Blocking



***Intra Cell Blocking is applicable only to a BSU in Bridge Mode only.***

The WORP Intra Cell Blocking feature restricts traffic between SUs which are registered to the same BSU. The two potential reasons to isolate traffic among the SUs are:

- To provide better security by isolating the traffic from one SU to another in a public space.
- To block unwanted traffic between SUs to prevent this traffic from using bandwidth.

The user can form groups of SUs at the BSU which define the filtering criteria. All data to/from SUs belonging to the same group are bridged. If a SU does not belong to any group, the BSU discards the data.

The user can also configure a Security Gateway to block traffic between SUs connected to different BSUs. All packets destined for SUs not connected to the same BSU are forwarded to the Security Gateway MAC address (configured under Security Gateway).

The following rules apply to Intra Cell Blocking Groups:

- A SU can be assigned to more than one group.
- A SU that has not been assigned to any group cannot communicate to any other SU connected to the same or different BSU.

**Example of Intra-Cell Blocking Groups**

Assume that four Intra Cell Blocking Groups have been configured on a BSU. SUs 1 through 10 are registered to the BSU.

Group1	Group2	Group3	Group4
SU1	SU2	SU6	SU8
SU4	SU3	SU1	SU9
SU5	SU8	SU7	SU10

In this example, SU1 belongs to two groups, Group 1 and Group 3. Therefore, packets from SU1 destined to SU4, SU5, SU6 and SU7 are not blocked. However, SU9 belongs to group 4 only and packets from SU9 are blocked unless sent to SU8 or SU 10.

To configuring Intra-Cell Blocking parameters, navigate to **ADVANCED CONFIGURATION > Filtering> WORP Intra Cell Blocking**. The following screen appears:



Figure 5-70 Intra Cell Blocking

This screen is classified into two categories: **Intra Cell Blocking** and **Security Gateway**. Tabulated below are the configuration details.

Parameter	Description
<b>Intra Cell Blocking</b>	
Status	By default, Intra Cell Blocking is disabled on a BSU. Select <b>Enable</b> to enable the feature and then Click <b>OK</b> and then <b>COMMIT</b> .
<b>Security Gateway</b>	
Status	By default, Security Gateway is disabled on a BSU. Select <b>Enable</b> to enable the feature.

Parameter	Description
MAC Address	Represents the MAC address of the security gateway. This gateway routes the packets transmitted by the SU to the different BSUs to which it belongs.
After configuring the required parameters, click <b>OK</b> and then <b>COMMIT</b> .	



Intra Cell Blocking is configurable only in Bridge mode. When you change the device from **Bridge** to **Routing** mode or vice-versa, Intra-Cell Blocking stops or starts working only after a **Reboot**.

### 5.10.6.1 WORP Intra Cell Blocking Group Table

The user can form groups of SUs at the BSU which define the filtering criteria. All data to/from SUs belonging to the same group are bridged. If a SU does not belong to any group, the BSU discards the data.

By default, a BSU supports 16 groups and each group can contain a maximum of 240 SUs. Please note that a single SU can be a member of all the existing groups.

To view and configure the Intra Cell Blocking Group table, navigate to **ADVANCED CONFIGURATION > Filtering > WORP Intra Cell Blocking > Group Table**. The **WORP Intra Cell Blocking Group Table** screen appears:

S.No.	Group Name	Entry Status
1	grpID1	Disable
2	grpID2	Disable
3	grpID3	Disable
4	grpID4	Disable
5	grpID5	Disable
6	grpID6	Disable
7	grpID7	Disable
8	grpID8	Disable
9	grpID9	Disable
10	grpID10	Disable
11	grpID11	Disable
12	grpID12	Disable
13	grpID13	Disable
14	grpID14	Disable
15	grpID15	Disable
16	grpID16	Disable

OK

Figure 5-71 WORP Intra Cell Blocking Group Table

This table displays the list of groups. If the Entry Status for a group is set to **Enable** then BSU discards all the packets coming from SUs which are not members of that group. If set to Disable, then allows all the packets coming from SUs which are not the members of that group. If you have changed the Entry Status of a group, then click OK and then **COMMIT**.

**5.10.6.2 WORP Intra Cell Blocking MAC Table**

The WORP Intra Cell Blocking MAC table allows to add SU's MAC address and assign them to the groups. A maximum of 250 SUs can be added to the table.

To add SU to the table, navigate to **ADVANCED CONFIGURATION > Filtering > WORP Intra Cell Blocking > MAC Table**. The **WORP Intra Cell Blocking MAC Table** screen appears:



Figure 5-72 WORP Intra Cell Blocking MAC Table

To add MAC addresses, click **Add**. The following screen appears.

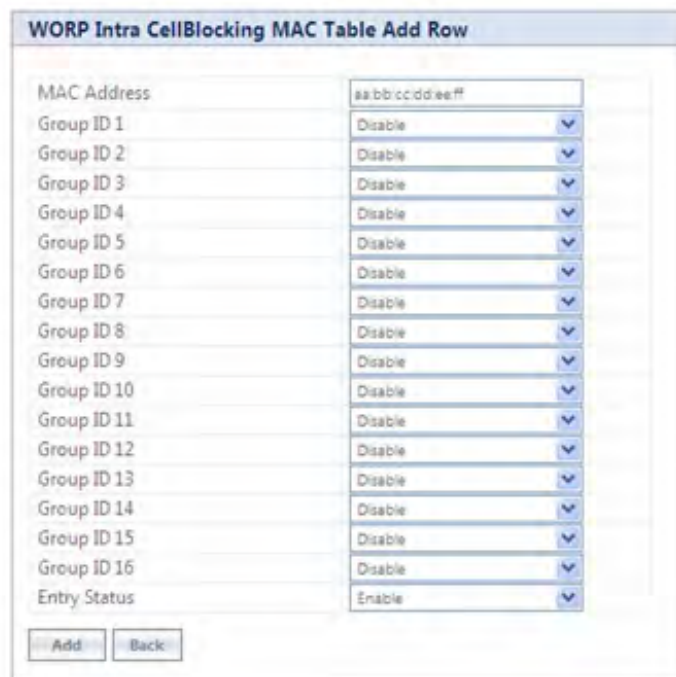


Figure 5-73 WORP Intra Cell Blocking MAC Table Add Row

Tabulated below is the table which explains the WORP Intra Cell Blocking MAC Table entries and the method to configure the configurable parameter(s):

Parameter	Description
MAC Address	Represents the SU's MAC address.
Group ID's 1 to 16	By default, a Group ID is disabled meaning which the SU is not a part of that group. To make it a part of that group, select <b>Enable</b> .
Entry Status	If SU is part of a group and its Entry Status is enabled then it can communicate with all the SUs belonging to that group. If Entry Status is disabled, then the communication is blocked.

After adding the MAC address, click **Add**.

To edit the existing MAC addresses, click **Edit** icon in the **WORP Intra Cell Blocking MAC Table** screen. Modify the parameters as desired in the **WORP Intra Cell Blocking MAC Table Add Row** screen and click **OK** and then **COMMIT**.

In the **WORP Intra Cell Blocking MAC Table**, you can change the Entry Status as either Enable/Disable/Delete. Once the status is changed, click **OK** and then **COMMIT**.

## 5.11 DHCP

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to assign an IP address to the DHCP client from a defined range of IP addresses configured for a given network. Allocating IP addresses from a central location simplifies the process of configuring IP addresses to individual DHCP clients, and also avoids IP conflicts.

### 5.11.1 DHCP Pool

DHCP Pool is a pool of defined IP addresses which enables a DHCP Server to dynamically pick IP address from the pool and assign it to the DHCP client.

To configure a range of IP addresses in the DHCP Pool, navigate to **ADVANCED CONFIGURATION > DHCP > DHCP Server > Pool**. The **DHCP Pool** screen appears:

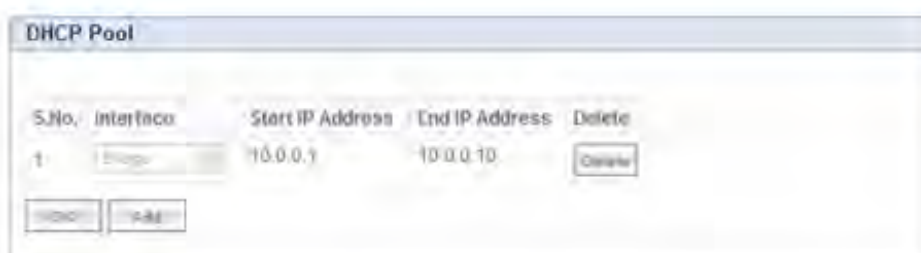


Figure 5-74 DHCP Pool

Each pool entry comprises the following tabulated information:

Parameter	Description
Interface	Specifies the interface type, that is, Bridge or Routing (Ethernet and Wireless).
Start IP Address and End IP Address	Specifies the start and end IP address of the addresses to be added to the pool.
Delete	Allows you to delete a pool entry.



: A maximum of five pool entries can be added to the table. A pool entry can be deleted but cannot be edited.

### 5.11.1.1 Adding a New Pool Entry

To add a new entry to the DHCP Pool, click **Add** on the **DHCP Pool** screen. The following **DHCP Pool Table Add Row** screen appears:

Figure 5-75 DHCP Pool Table Add Row

Enter the pool details and click **Add**. The entry will be updated in the DHCP pool table. To apply the configured changes, click **COMMIT**.

### 5.11.2 DHCP Server

If DHCP Server is enabled, it picks automatically the IP addresses from the specific interface address pool and assigns them to the respective DHCP clients.

DHCP Server feature is applicable to both **Bridge** and **Routing** Mode. In Routing mode, DHCP Server can be configured for each interface (Ethernet and Wireless) 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.

To configure the DHCP server parameters, navigate to **ADVANCED CONFIGURATION > DHCP > DHCP Server > Interface**. The **DHCP Server** screen appears:

S.No.	Interface	Net Mask	Default Gateway	Primary DNS	Secondary DNS	Default Lease Time (secs)	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).

Figure 5-76 DHCP Server

Tabulated below is the table which explains DHCP Server parameters and the method to configure the configurable parameter(s):

Parameter	Description
DHCP Server Status	By default, DHCP Server is disabled on a device. To enable DHCP Server, select <b>Enable</b> .  A DHCP Server can be enabled only when the following two conditions are satisfied: 1. Before enabling, atleast one interface should be enabled on which the DHCP Server has to run. 2. The DHCP pool table should have atleast one pool configured for that interface.
Max Lease Time	Specifies the maximum lease time for which the DHCP client can use the IP address provided by the DHCP Server. The value ranges from 3600 - 172800 seconds.
<b>DHCP Interface Table</b>	
Interface Type	Specifies the interface for which the DHCP Server functionality shall be configured. That is Bridge or Ethernet/Wireless in case of Routing mode.
Net Mask	Specifies the subnet mask to be sent to the DHCP 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 DHCP client along with the 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 DHCP client.
Secondary DNS	Specifies the secondary DNS IP address to be sent to the DHCP client.
Default Lease Time	DHCP Server uses this option to specify the lease time it is willing to offer to the DHCP client over that interface. Once the lease time expires, the DHCP Server allocates a new IP address to the device. The <b>Default Lease Time</b> should be less than or equal to the configured <b>Max Lease Time</b> .
Comment	Specifies a note for the device administrator.
Entry Status	Used to <b>Enable</b> or <b>Disable</b> the DHCP Server functionality over the interface.

After configuring the required parameters, click **OK** and then **COMMIT**.

### 5.11.3 DHCP Relay (Routing Mode only)

The DHCP relay agent forwards DHCP requests to the configured DHCP Server. A maximum of 5 DHCP Servers can be configured. There must be at least one DHCP Server configured in order to relay DHCP request.



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

To view and configure DHCP Relay Server parameters, navigate to **ADVANCED CONFIGURATION > DHCP > DHCP Relay > Relay Server**. The **DHCP Relay** screen appears:

**DHCP Relay**

DHCP Relay Status:

**DHCP Relay Server Table**

S.No.	IP Address	Delete
1	169.254.128.160	<input type="button" value="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.

Figure 5-77 DHCP Relay

By default, DHCP Relay is disabled on the device. To enable it, atleast one DHCP Server IP address should be configured.

To add a DHCP Server to the Relay Server Table, click **Add** in the **DHCP Relay** screen. The **DHCP Relay Server Add Row** screen appears:

**DHCP Relay Server Add Row**

Server IP Address:

Entry Status:

Figure 5-78 DHCP Relay Server Add Row

Enter the DHCP Server IP Address and then click **Add**.

After configuring the required parameters, click **OK** and then **COMMIT**.



: DHCP server is disabled automatically if DHCP Relay agent is enabled and vise-verse.

## 5.12 IGMP Snooping

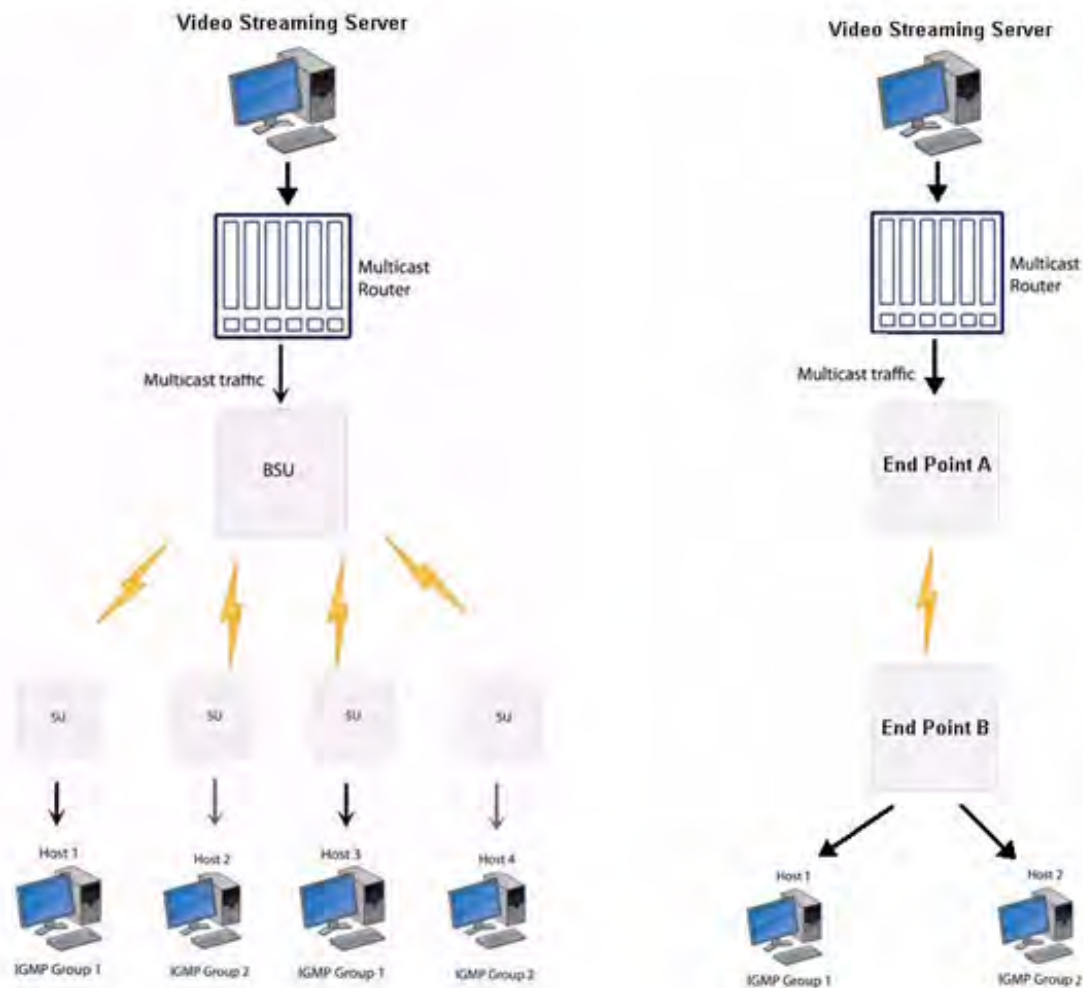


***IGMP Snooping is applicable only in a Bridge Mode.***

Proxim's Tsunami® devices support Internet Group Management Protocol (IGMP) Snooping feature. With IGMP Snooping enabled on the device, multicast traffic is only forwarded to ports that are members of the specific multicast group. By forwarding the traffic only to the destined ports, reduces unnecessary load on devices to process packets.

Explained below is the IGMP Snooping process with the help of a diagram:





**Figure 5-79 IGMP Snooping Process**

The router forwards the IP multicast data to the BSU/End Point A.

Lets say, with IGMP Snooping not enabled on the BSU/End Point A, the multicast data is transmitted over the wireless medium irrespective of whether the multicast group address is a member of the multicast group table maintained in each BSU/End Point A. With IGMP Snooping enabled, the BSU/End Point A transmits the data only when the multicast group address is a member of the multicast group table, else drops the packet. The SU/End Point B will receive the multicast data.

Similarly, with IGMP Snooping not enabled on the SU/End Point B, the multicast data is transmitted irrespective of whether the multicast group address is a member of the multicast group table maintained in each SU/End Point B. With IGMP Snooping enabled, the SU/End Point B transmits the data to the host only when the multicast group address is a member of the multicast group table, else drops the packet.

IGMP Snooping is of 2 kinds:

- **Active:** Active IGMP Snooping listens to IGMP traffic and filters IGMP packets to reduce load on the multicast router.
- **Passive:** Passive IGMP Snooping simply listens to IGMP traffic and does not filter or interfere with IGMP.



- Tsunami® devices supports only passive IGMP Snooping.
- IGMP versions v1,v2 and v3 are supported.
- The device can add a maximum of 64 Multicast groups in the Snooping table.

To configure IGMP Snooping parameters, navigate to **ADVANCED CONFIGURATION > IGMP Snooping**. The following **IGMP Snooping** screen appears:

**Figure 5-80 IGMP Snooping**

Tabulated below is the table which explains IGMP Snooping parameters and the method to configure the configurable parameter(s):

Parameter	Description
IGMP Snooping Status	By default, IGMP Snooping Status is disabled on the device, meaning which, the device transmits IP multicast traffic to all the ports. To forward the traffic only to the members of the specific multicast group, enable IGMP Snooping Status.
IGMP Membership Aging Timer	Represents the time after which the IGMP multicast group age-outs or elapses. It ranges from 135 to 635 seconds. The default Aging Timer is <b>260 seconds</b> .
IGMP Router Port Aging Timer	Represents the time after which the IGMP Router port age-outs or elapses. It ranges from 260 to 635 seconds. The default Aging Timer is <b>300 seconds</b> .
IGMP Forced Flood	If you select <b>Yes</b> , all the unregistered IPv4 multicast traffic (with destination address which does not match any of the groups announced in earlier IGMP Membership reports) and IGMP Membership Reports will be flooded to all the ports. By default, IGMP Forced Flood is set to <b>No</b> .

After configuring the required parameters, click **OK** and then **COMMIT**.

## 5.13 Routing Mode Features

This section provides an overview of all the features applicable in routing mode only.

### 5.13.1 Static Route Table

The Static Route Table stores the route to various destinations in the network. When packets are to be routed, the routing table is referred for the destination address.

To configure the static routing table, navigate to **ADVANCED CONFIGURATION > Network > Static Route Table**. The **Static Route Table** screen appears.

S.No.	Destination Address	Subnet Mask	Route Next Hop	Admin Metric	Entry Status
1	10.0.0.0	255.0.0.0	169.254.128.101	4	Enable
2	169.254.150.0	255.255.255.0	169.254.130.101	5	Enable

**Figure 5-81 Static Route Table**

Tabulated below is the table which explains Static Route Table entries and the method to configure the configurable parameter(s):

Parameter	Description
Static Route Status	If Static Route Status is enabled, the packets are sent as per route configured in the static routing table. If disabled, forwards the packet to the default gateway.
Destination Address	Represents the destination IP address to which the data has to be routed.
Subnet Mask	Represents the subnet mask of the destination IP address to which the data has to be routed.
Route Next Hop	Represents the IP address of the next hop to reach the destination IP address. Next hop IP should belong to at least one of the subnets connected to the device.
Admin Metric	It is a metric that specifies the distance to the destination IP address, usually counted in hops. The lower the metric, the better. The metrics can range from 0 to 16.
Entry Status	If enabled, considers the packets for routing. If disabled, forwards the packet to the default gateway.

### 5.13.1.1 Adding Static Route Entries

Click **Add** in the **Static Route Table** screen. The following **Static Route Table Add Row** screen appears:

The screenshot shows a web-based configuration form titled "Static Route Table Add Row". It contains the following fields and values:

- Destination Address: 169.254.150.0
- Subnet Mask: 255.255.255.0
- Route Next Hop: 169.254.130.101
- Metric: 1 (with a range of 0-16 indicated to the right)
- Entry Status: Enable (with a dropdown arrow)

At the bottom of the form, there are two buttons: "Add" and "Back".

Figure 5-82 Static Route Table Add Row

Add the route entries and click **Add** and then **COMMIT**.



- A maximum of 256 routes can be added to the static route table.
- The IP address of the Next Hop must be on the subnet of one of the device's network interfaces.

### 5.13.2 Network Address Translation (NAT)



**NAT is applicable only to a SU and an End Point B.**

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

The SU/End Point B device supports Network Address Port Translation (NAPT) feature, where all the private IP addresses are mapped to a single public IP address.

The SU/End Point B device supports 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/End Point B 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. A maximum of 100 entries are supported in the static port bind table.
2. **Dynamic NAT:** In dynamic mapping, the SU/End Point B 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.



- When NAT is enabled, the network on the wireless side of the device is considered public and the network on the Ethernet side is 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 configure NAT parameters, navigate to **ADVANCED CONFIGURATION > Network > NAT**. The following **NAT** screen appears:

**NAT**

Status: Disable

Dynamic Start Port: 1 (1-65535)

Dynamic End Port: 65535 (1-65535)

Port Forwarding Status: Disable


**Notes:**

1. To enable NAT RIP must be disabled.
2. To enable NAT DHCP Relay Agent must be disabled.
3. When NAT is enabled the Wireless interface side is the Public network and the Ethernet interface side is the Private.
4. It is recommended that Dynamic port range and Static port range do not overlap.
5. \* Reboot is required

OK

Figure 5-83 NAT

Tabulated below is the table which explains NAT parameters and the method to configure the configurable parameter(s):

Parameter	Description
Status	This parameter is used to either <b>enable</b> or <b>disable</b> NAT on a SU or an End Point A.
Dynamic Start Port and Dynamic End Port	Represents the start and end port sessions originated from private to public host.  By default, the Dynamic Start Port is configured to <b>1</b> and Dynamic End Port is configured to <b>65535</b> . Configure the start and end port as desired.   Care should be taken to avoid overlap of Dynamic Port range and Static Port range.
Port Forwarding Status	This parameter is used to either <b>enable</b> or <b>disable</b> the <b>Static NAT</b> feature within different networks. It allows public hosts to access hosts in a private network. By default, it is disabled.

After configuring the required parameters, click **OK** and then **COMMIT**.




- To enable **Dynamic NAT**, set the **NAT Status** to **Enable**. To enable **Static NAT**, set the **NAT Status** to **Enable** and the **Port Forwarding Status** to **Enable**.
- NAT uses the IP address of the wireless interface as the Public IP address.

To add entries in the **NAT Port Bind Table**, navigate to **ADVANCED CONFIGURATION > Network > NAT > Static Port Bind**. The **NAT Port Bind Table** screen appears. Click **Add** in the **NAT Port Bind Table** screen. The following **NAT Port Bind Table Add Row** appears:

**Figure 5-84 NAT Port Bind Table Add Row**

Tabulated below is the table which explains the NAT Port Bind Table entries and the method to configure the configurable parameter(s):

Parameter	Description
Local Address	Enter the local IP Address of the host on the Ethernet (private) side of the SU/End Point B.
Port Type	Select the Port Type as: <b>TCP</b> , <b>UDP</b> , or <b>Both</b> .
Start and End Port Number	Represents the start and end port for transferring the data from public to private host.  : Care should be taken to avoid overlap of Dynamic Port range and Static Port range.
Entry Status	If enabled, the data is transferred from the public network to the private host, on the specified ports.

After configuring the required parameters, click **ADD** and then **COMMIT**.

### 5.13.2.1 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/End Point B. The following table lists the 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

S.No.	Protocol	Support	Applications
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	SNMP	SNMP ALG	Network Management
10	DNS	Port Mapping for inbound connection	Domain Name Service

### 5.13.3 RIP

Routing Information Protocol (RIP) is a dynamic routing protocol, which can be used to automatically propagate routing table information between routers. The device 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.



: RIP is configurable only when the devices are in Routing Mode and Network Address Translation (NAT) is disabled.

To configure RIP parameters, navigate to **ADVANCED CONFIGURATION > Network > RIP**. The following **RIP** screen appears:

S.No.	Name	Status	Authorization Type	Authorization Key	Version Number	Direction
1	Ethernet 1	Enable	md5	*****	v2	Rx and Tx
2	Ethernet 2	Disable	Simple	*****	v2	Rx and Tx
3	Wireless 1	Disable	None		v2	Rx and Tx

Notes : 1. To enable RIP, NAT must be disabled.  
2. Auth. Type & Key are valid for V2 version only  
3. If Auth. Type is "None" Auth. Key is ignored.

Figure 5-85 RIP

By default, RIP is not enabled on the device. To enable, select **Enable** and click **OK**. The RIP screen is updated with the following tabulated parameters:

Parameter	Description
Name	Displays the interface type as either <b>Ethernet 1</b> , <b>Ethernet 2</b> , or <b>Wireless</b> .
Status	Enables you to either enable or disable RIP for a particular network interface.

Parameter	Description
Authorization Type	Enables you to select the appropriate Authorization Type. This parameter is not applicable if <b>RIP v1</b> is selected as the <b>Version number</b> .
Authorization Key	Enter the authorization key. This parameter is not applicable if <b>RIP v1</b> is selected as the <b>Version number</b> . It is not applicable when the Authorization Type is set to <b>None</b> .
Version Number	Select RIP Version number from the <b>Version Number</b> list. Available options are <b>V1</b> , <b>V2</b> and <b>both</b> . The default is <b>V2</b> .
Direction	You can enable RIP for both receiving and transmitting the data. To enable RIP only for Receiving, select <b>Rx Only</b> . To enable RIP for both receiving and transmitting, select <b>Rx and Tx</b> .

After configuring the required parameters, click **OK** and then **COMMIT**.



- **Authorization Type** and **Authorization Key** are valid only for RIPV2 and both versions.
- The maximum metric of a RIP network is 15 hops, that is, 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 or 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.

#### 5.13.4 PPPoE End Point (SU Only)

Proxim's SU devices support **Point-to-Point Protocol over Ethernet (PPPoE)** which is a network protocol for transmitting PPP frames over Ethernet. This feature is commonly used by Internet Service Providers (ISPs) to establish a Digital Subscriber Line (DSL) Internet service connection with clients.

The Proxim's SU devices support PPPoE only when they are configured in **Routing Mode** with NAT enabled. Also, the BSU should always operate in **Bridge Mode**.

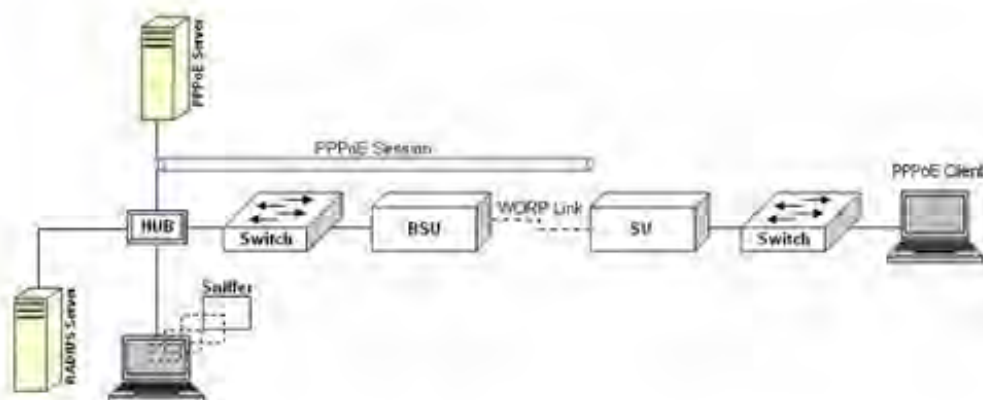


Figure 5-86 PPPoE Architecture

Given below are the stages for a PPPoE client to establish link with the PPPoE server and then transfer PPP frames over Ethernet:



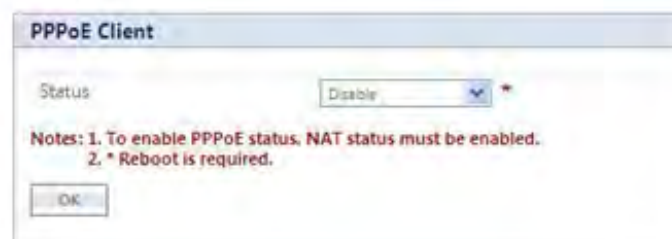
- **Discovery and Session Stage:** In this stage, to initiate a PPPoE session, the PPPoE client discovers a PPPoE server (called Access Concentrator). Once discovered, a session ID is assigned and a session is established.
- **Point-to-point Protocol (PPP) Stages:** The PPP stage comprises the following sub-stages:
  1. **Physical Link:** For sending and receiving PPP frames, the PPP driver calls the services of PPP Channels (used in connection with serial links). A PPP channel encapsulates a mechanism for transporting PPP frames from one machine to another and then the frames are forwarded on the physical Ethernet link.
  2. **Link Establishment:** In this stage, Link Configuration Protocol (LCP) performs the basic setup of the link. As part of this setup, the configuration process is undertaken whereby the PPPoE client and the server negotiate and agree on the parameters on how data should be passed between them. Only when both the client and server come to an agreement, the link is considered to be open and will proceed to the Authentication stage.
  3. **Authentication:** In this stage, LCP invokes an authentication protocol (PAP/CHAP/MS CHAP v2/EAP-MD5) when PPP is configured to use authentication.
  4. **Encryption:** In this stage, both PPPoE client and server negotiate the encryption protocol configuration. Our device support MPPE as encryption protocol. MPPE is negotiated within option 18 in the PPP Compression Control Protocol (CCP).
  5. **Network Layer Protocol:** After successful authentication, the link proceeds to the Network-Layer Protocol stage. In this stage, the specific configuration of the appropriate network layer protocol is performed by invoking the appropriate Network Control Protocol (NCP) such as IPCP. We support only IPCP Protocol as a part of NCP.

Given below are the features supported by PPPoE client:

- Preferred Server Configuration by using Access Concentrator Name/Service Name
- PAP/CHAP/MSCHAP v2/EAP-MD5 Authentication Protocols
- IP Configuration: Static IP/ PPPoE-IPCP
- Echo Interval and Echo Failure to detect server unavailability
- MPPE with stateful and stateless mode aligned with 40/56/128 bit encryption

To configure PPPoE feature,

1. Navigate to **ADVANCED CONFIGURATION > Network > PPPoE > PPPoE Client**. The following **PPPoE Client** screen appears:



**Figure 5-87 PPPoE Client Status**

2. By default, the PPPoE feature is disabled on the client. To enable, select **Enable** from **Status** drop-down box.
3. Next, click **OK**. Please note that a change in the PPPoE client status requires you to reboot the device.
4. On enabling the PPPoE client feature, the following screen appears:

### PPPoE Client


Status	Enable	*
Authentication Protocol	MSCHAPv2	
LCP Echo Interval	30	(5-300) secs
LCP Echo Failure	5	(1-25)
Preferred Service Name		(0-32) characters
Access Concentrator Name		(0-32) characters
User Name	guestuser	(4-32) characters
Password	*****	(6-32) characters
MPPE Status	Mandatory	
Stateless Encryption Mode	Disable	
MPPE Key Length	128 Bit	
Link Status	Disconnected	




**Notes:** 1. To enable PPPoE status, NAT status must be enabled.  
 2. \* Reboot is required.  
 3. PPPoE client will accept responses from all servers, if Preferred Service Name and Access Concentrator Name are left empty. Else it will filter out the responses based on those fields.  
 4. PPPoE Client Authentication Protocol is not negotiable. If pppoe server doesn't support it, then tunnel will not be established.  
 5. MPPE parameters are only configurable when the authentication protocol selected is MSCHAPv2.  
 6. Enabling stateless mode increases per-packet processing hence degrades the performance of ppp link, it should be used only in case of noisy conditions.


Figure 5-88 PPPoE Client Configuration

5. Tabulated below is the table which explains PPPoE client parameters and the method to configure the configurable parameter(s):

Parameter	Description
Authentication Protocol	<p>PPPoE supports the following types of user authentication protocols that provide varying levels of security:</p> <ul style="list-style-type: none"> <li>• <b>None:</b> Represents that no authentication is required for transferring PPP frames over Ethernet between PPPoE client and server.</li> <li>• <b>Password Authentication Protocol (PAP):</b> PAP is an access control protocol used to authenticate client's password on the server. The server requests a password from the client and sends the retrieved password to an authentication server for verification. As an authentication protocol, PAP is considered the least secure because the password is not encrypted in transmission.</li> <li>• <b>Challenge Handshake Authentication Protocol (CHAP):</b> CHAP is similar to PAP with several unique characteristics. Instead of requesting a password, the server sends a challenge message to the client. The challenge message is a random value. The client encrypts the challenge message with user's password and sends the combination back to the server. The server forwards the challenge/password combination to the authentication server. The authentication server encrypts the challenge with the user's password stored in the authentication database. If the user's response is a match, the password is considered authentic. CHAP uses the model of a shared secret (the user password) to authenticate the user. The use of CHAP is considered a moderately secure method of authentication.</li> <li>• <b>Microsoft Challenge-Handshake Authentication Protocol version 2 (MSCHAP v2):</b> MSCHAP V2 is a mutual authentication method that supports password-based user or computer authentication. During the MSCHAP v2 authentication process, both the client and the server prove that they have knowledge of the user's password for authentication to succeed. Mutual authentication is provided by including an authenticator packet returned to the client after a successful server authentication. This method is proprietary to the Microsoft and is mostly used in windows servers and client.</li> <li>• <b>EAP-MD5:</b> EAP-MD5 enables a server to authenticate a connection request by verifying an MD5 hash of a user's password. The server sends the client a random challenge value, and the client proves its identity by hashing the challenge and its password with MD5.</li> </ul> <p>By default, the authentication protocol is set to <b>CHAP</b>. You can configure the authentication protocol to the desired one and click <b>OK</b>.</p>
LCP Echo Interval	<p>To check the link connection, periodically the PPPoE client sends an LCP echo-request frame to the PPPoE server. If the PPPoE server respond to the echo-request by sending an echo-reply, then the connection is alive.</p> <p>To configure LCP Echo Interval, enter a time ranging from 5 to 300 seconds. By default, the echo interval is set to <b>30 seconds</b>.</p>

Parameter	Description
LCP Echo Failure	<p>This parameter indicates the maximum number of consecutive failures to receive the LCP echo-reply to consider the connection to be down.</p> <p>To configure LCP Echo Failure value, enter a a value ranging from 1 to 25. By default, the echo failure is set to 5. On a noisy wireless link, it is recommended to set this value to higher.</p>
Preferred Service Name	<p>Specifies the service which the PPPoE server (Access Concentrators) provides to the PPPoE client.</p> <p>Leave this parameter blank, if PPPoE client accepts any service offered by the PPPoE server. To specify the desired service name, enter the service name ranging from 1 to 32 characters.</p>
Access Concentrator Name	<p>Specifies Access Concentrator (PPPoE server) name.</p> <p>Leave this parameter blank, when PPPoE client can connect to any PPPoE server on the network. To connect to a desired PPPoE server, type the server name ranging from 1 to 32 characters.</p>
User Name and Password	<p>Before establishing a link, the PPPoE server first authenticates the PPPoE client based on the User Name and Password as shared by the service provider.</p> <p>Type the user name and password in the <b>User Name</b> and <b>Password</b> box respectively. You can type user name ranging from 4 to 32 characters and password ranging from 6 to 32 characters.</p> <p> : User Name and Password parameters are not applicable when the Authentication Protocol is configured as "None".</p>

Parameter	Description
MPPE Status	 : MPPE Status parameter is applicable only when the Authentication Protocol is configured as "MSCHAP v2".  Microsoft Point-to-Point Encryption (MPPE) is a protocol for transferring encrypted data over point-to-point links. The PPPoE client negotiates on the encryption parameters based on the MPPE Status configured.  The MPPE Status can be configured as following: <ul style="list-style-type: none"> <li>• <b>Mandatory</b>: When the MPPE status is configured as <b>Mandatory</b>, the PPPoE client negotiates the configured MPPE parameters with the PPPoE server. If the server does not agree to the parameters then the link will not be established.</li> <li>• <b>Optional</b>: When the MPPE status is configured as <b>Optional</b>, the link is established with or without encryption depending on the PPPoE server configuration. If the PPPoE server supports MPPE encryption then the PPPoE client agrees with the PPPoE server's MPPE parameters and link gets established with encryption. If the PPPoE server does not support MPPE encryption then link gets established without encryption.</li> <li>• <b>Disable</b>: When the MPPE status is configured as <b>Disable</b>, then the PPPoE client does not agree to the MPPE parameters suggested by the PPPoE server.</li> </ul> Configure the desired status and click <b>OK</b> .
Stateless Encryption Mode	 : This parameter is applicable only when <b>Authentication Protocol</b> is configured as "MSCHAP v2" and <b>MPPE Status</b> is configured as "Mandatory".  When stateless encryption is negotiated, the session key changes for every packet transferred. In stateless mode, the sender must change its key before encrypting and transmitting each packet and the receiver must change its key after receiving, but before decrypting, each packet.  When stateful encryption is negotiated, the PPPoE server and the client monitor the synchronization of MPP encryption engine on both the sides. When one of the peer detects that they are out of sync then the peer should transmit a packet with the coherency count set to 0xFF(a flag packet); the sender must change its key before encrypting and transmitting any packet and the receiver must change its key after receiving a flag packet, but before decrypting.  To enable stateless encryption, select <b>Enable</b> . To enable stateful encryption, select <b>Disable</b> .   : Enabling Stateless Encryption impacts throughput. It is useful to enable Stateless encryption when packet drops are more in the wireless link.

Parameter	Description
MPPE Key Length	 : This parameter is applicable only when <b>Authentication Protocol</b> is configured as “MSCHAP v2” and <b>MPPE Status</b> is configured as “Mandatory”.  MPPE supports 40-bit, 56-bit and 128-bit encryption key length. To configure the desired key length, select a key length from the <b>MPPE Key Length</b> drop-down box.
Link Status	<p>Indicates the status of the PPPoE link between the PPPoE client and server.</p> <p>The link can be in any of the following three stages:</p> <ul style="list-style-type: none"> <li>• <b>Disconnected:</b> No connection is established between PPPoE client and server.</li> <li>• <b>Connecting:</b> A connection attempt is in progress between PPPoE client and server.</li> <li>• <b>Connected:</b> Connection is established between PPPoE client and server.</li> </ul> <p>The Link Status can be viewed in <a href="#">Home Page</a>.</p>

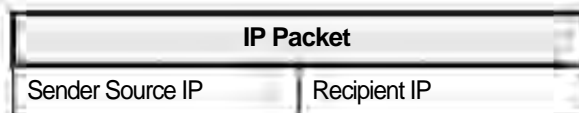
- After configuring the required parameters, click **OK** and then **COMMIT**. Reboot the device, if you have changed the PPPoE Status configuration.

### 5.13.5 IP over IP Tunneling

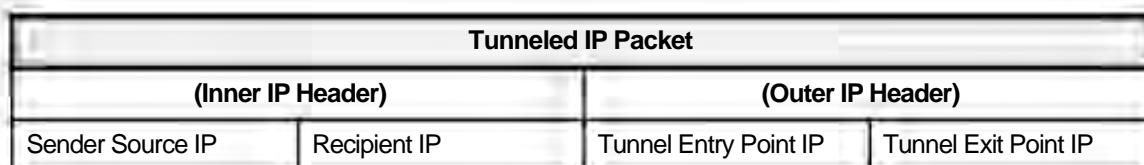
Proxim’s point-to-multipoint and point-to-point devices support IP Tunnelling, which serves as a communication channel between two disjoint IP networks that do not have a native routing path to communicate with each other.

To enable communication between two disjoint networks using IP Tunneling, the following steps are involved:

- The tunnel entry point receives the IP packet (Sender Source IP + Recipient IP) sent by the original sender.



- The tunnel entry point encapsulates the IP packet (Sender Source IP + Recipient IP) with the IP addresses of the tunnel endpoints. The tunneled packet (Sender Source IP + Recipient IP + Tunnel Entry Point IP + Tunnel Exit Point IP) is then forwarded to the tunnel exit point.



- On receiving the tunneled packet, the tunnel exit point removes the tunnel IP addresses and forwards the packet to the recipient. The inner IP header Source Address and Destination Address identify the original sender and recipient of the packet, respectively. The outer IP header Source Address and Destination Address identify the endpoints of the tunnel.

The following figure shows an IP tunnel configuration using two end points.

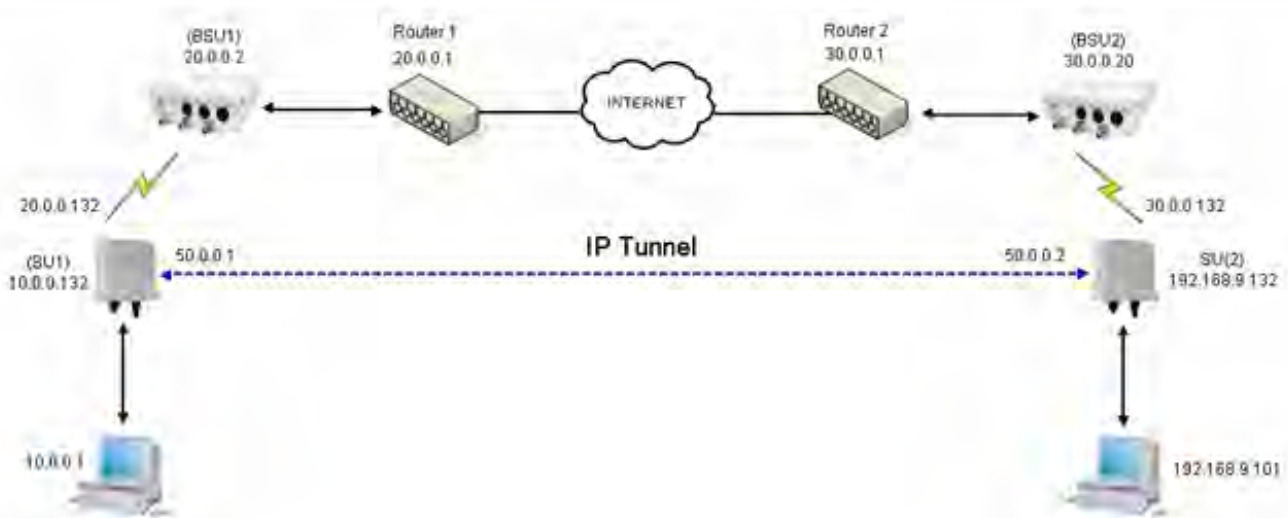


Figure 5-89 An Example: Tunnel Configuration

Lets say that the Computer with an IP address: 10.0.0.1 wants to communicate with the Computer with an IP address: 192.168.9.101. Since there is no native routing path between these two computers, the communication can happen via the tunnel. The SU1 device with wireless IP address: 20.0.0.132 and SU2 device with wireless IP address: 30.0.0.132 are the end points of the tunnel, respectively.

With IP tunneling, the tunnel entry point (SU1) encapsulates the tunnel end points IP addresses (20.0.0.132 + 30.0.0.132) with the sender IP addresses (10.0.0.1 + 192.168.9.101) before sending the data through the tunnel. When the tunnel exit point (SU2) receives traffic, it removes the outer IP header before forwarding the packet to the recipient.

IP Packet	
Sender Source IP (10.0.0.1)	Recipient IP (192.168.9.101)

Tunneled IP Packet			
(Inner IP Header)		(Outer IP Header)	
Sender Source IP (10.0.0.1)	Recipient IP (192.168.9.101)	Tunnel Entry Point IP (20.0.0.132)	Tunnel Exit Point IP (30.0.0.132)



: IP tunnel establishment does not involve any protocol message exchange. To setup an IP tunnel, the device has to be configured properly on both the ends.

By following the steps below, the tunnel is automatically established.

1. Create a tunnel (Refer to [Create a Tunnel](#))

To create a tunnel as given in [Figure 5-89](#), do the following: **SU1 Configuration**

- Virtual IP Address = 50.0.0.1
- Local IP Address = 20.0.0.132

— Remote IP Address = 30.0.0.132

### SU2 Configuration

— Virtual IP address = 50.0.0.2

— Local IP Address = 30.0.0.132

— Remote IP Address = 20.0.0.132

2. Add a Static Route for Remote IP Address of the tunnel (Refer to [Static Route Table](#))
  - On SU1, add a static route for 30.0.0.xxx as next hop 20.0.0.1
  - On SU2, add a static route for 20.0.0.xxx as next hop 30.0.0.1
3. Add a route for the pass-through traffic through the tunnel (Next Hop IP Address should be that of the tunnel interface).
  - On SU1, add a static route for 192.168.9.xxx as next hop 50.0.0.1
  - On SU2, add a static route for 10.0.0.xxx as next hop 50.0.0.2

#### 5.13.5.1 Create a Tunnel

To create a Tunnel interface,

1. Navigate to **ADVANCED CONFIGURATION > Network > IP Tunneling**. The following **IP Tunneling** screen appears:

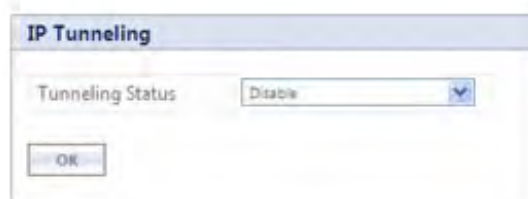


Figure 5-90 IP Tunneling Status

2. By default, the IP Tunneling feature is disabled on the device. To enable, select **Enable** from the **Tunneling Status** drop-down box.
3. Next, click **OK**.
4. On enabling the IP Tunneling feature, the following screen appears:



Figure 5-91 IP Tunneling Interfaces

5. Click **Add**, to create a new tunnel interface. The following **Tunneling Table Add Row** screen appears:



**Tunneling Table Add Row**

Name:

Encapsulation Method:

Virtual IP Address:

Local IP Address:

Remote IP Address:

TTL:  (0-255)

Entry Status:

Notes: 1. Local IP Address should be one of the interface IP address on which tunnel has to be created.  
2. Remote IP Address should be routable.

Figure 5-92 Adding a new Tunnel Interface

6. Tabulated below is the table which explains the parameters for creating a new tunnel:

Parameter	Description
Name	Represents the name of the tunnel interface. Type a name for the tunnel interface.
Encapsulation Method	The device supports two types of network tunnels: <ul style="list-style-type: none"> <li><b>ipip</b>: A tunnelling protocol that allow only IP traffic over the tunnel.</li> <li><b>gre (Generic Routing Encapsulation)</b>: A tunneling protocol that allows encapsulation of a wide variety of packet types in Internet Protocol (IP) packets, thereby creating a virtual point-to-point link.</li> </ul> Select the tunnel type as either <b>ipip</b> or <b>gre</b> .
Virtual IP Address	Represents the virtual IP address of the tunnel interface. Enter the virtual IP address of the tunnel interface.
Local IP Address	Represents the IP address of the tunnel entry point. Select the IP address of the tunnel entry point from the available list of addresses.
Remote IP Address	Represents the IP address of the tunnel exit point. Type the IP address of the tunnel exit point. Please note that the Remote IP address should be routable.
TTL	TTL stands for <b>Time to Live</b> . This parameter enables to configure a fixed TTL value on the tunneled packets. The TTL value can be configured in the range 0 to 255. By default, the TTL value is set to 0 meaning that tunneled packets inherit the TTL value from the IP packet originated by the sender.
Entry Status	By using this parameter, a tunnel interface can be enabled or disabled. By default, it is enabled. To disable, select <b>Disable</b> .

7. Next, click **Add**.



- A maximum of 16 tunnels can be created on a device.

- The Maximum Transmission Unit (MTU) of the tunnel interface depends on the underlying interface.
- It is advised that both PPPoE and the IP Tunneling feature do not function simultaneously on the device.
- IP configuration of Ethernet and Wireless interface should NOT be in the same subnet of virtual IP addresses of tunnels.

### 5.13.5.2 View Existing Tunnels

The IP Tunneling screen displays all the tunnels created on the device. The entries against each tunnel cannot be edited. However, the status of each tunnel entry can be modified.

You can either enable, disable or delete a tunnel by selecting the desired one from **Entry Status** box in the **IP Tunneling** screen.

S.No.	Name	Encapsulation Method	Virtual IP Address	Local IP Address	Remote IP Address	TTL	Entry Status
1	Interface1	ipip	50.0.0.1	20.0.0.132	30.0.0.132	3	Enable

Figure 5-93 IP Tunneling Interfaces

## Management

This chapter provides information on how to manage the device by using Web interface. It contains information on the following:

- [System](#)
- [File Management](#)
- [Services](#)
- [Simple Network Time Protocol \(SNTP\)](#)
- [Access Control](#)
- [Reset to Factory](#)
- [Convert QB to MP](#)

### 6.1 System

The **System** tab enables you to configure system specific information such as System Name, contact information of the person managing the device, and view system inventory and license information.

#### 6.1.1 System Information

The **System Information** tab enables you to view and configure system specific information such as System Name, System Description, Contact Details of the person managing the device, and so on.

To view and configure system specific Information, navigate to **MANAGEMENT > System > Information**. The **System Information** screen appears:

System Information	
System Up-Time	00:01:25:26 (dd hh:mm:ss)
System Description	Tsunami MP-8100-BSU-WD-v2.4.0
System Name	<input type="text" value="System-Name"/> (0-64) characters
Email	<input type="text" value="name@Organization.com"/> (6-32) characters
Phone Number	<input type="text" value="Contact-Phone-Number"/> (6-32) characters
Location	<input type="text" value="System-Location"/> (0-255) characters
GPS Longitude	<input type="text" value="-121.9171"/> (0-255) characters
GPS Latitude	<input type="text" value="37.4097"/> (0-255) characters
GPS Altitude	<input type="text" value="10"/> (0-255) characters

OK

**Figure 6-1 System Information**

Tabulated below is the table which explains System parameters and the method to configure the configurable parameter(s):

Parameter	Description
System Up-Time	This is a read-only parameter. It represents the operational time of the device since its last reboot.
System Description	This is a read-only parameter. It provides system description such as system name, firmware version and the latest firmware build supported.  For example: Tsunami MP-8100-BSU-WD-v2.4.0
System Name	Represents the name assigned to the device. You can enter a system name of maximum 64 characters.
Email	Represents the email address of the person administering the device. You can enter an email address of minimum 6 and maximum 32 characters.
Phone Number	Represents the phone number of the person administering the device. You can enter a phone number of minimum 6 and maximum 32 characters.
Location	Represents the location where the device is installed. You can enter the location name of minimum 0 and maximum 255 characters.
GPS Longitude	Represents the longitude at which the device is installed. You can enter a longitude value of minimum 0 and maximum 255 characters.
GPS Latitude	Represents the latitude at which the device is installed. You can enter a latitude value of minimum 0 and maximum 255 characters.
GPS Altitude	Represents the altitude at which the device is installed. You can enter a altitude value of minimum 0 and maximum 255 characters.

After configuring the required parameters, click **OK** and then **COMMIT**.

## 6.1.2 Inventory Management

The **Inventory Management** tab provides inventory information about the device.

To view inventory information, navigate to **MANAGEMENT > System > Inventory Management**. The **System Inventory Management Table** appears.

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 (8x60)	2300	1	1	0	0
2		Application Software Image	2103	1	2	3	2
3	S200000015000	Hardware Inventory	2001	1	1	0	0
4	-NA-	BSP-Bootloader	2107	1	1	2	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

Figure 6-2 Inventory Management

By default, the components information is auto-generated by the device and is used only for reference purpose. Click **Refresh**, to view the updated system inventory management information.

### 6.1.3 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 of the device 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 set on the device, click **MANAGEMENT > System > Licensed Features**. The **Licensed Features** screen appears.

Licensed Features	
Product Description	= Tsunami HP-8100-BSU-WD
Number of Radios	= 1
Number of Ethernet Interfaces	= 2
Radio 1 Allowed Frequency Band	= 2.4 GHz, 4.9 GHz, 5 GHz
Maximum Output Bandwidth	= 300 Mbps
Maximum Input Bandwidth	= 300 Mbps
Maximum Aggregate Bandwidth	= 600 Mbps
Product Family	= Tsunami HP
Product Class	= Outdoor
Maximum SUs Allowed	= 250
Allowed Operations Modes of Radio 1	= BSU, SU
Mac Address of the Device is	= 00:20:A6:05:0A:0B

Figure 6-3 Licensed Features

Tabulated below is the table which explains each of the parameters:

Parameter	Description
Product Description	Description about the device.

Parameter	Description
Number of Radios	The number of radios that the device is licensed to operate.
Number of Ethernet Interfaces	The number of Ethernet interfaces supported by the device.
Radio 1 Allowed Frequency Band	The operational frequency band supported by the device radio.
Maximum Output Bandwidth	The maximum output bandwidth limit of the device. It is represented in mbps.
Maximum Input Bandwidth	The maximum input bandwidth limit of the device. It is represented in mbps.  : The Input and Output Bandwidth features are referred with respect to the wireless interface. Input bandwidth refers to the data received on the wireless interface and output bandwidth refers to the data sent out of the wireless interface.
Maximum Aggregate Bandwidth	The maximum cumulative bandwidth of the device, which is the sum of configured output and input bandwidths.
Product Family	Represents the product family of the device.
Product Class	Represents the product class of the device, which is either indoor or outdoor.
Allowed Operational Modes of Radio1	Represents the operational mode of the device, that is, BSU/SU/End Point A/End Point B.
Maximum SUs Allowed	The maximum number of SUs that a BSU supports.
MAC address of the Device is	The MAC address of the device.

## 6.2 File Management

The **File Management** tab enables you to upgrade the firmware and configuration files onto the device, and retrieve configuration and log files from the device through Hypertext Transfer Protocol (HTTP) and Trivial File Transfer Protocol (TFTP).

### 6.2.1 TFTP Server

A Trivial File Transfer Protocol (TFTP) server lets you transfer files across a network. By using TFTP, you can retrieve files from the device for backup or copying, and you can upgrade the firmware or the configuration files onto the device. You can download the SolarWinds TFTP server application from <http://support.proxim.com>. You can also download the latest TFTP software from SolarWinds Web site at <http://www.solarwinds.net>.

While using TFTP server, ensure the following:

- The upload or download directory is correctly set (the default directory is **C:\TFTP-Root**).
- The required firmware file is present in the directory.
- The TFTP server is running during file upload and download. You can check the connectivity between the device and the TFTP server by pinging the device from the Personal Computer that hosts the TFTP server. The ping program should show replies from the device.

- The TFTP server should be configured to transmit and receive files (on the Security tab under **File > Configure**), with no automatic shutdown or time-out (on the **Auto-Close** tab).



: The instructions listed above are based on the assumption that you are using the SolarWinds TFTP server; otherwise the configuration may vary.

## 6.2.2 Text Based Configuration (TBC) File Management

Text Based Configuration (TBC) file is a simple text file that holds device template configurations. The device supports the TBC file in XML format which can be edited in any XML or text editors.

You can generate the TBC file from the CLI Session and manually edit the configurations and then load the edited TBC file to the device so that the edited configurations are applied onto the device. It differs mainly from the binary configuration file in terms of manual edition of configurations. The generated TBC file is a template which has only the default and modified configurations on the live CLI session.

### 6.2.2.1 Generating TBC File

The TBC file is generated through CLI by executing **generate** command.

While generating the TBC file from CLI, there is an option to generate it with or without all Management and Security Passwords. The management passwords include CLI/WEB/SNMP passwords. The security passwords include Network-Secret/Encryption-Key(s)/RADIUS-Shared-Secret. If included, these passwords become a part of the generated TBC file and are in a readable form. If excluded, all these passwords are not part of the generated TBC file.

The commands used for the generation of TBC file are:

```
T8000-00:00:01# generate tbc-with-pwds
T8000-00:00:01# generate tbc-without-pwds
```

The generated TBC file contains,

- Default configurations
- Any user-added or edited configurations on current live CLI session

The generated Text Based Template Configuration file appears as shown below:

```

-<!--
  *** Proxim Corporation - Text Based Template Configuration File ***
  *** NOTE: Please remove all unmodified parameters before importing to the device. ***
-->
- <pxm>
- <configuration>
- <management>
- <system-information>
  <email value="name@organization.com"/>
  <phone-number value="Contact-Phone-Number"/>
  <location value="System-Location"/>
  <gps-longitude value="-121.8893"/>
  <gps-latitude value="37.3321"/>
  <gps-altitude value="10"/>
  <system-name value="System-Name"/>
  <restore value="no"/>
  <factory-reset value="no"/>
</system-information>
- <tftp>
  <server-ip value="169.254.128.133"/>
  <file-name value="image.bin"/>
  <file-type value="image"/>
  <operation-type value="none"/>
</tftp>
- <access-ctrl>
  <all-access-ctrl value="enable"/>
  <http-ctrl value="enable"/>
  <https-ctrl value="enable"/>
  <snmp-ctrl value="enable"/>
  <telnet-ctrl value="enable"/>
  <ssh-ctrl value="enable"/>
</access-ctrl>
- <trap-host-table>
- <rowedit value="1">
  <ipaddress value="169.254.128.133"/>
  <password value="public"/>
  <comment value="Default"/>

```

Figure 6-4 TBC File in xml Format

### 6.2.2.2 Editing the TBC File

The TBC file can easily be opened and edited in any standard Text-Editors like Wordpad, MS-Word, Notepad++, Standard XML Editors. Proxim recommends XML Notepad 7 editor for editing the TBC file.

- You can modify any value between the double quotes("") in the TBC file. It is recommended not to change the text outside the double quotes (") or XML tags in the TBC file.
- Remove unchanged configurations from the TBC file before loading onto the device.

### 6.2.2.3 Loading the TBC file

The TBC file can be loaded onto the device by using either SNMP, Web Interface or CLI. You can either use **TFTP** or **HTTP** to load the TBC file.



By using Web Interface, you can load the TBC file by navigating to **MANAGEMENT > File Management > Upgrade Configuration**. To load the TBC file, it should be generated or downloaded onto the device. While loading the TBC file onto the device, any file name is accepted. Once loaded, the TBC file name is renamed to **PXM-TBC.xml**.

If the TBC file does not contain correct XML syntax, the file will be discarded with **DOM** error and no configurations will be loaded. All duplicate values entered are considered as errors while loading and syslogs will be generated accordingly. Therefore, it is recommended to delete all unchanged parameters from the TBC file during its edition. Commit is required to retain the configurations across reboots after loading the TBC file.



: Both Commit and Reboot are required to accept the modifications done in the TBC File. Only reboot is required to reject the modifications.

Loading the TBC file is allowed only once in an active device session (that is, if TBC file is loaded, reboot is required to apply all configurations or to load another TBC file). All configurations in the TBC file are loaded to the device irrespective of their default or modified or added configurations. Loading the TBC file takes approximately 10-20 seconds depending on the number of configurations added.



- Remove any unmodified parameters from the TBC file, before loading it.
- If you get any timeout errors while loading TBC file from SNMP interface, increase the time-out value to more than 30 seconds in the MIB Browser.

### 6.2.3 Upgrade Firmware

You can update the device with the latest firmware either through HTTP or TFTP.



: Make sure the firmware being loaded is compatible to the device being upgraded.

#### 6.2.3.1 Upgrade Firmware via HTTP

To upgrade the firmware via HTTP, do the following:

1. Navigate to **MANAGEMENT > File Management > Upgrade Firmware > HTTP**.

The screenshot shows the 'Upgrade Firmware' web interface. At the top, there are two tabs: 'HTTP' (selected) and 'TFTP'. Below the tabs is a 'File Name' input field containing the text 'C:\Documents and Settings\' followed by a 'Browse...' button. Below the input field, there are four red notes:
 

1. Please do not Navigate away from this page when the update is in progress.
2. After Upgrading the firmware, Reboot is required to work with new upgraded firmware.
3. File Name should not contain space or special characters.
4. Firmware file should be compatible with the device.

 At the bottom left of the form is an 'Update' button.

Figure 6-5 Upgrade Firmware - HTTP

2. In the HTTP screen, click **Browse** to select the latest firmware file from the desired location. Ensure that the file name does not contain any space or special characters.

3. Click **Update**.
4. Once the update successfully completes, reboot the device.

### 6.2.3.2 Upgrade Firmware via TFTP

To upgrade the firmware via TFTP Server, do the following:

1. Navigate to **MANAGEMENT > File Management > Upgrade Firmware > TFTP**.



Figure 6-6 Upgrade Firmware - TFTP

2. Enter the TFTP Server IP Address in the **Server IP Address** box.
3. Enter the name of the latest firmware file (including the file extension) that has to be loaded onto the device in the **File Name** box.
4. To update the device with new firmware, click either **Update**, or **Update & Reboot**. If you click **Update**, then you should reboot the device after loading the files. Whereas, if you click **Update and Reboot**, the system will automatically reboot the device after loading the files.



- After updating the device with the new firmware, reboot the device; Otherwise the device will continue to run with the old firmware.
- It is recommended not to navigate away from the upgrade screen, while the update is in progress.

## 6.2.4 Upgrade Configuration

You can update the device with the latest configuration files either through HTTP or TFTP.



: Make sure the configuration file being loaded into the device is compatible. That is, the configuration file being loaded should have been retrieved from a device of the same SKU.

### 6.2.4.1 Upgrade Configuration via HTTP

To upgrade the configuration files by using HTTP, do the following:

1. Navigate to **MANAGEMENT > File Management > Upgrade Configuration > HTTP**.

**Upgrade Configuration**

HTTP TFTP

File Name: C:\Documents and Settings\ Browse...

**Notes:**

1. File Name should not contain space or special characters.
2. Please select "flashcfg.cfg" for binary config file and "PXM-TBC.xml" to upgrade the Text Based Config file.
3. Please do not navigate away from this page when the update is in progress.
4. After Upgrading the binary configuration, Reboot to work with new configuration. For TBC after update please load to apply changes.
5. Configurage file should be compatible with the device.

Update Load Update & Load

**Figure 6-7 Upgrade Configuration - HTTP**

2. In the HTTP screen, click **Browse** to locate the configuration file. Select **Flashcfg.cfg** for Binary Configuration file and **PXM-TBC.xml** for Text Based Configuration file. Make sure that the file name does not contain any space or special characters.
3. If you are updating the device with Binary Configuration file then click **Update** and then reboot the device.
4. If you are updating the device with Text Based Configuration file then,
  - a. Click **Update** to update the device with the config file and then click **Load** for loading the config file onto the device. Alternatively, you can perform both update and load operation in one single step, by clicking **Update & Load**.
  - b. For the changes to take effect, click **COMMIT** and then **REBOOT**.

#### 6.2.4.2 Upgrade Configuration via TFTP

To upgrade the configuration files by using TFTP Server, do the following:

1. Navigate to **MANAGEMENT > File Management > Update Configuration > TFTP**.

**Upgrade Configuration**

HTTP TFTP

Binary Config  Text Based Config

Server IP Address: 169.254.128.133

File Name: flashcfg.cfg

**Notes:**

1. After Upgrading the binary configuration, Reboot to work with new configuration. For TBC after update please load to apply changes.
2. Please don't Navigate away from this page when the update in progress.
3. Configurage file should be compatible with the device.

Update Update & Reboot

**Figure 6-8 Upgrade Binary Configuration via TFTP**

2. You can update the device with two configuration files: Binary and Text Based. To update the device with Binary Configuration file, select **Binary Config**.
  - Enter the TFTP server IP Address in the **Server IP Address** box.

- Enter the name of the Binary file (including the file extension) that has to be downloaded onto the device in the **File Name** box.
- To update the device with Text Based Configuration files, select **Text Based Config**.
    - Enter the TFTP server IP Address in the **Server IP Address** box.
    - Enter the name of the Text Based file (including the file extension) that has to be downloaded onto the device in the **File Name** box.

The screenshot shows the 'Upgrade Configuration' window with the 'TFTP' tab selected. Under 'Text Based Config', the 'Server IP Address' is set to '168.254.128.133' and the 'File Name' is 'PXM-TBC.xml'. Below the input fields, there are three buttons: 'Update', 'Load', and 'Update & Load'. A red note is displayed below the buttons.

**Notes :**

1. After Upgrading the binary configuration, Reboot to work with new configuration. For TBC after update please load to apply changes.
2. Please don't Navigate away from this page when the update in progress.
3. Configurage file should be compatible with the device.

**Figure 6-9 Upgrade Text Based Configuration via TFTP**

- If you are updating the device with Binary Configuration file then click **Update** and then reboot the device or alternatively click **Update & Reboot**.
- If you are updating the device with Text Based Configuration file then
  - Click **Update** to copy the text config file onto the device and then click **Load** for updating the device with text config file.
  - Alternatively, you can perform both update and load operation in one single step, by clicking **Update & Load**.
  - For the changes to take effect, click **COMMIT** and then **REBOOT**.



: It is recommended not to navigate away from the upgrade screen, while the update is in progress.

## 6.2.5 Retrieve From Device

The **Retrieve From Device** tab allows you to retrieve logs and config files from the device either through HTTP or TFTP.

### 6.2.5.1 Retrieve from Device via HTTP

To retrieve files from the device by using HTTP, do the following:

- Navigate to **MANAGEMENT > File Management > Retrieve from Device > HTTP**.



Figure 6-10 Retrieve Files via HTTP

2. Select the type of file that you want to retrieve from the device from the **File Type** drop down box. The files may vary depending on your device.
3. Click **Retrieve**. Based on the selected file, the following **Download** screen appears.

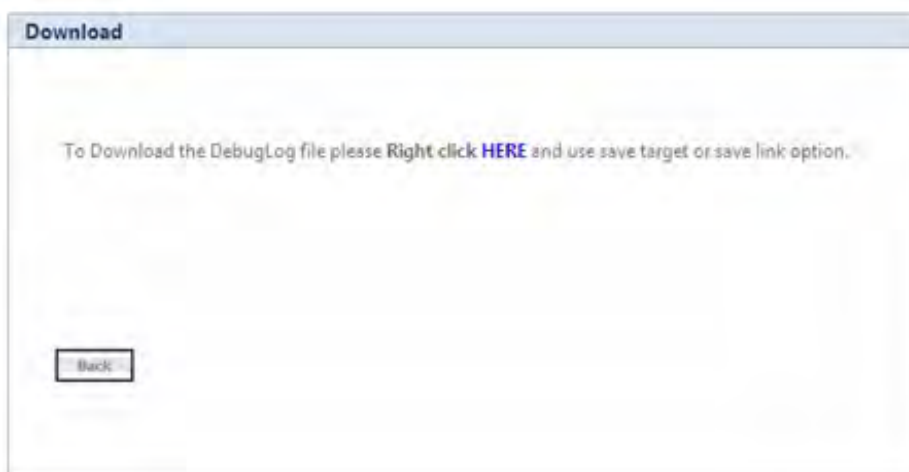


Figure 6-11 Download Screen

4. Right-click the **Download** link and select **Save Target As** or **Save Link As** to save the file to the desired location.

### 6.2.5.2 TFTP Retrieve

To retrieve files from the device by using TFTP, do the following:

1. Navigate to **MANAGEMENT > File Management > Retrieve from Device > TFTP**.

Figure 6-12 Retrieve Files via TFTP

2. Enter the TFTP server IP Address in the **Server IP Address** box.
3. Enter the name of the file (including the file extension) that has to be retrieved from the device, in the **File Name** box.
4. Select the file type that you want to retrieve from the device, from the **File Type** drop down box.
5. Click **Retrieve**. The retrieved file can be found in the TFTP Server folder.



- When the device is running with default factory settings, there is no Binary Configuration file present and hence it cannot be retrieved.
- Similarly, the Text Based Template Configuration file does not exist if it is not generated from the CLI.
- You can retrieve Event Logs only when they are generated by the device.

## 6.3 Services

The **Services** tab lets you configure the HTTP/HTTPS, Telnet/SSH and SNMP interface parameters.

### 6.3.1 HTTP/HTTPS

To configure HTTP/HTTPS interface parameters, navigate to **MANAGEMENT > Services > HTTP / HTTPS**.

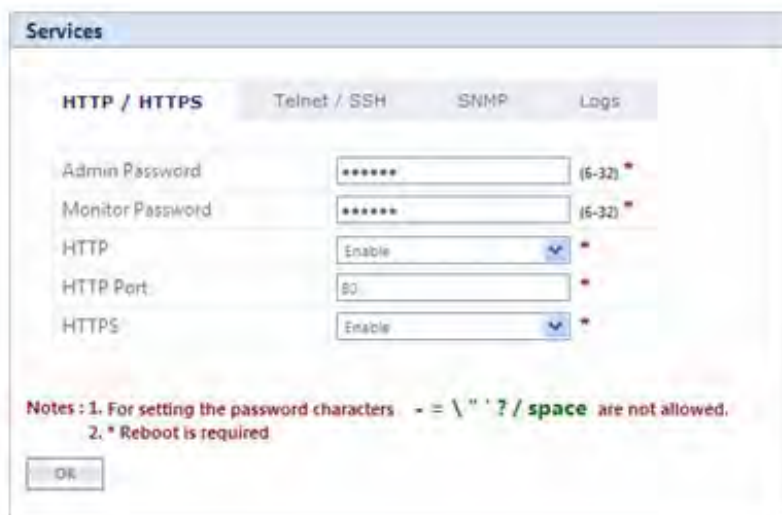





Figure 6-13 HTTP/HTTPS

Tabulated below is the table which explains HTTP/HTTPS parameters and the method to configure the configurable parameter(s).

Parameter	Description
Admin Password	By default, the Administrator password to access HTTP/HTTPS interface is <b>public</b> . For security reasons, it is recommended to change the default password. The password should be alphanumeric with minimum of 6 and maximum of 32 characters.  : The following special characters are not allowed in the password: - = \ " ' ? / space
Monitor Password	The Administrator user has the privilege to change the Monitor user password. By default, the Monitor user password to access HTTP/HTTPS interface is <b>public</b> . For security reasons it is recommended to change the default password. The password should be alphanumeric with minimum of 6 and maximum of 32 characters.  : The following special characters are not allowed in the password: - = \ " ' ? / space
HTTP	By default, a user can manage the device through Web Interface. To prevent access to the device through Web Interface, select <b>Disable</b> .
HTTP Port	Represents the HTTP port to manage the device using Web Interface. By default, the HTTP port is <b>80</b> .

Parameter	Description
HTTPS	<p>By default, a user can manage the device through Web Interface over secure socket Layer (HTTPS). To prevent access to the device through HTTPS, select <b>Disable</b>.</p> <p> : The password configuration for HTTPS is same as configured for HTTP.</p>

After configuring the required parameters, click **OK**, **COMMIT** and then **REBOOT**.

### 6.3.2 Telnet/SSH

To configure Telnet/SSH interface parameters, navigate to **MANAGEMENT > Services > Telnet / SSH**.

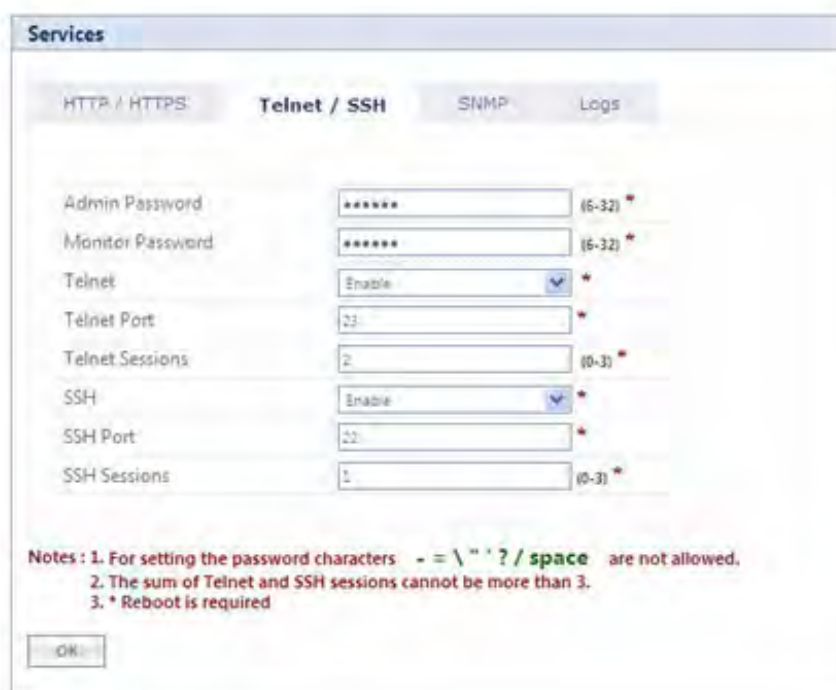





Figure 6-14 Telnet/SSH

Tabulated below is the table which explains Telnet/SSH parameters and the method to configure the configurable parameter(s):

Parameter	Description
Admin Password	<p>By default, the Administrator password to access Telnet/SSH interface is <b>public</b>. For security reasons, it is recommended to change the default password. The password should be alphanumeric with minimum of 6 and maximum of 32 characters.</p> <p> : The following special characters are not allowed in the password:  <b>- = \ " ' ? / space</b></p>



Monitor Password	<p>The Administrator user has the privilege to change the Monitor user password. By default, the Monitor user password to access Telnet/SSH interface is <b>public</b>. For security reasons it is recommended to change the default password. The password should be alphanumeric with minimum of 6 and maximum of 32 characters.</p>  : The following special characters are not allowed in the password: <b>- = \ " ' ? / space</b>
Telnet	By default, a user can manage the device through Telnet. To prevent access to the device through Telnet, select <b>Disable</b> .
Telnet Port	Represents the port to manage the device using Telnet. By default, the Telnet port is <b>23</b> .
Telnet Sessions	The number of Telnet sessions which controls the number of active Telnet connections. A user is restricted to configure a maximum of 3 Telnet sessions. By default, the number of Telnet sessions allowed is <b>2</b> .
SSH	By default, a user can manage the device through SSH. To prevent access to the device through SSH, select <b>Disable</b> .
SSH Port	Represents the port to manage the device using Secure Shell. By default, the Secure Shell port is <b>22</b> .
SSH Sessions	<p>The number of SSH sessions which controls the number of active SSH connections. A user is restricted to configure a maximum of 3 SSH sessions. By default, the number of SSH sessions allowed is <b>1</b>.</p>  : The 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 0 or 1.

After configuring the required parameters, click **OK**, **COMMIT** and then **REBOOT**.

### 6.3.3 SNMP

To configure SNMP interface parameters, navigate to **MANAGEMENT > Services > SNMP**.

The screenshot shows the 'Services' configuration page with the 'SNMP' tab selected. The configuration includes:

- SNMP:** Enable (dropdown menu)
- Version:** SNMPv1-v2c (dropdown menu)
- Read Password:** [masked] (6-32)
- Read/Write Password:** [masked] (6-32)

**SNMP Trap Host Table \***

S.No.	IP Address	Password	Comment	Entry Status
1.	109.254.128.133	[masked]	Default	Enable

**Notes :**

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



Buttons: OK, Add




Figure 6-15 SNMPv1-v2c



Figure 6-16 SNMPv3

Tabulated below is the table which explains SNMP parameters and the method to configure the configurable parameter(s):

Parameter	Description
SNMP	By default, the user has the access to manage the device through SNMP Interface. To prevent access to the device through SNMP, select <b>Disable</b> .   : Any change in the SNMP status will affect the Network Management System access.
Version	Allows you to configure the SNMP version. The supported SNMP versions are v1-v2c and v3. By default, the SNMP version is <b>v1-v2c</b> .
<b>SNMP v1-v2c Specific Parameters</b>	
Read Password	Represents the read only community string 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”. The password should be of minimum 6 and maximum 32 characters.   : The following special characters are not allowed in the password: - = \ “ ‘ ? / space

Read/Write Password	<p>Represents the read-write community string 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". The password should be of minimum 6 and maximum 32 characters.</p> <p> : The following special characters are not allowed in the password: - = \ " ' ? / space</p>
<b>SNMP v3 Specific Parameters</b>	
Security level	The supported security levels for the device are <b>AuthNoPriv</b> and <b>AuthPriv</b> . Select <b>AuthNoPriv</b> for Extensible Authentication or <b>AuthPriv</b> for both Authentication and Privacy (Encryption).
Priv Protocol	<p>Applicable only when the Security Level is set to <b>AuthPriv</b>.</p> <p>Represents the type of privacy (or encryption) protocol. Select the encryption standard as either AES-128 (Advanced Encryption Standard) or DES (Data Encryption Standard). The default Priv Protocol is AES-128.</p> <p> : The following special characters are not allowed in the password: - = \ " ' ? / space</p>
Priv Password	<p>Applicable only when the Security Level is set to <b>AuthPriv</b>.</p> <p>Represents the pass key for the selected Privacy protocol. The default password is <b>public123</b>. The password should be of minimum 8 and maximum 32 characters.</p> <p> : The following special characters are not allowed in the password: - = \ " ' ? / space</p>
Auth Protocol	Represents the type of Authentication protocol. Select the encryption standard as either <b>SHA</b> (Secure Hash Algorithm) or <b>MD5</b> (Message-Digest algorithm). The default Auth Protocol is <b>SHA</b> .
Auth Password	Represents the pass key for the selected Authentication protocol. The default password is <b>public123</b> . The password should be of minimum 8 and maximum 32 characters.

After configuring the required parameters, click **OK**, **COMMIT** and then **REBOOT**.

### 6.3.3.1 SNMP Trap Host Table

The SNMP Trap Host table allows you to add a maximum of 5 Trap server's IP address to which the SNMP traps will be delivered. By default, the SNMP traps are delivered to 169.254.128.133.



: The default SNMP Trap Host Table entry cannot be deleted.

To add entries to the Trap Host Table, click **Add** in the **Services** screen. The **SNMP Trap Host Table Add Row** screen appears:

Figure 6-17 Add Entries to SNMP Host Table

Configure the following parameters:

- **IP Address:** Type the IP address of the Trap server to which SNMP traps will be delivered.
- **Password:** Type the password to authenticate the Trap Server. The following special characters are not allowed in the password: - = \ " ' ? / **space**



: Applicable only to SNMP v1-v2c.

- **Comment:** Type comments, if any.
- **Entry Status:** Select the entry status as either Enable or Disable. If enabled, the device will send SNMP traps to the authenticated Trap Server.
- After configuring the required parameters, click **Add** and then **COMMIT**.

### 6.3.3.2 Edit SNMP Trap Host Table

Edit the desired SNMP Trap Host Table entries and click **OK**, **COMMIT** and then **REBOOT**.

### 6.3.4 Logs

The device supports two types of log mechanisms:

1. **Event Log:** Based on the configured event log priority, all the log messages are logged and used for any analysis. This log messages remain until they are cleared by the user.
2. **Syslog:** They are similar to Event logs except that they are cleared on device reboot.

To configure Event log and Syslog priority, navigate to **MANAGEMENT > Services > Logs**. The following screen appears:

The screenshot shows the 'Services' configuration window with the 'Logs' tab selected. It contains three dropdown menus: 'Event Log Priority' (Notice), 'Syslog Status' (Enable), and 'Syslog Priority' (Critical). Below is a 'Syslog Host Table' with a single row: S.No. 1, IP Address 189.254.128.140, Port 514, Host Comment, and Entry Status Enable. There are 'OK' and 'Add' buttons at the bottom.

Figure 6-18 Logs

- **Event Log Priority:** By default, the priority is set to Notice. You can configure the event log priority as one of the following:
  - Emergency
  - Alert
  - Critical
  - Error
  - Warning
  - Notice
  - Info
  - Debug

Please note that the priorities are listed in the order of their severity, where **Emergency** takes the highest severity and **Debug** the lowest. When the log priority is configured as high, all the logs with low priority are also logged. For example, if **Event Log Priority** is set to **Notice**, then the device will log all logs with priorities Notice, Warning, Error, Critical, Alert and Emergency.

- **Syslog Status:** By default, **Syslog Status** is enabled and default priority is **Critical**. If desired, you can choose to disable.
- **Syslog Priority:** Configuration is same as Event Log Priority.
- After configuring the required parameters, click **OK** and then **COMMIT**.

#### 6.3.4.1 Configure a Remote Syslog host

To forward the syslog messages to a remote syslog host, do the following:

1. Click **Add** in the **Syslog Host Table** screen. The **Syslog Host Table Add Row** screen appears:

**Figure 6-19 Syslog Host Table Add Row**

2. **IP Address:** Enter the IP address of the Syslog host.
3. **Host Port:** Represents the port on which the Syslog host listens to the log messages sent by the device. The default port is 514.



: The user must configure the correct port number on which the Syslog host is running. Choice of port number must be in line with the standards for port number assignments defined by Internet Assigned Numbers Authority (IANA).

4. **Comments:** Types comments, if any.
5. **Entry Status:** By default, the configured Syslog host is enabled on the device. To delete the configured Syslog host, click **Delete**. To disable an entry in the Syslog Host Table, click **Disable**.
6. Click **Add**.
7. Click **OK** and then **COMMIT**.

## 6.4 Simple Network Time Protocol (SNTP)

Proxim's point-to-multipoint and point-to-point devices are furnished with Simple Network Time Protocol (SNTP) Client software that enables to synchronize device's time with the network time servers.



The SNTP Client when enabled on the device(s), sends an NTP (Network Time Protocol) request to the configured time servers. Upon receiving the NTP response, it decodes the response and sets the received date and time on the device after adjusting the time zone and day light saving.

In case, the time servers are not available, then users also have the option to manually set the date and time on the device.


To synchronize device's time with time servers or manually set the time, navigate to **MANAGEMENT > SNTP**. The **SNTP** screen appears:

**Figure 6-20 Time Synchronization**

Tabulated below is the table which explains SNTP parameters and the method to configure the configurable parameter(s):

Parameter	Description
Enable SNTP Status	Select this parameter to enable SNTP Client on the device. If enabled, the SNTP Client tries to synchronize the device's time with the configured time servers.  By default, the SNTP status is disabled.
Primary Server IP Address/Domain Name	Enter the host name or the IP address of the primary SNTP time server. The SNTP Client tries to synchronize device's time with the configured primary server time.   : If host name is configured, instead of IP address then make sure that DNS server IP is configured on the device.
Secondary Server IP Address/Domain Name	Enter the host name or the IP address of the secondary SNTP time server. If the primary server is not reachable, then SNTP client tries to synchronize device's time with the secondary server time.   : If the SNTP Client is not able to synchronize the time with both the servers (primary and secondary), then it tries to synchronize again after every one minute.
Time Zone	Configure the time zone from the available list. This configured time zone is considered before setting the time, received from the time servers, on the device.
Day Light Saving Time	Configure the Day Light Saving time from the available list. This configured Day Light Saving time is considered before setting the time, received from the time servers, on the device.



Parameter	Description
ReSync Interval	Set ReSync time interval ranging from <b>0 to 1440</b> minutes. Once the time is synchronized, the SNTP Client tries to resynchronize with the time servers after every set time interval.
Sync Status	Specifies the SNTP Client sync status when it tries to ReSync again with the time servers. The status is as follows: <ul style="list-style-type: none"> <li>• <b>Disabled:</b> The SNTP client will not synchronize the time with the time servers and displays the status as Disabled.</li> <li>• <b>Synchronizing:</b> The SNTP client is in the process of synchronizing time with the time servers.</li> <li>• <b>Synchronized:</b> The SNTP client has synchronized time with the time servers.</li> </ul>
Current Date/Time	Displays the current date and time.  If SNTP is enabled, it displays the time the device received from the SNTP server. If SNTP is not enabled, then it displays the time manually set by the user.
Manual Time Configuration	If SNTP Client is disabled on the device or the time servers are not available on the network, then the user can manually set the time. Enter the time manually in the format: MM-DD-YYYY HH:MM:SS.   <ul style="list-style-type: none"> <li>• Manual time configuration is not retained across reboots. After every reboot the user has to set the time again.</li> <li>• With manual time configuration, the device may lag behind the actual time over a period of time. So, it is recommended to periodically check and adjust the time.</li> </ul>

To save the configured parameters, click **Ok** and then **COMMIT**.

## 6.5 Access Control

The **Access Control** tab enables you to control the device management access through specified host(s). You can specify a maximum of 5 hosts to control device management access.

To configure management access control parameters, navigate to **MANAGEMENT > Access Control**. The **Management Access Control** screen appears:

**Management Access Control**

Access Table Status:

**Management Access Control Table\***

S.No.	IP Address	Entry Status
1	109.254.128.145	Enable
2	109.254.128.140	Enable

**Notes:** 1. \* Reboot is required.  
2. Maximum 5 Entries are allowed.

**Figure 6-21 Management Access Control**

By default, the Management Access Control feature is disabled on the device. To enable, select **Enable** from the **Access Table Status** box and click **OK**. Reboot the device, for the changes to take effect.



: Only when the Access Table Status is enabled, you can add host(s) to the Management Access Control Table.

#### 6.5.0.1 Add Host(s) to Management Access Control Table

To add a host to the Management Access Control Table, do the following:

1. Click **Add** in the **Management Access Control** screen. The **Management Access Table Add Row** screen appears:

**Management Access Table Add Row**

IP Address:

Entry Status:

**Figure 6-22 Management Access Table Add Row**

2. **IP Address:** Type the IP address of the host that controls the device management access.
3. **Entry Status:** By default, the entry status is enabled meaning which the specified host can control the device management access. Edit the status to **Disable**, if you do not want the host to control the device management access.
4. Click **Add**.

#### 6.5.0.2 Edit Management Access Control Table Entries

Edit the desired host entries and click **OK**, **COMMIT** and then **REBOOT**.

## 6.6 Reset to Factory

The **Reset to Factory** tab allows you to reset the device to its factory default state. When this operation is performed, the device will reboot automatically and comes up with default configurations.

To reset the device to its factory defaults, navigate to **MANAGEMENT > Reset To Factory**. The Factory Reset screen appears:



Figure 6-23 Reset to Factory Defaults

Click **OK**, if you wish to proceed with factory reset, else click **Cancel**.

## 6.7 Convert QB to MP

The **Convert QB to MP** tab lets you convert a QB to SU so that the converted device can connect to a BSU and operate as a regular SU.

This feature is applicable only to,

- Tsunami® QB-8100-EPA which converts to a Tsunami® MP-8100-SUA, and
- Tsunami® QB-8150-EPR which converts to a Tsunami® MP-8150-SUR

You can convert a QB to SU mode by using two methods:

- **Method 1:** Web Interface
- **Method 2:** Load a SU config file (retrieved from another SU) onto the QB device and then reboot.



: Even after conversion from QB to MP, the device description still shows as QB.

To convert a QB to SU using Web Interface, do the following:

1. Navigate to **MANAGEMENT > Convert QB to MP**. The **Convert QB to MP** screen appears:

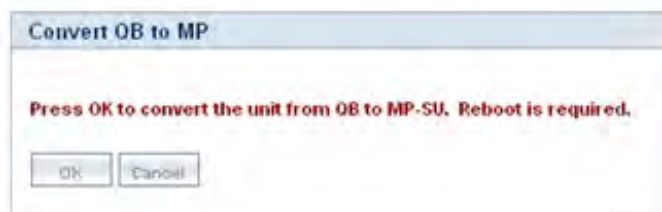


Figure 6-24 Convert QB to MP

2. Click **OK**.
3. Reboot the device for the changes to take effect.



- A QB after converting to SU will function in SU mode only. It will accept only MP firmware for upgrade.
- The version of the firmware being upgraded to should be 2.4.0 or later. If earlier version of the firmware is loaded, the device will reset to factory default upon initialization and operate in QB mode.
- When upgrading a converted device from Bootloader, it must be done using a QB image, as the device is licensed as QB.
- The conversion of the device from QB to SU requires a reboot.

- In case of Method 1 conversion, QB mode configuration will be deleted.
- Reset to factory defaults, always results in the device initializing in QB mode.

## Monitor

This chapter contains information on how to monitor the device by using Web interface. It contains information on the following:

- [Interface Statistics](#)
- [WORP Statistics](#)
- [Active VLAN](#)
- [Bridge](#)
- [Network Layer](#)
- [RADIUS \(BSU or End Point A only\)](#)
- [IGMP](#)
- [DHCP](#)
- [Logs](#)
- [Tools](#)
- [SNMP v3 Statistics](#)

### 7.1 Interface Statistics

Interface Statistics allows you to monitor the status and performance of the Ethernet and Wireless interfaces of the device.

#### 7.1.1 Ethernet Statistics

To view the Ethernet interface statistics, click **MONITOR > Interface Statistics**. The **Interface Statistics** screen appears:



The screenshot shows the 'Interface Statistics' web page. It has three tabs: 'Ethernet 1' (selected), 'Ethernet 2', and 'Wireless 1'. There are 'Refresh' and 'Clear' buttons. The statistics table is as follows:

Interface	Value
MTU	1500
MAC Address	00:20:a6:11:22:4b
Operational Status	DOWN
In Octets	0
In Unicast Packets	0
In Non-unicast Packets	0
In Errors	0
Out Octets	0
Out Unicast Packets	0
Out Discards	0
Out Errors	0

Figure 7-1 Ethernet Interface Statistics

To view Ethernet statistics, click **Ethernet 1** or **Ethernet 2** depending on the Ethernet interfaces supported by your device.

Tabulated below is the table which explains the parameters displayed in the Ethernet Statistics screen:

Parameter	Description
MTU	Specifies the largest size of the data packet received or sent on the Ethernet interface.
MAC Address	Specifies the MAC address at the Ethernet protocol layer.
Operational Status	Specifies the current operational state of the Ethernet interface.
In Octets	Specifies the total number of octets received on the Ethernet interface.
In Unicast Packets	Specifies the number of subnetwork- unicast packets delivered to the higher level protocol.
In Non-unicast Packets	Specifies the number of non-unicast subnetwork packets delivered to the higher level protocol.
In Errors	Specifies the number of inbound packets that contained errors and are restricted from being delivered.
Out Octets	Specifies the total number of octets transmitted out of the Ethernet interface.
Out Unicast Packets	Specifies the total number of packets requested by the higher level protocol and then, transmitted to the non-unicast address.
Out Discards	Specifies 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	Specifies the number of outbound packets that could not be transmitted because of errors.

To view the updated Ethernet statistics, click **Refresh**.

To delete the Ethernet statistics, click **Clear**.

## 7.1.2 Wireless Statistics

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



**Figure 7-2 Wireless Interface Statistics**

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

Parameter	Description
Retunes	Specifies the number of times the radio is retuned for better performance of the device.
<b>SNR Statistics</b>	
SNR Statistics represents the signal strength with regard to the noise at the antenna ports.	
Antenna	Specifies the antenna ports available for the product. Please note that the antenna ports vary depending on the product.
Status	Specifies the configuration status of the antenna ports. <b>ON</b> indicates that antenna port is enabled and <b>OFF</b> indicates that antenna port is disabled.
Control	Specifies the SNR value of the packet received at the selected channel frequency.

Parameter	Description
Extension	This parameter is applicable only to the 40 MHz modes, that is, 40 PLUS and 40 Minus. It specifies the SNR value of the packet received on the extension channel (20MHz).
<b>Rx Error Details</b>	
Decrypt Errors	This parameter is applicable only if 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.
PHY Errors	Specifies the total Rx PHY Errors. It generally indicates the interference in the wireless medium.

To view the updated Wireless statistics, click **Refresh**.

To delete the Wireless statistics, click **Clear**.

### 7.1.3 PPPoE Statistics



: Applicable only to a SU in Routing mode.

To view PPPoE interface statistics, navigate to **MONITOR > Interface Statistics > PPPoE > PPP Interface Stats**.

PPP Interface Stats	
MTU	1492
Operational Status	UP
In Octets	109
In Unicast Packets	0
In Non-unicast Packets	0
In Errors	0
Out Octets	91
Out Unicast Packets	0
Out Discards	0
Out Errors	0

**Figure 7-3 PPPoE Interface Statistics**

The PPPoE interface parameters are same as the Ethernet interface parameters. Please note that if a link is not established between a PPPoE client and server, then the device displays the following message.





Figure 7-4 PPPoE Server - No Link Established

To view the updated PPPoE interface statistics, click **Refresh**. Please note that for every 4 seconds, the interface statistics gets refreshed.

To view the PPPoE connection status such as the number of attempts made to start a session between PPPoE client and server, and the number of attempts failed to establish a connection, click **PPPoE Connection Stats**.



Figure 7-5 PPPoE Connection Statistics

To view updated connection statistics, click **Refresh**.

To restart the session between the PPPoE client and server, click **Restart PPPoE Session**. On successfully re-establishing a session, the IP address of the wireless interface will be assigned again by the PPPoE server, if Address Type is set to PPPoE-ippcp.

To clear the existing connection statistics, click **Clear**.

#### 7.1.4 IP Tunnels





: Applicable only in Routing Mode.

To view IP Tunnels interface statistics, click **MONITOR > Interface Statistics > IP Tunnels**. The following **IP Tunnel Interface Statistics** screen appears:

S.No.	Name	Alias	MTU	Operational Status	Details
1	Interface 2	tunn0	1480	UP	

Figure 7-6 IP Tunnels Interface Statistics

Tabulated below is an explanation to each of these parameters:

Parameter	Description																								
Name	Specifies the tunnel interface name.																								
Alias	Specifies a supplementary tunnel interface name.																								
Maximum Transmission Unit (MTU)	<p>Specifies the largest size packet or frame that can be sent over the tunnel interface.</p> <p>The MTU of the tunnel interface is derived from the underlying interface:  <b>For IP-IP tunnel interface:</b> MTU = Underlying interface MTU - 20 bytes (IP header)  <b>For IP-GRE interface:</b> MTU = Underlying interface MTU - 24 bytes (IP header + gre protocol)</p>																								
Operational Status	<p>The Operational Status indicates only the tunnel interface status. The status can be either UP or DOWN.</p> <p> : For the tunnel to function correctly both ends should be configured correctly.</p>																								
Details	<p>Provides a more detailed statistics about the tunnel interface. To view the detailed statistics, click </p> <div data-bbox="635 1081 1246 1756" data-label="Figure"> <p>The screenshot shows a window titled "IP Tunnel Interface Statistics" with a "Refresh" and "Close" button at the top right. The main content is a table of statistics:</p> <table border="1"> <tr><td>Name</td><td>Interface1</td></tr> <tr><td>Alias</td><td>tunn0</td></tr> <tr><td>MTU</td><td>1480</td></tr> <tr><td>Operational Status</td><td>UP</td></tr> <tr><td>In Octets</td><td>0</td></tr> <tr><td>In Ucast Packets</td><td>0</td></tr> <tr><td>In NUcast Packets</td><td>0</td></tr> <tr><td>In Errors</td><td>0</td></tr> <tr><td>Out Octets</td><td>0</td></tr> <tr><td>Out Ucast packets</td><td>0</td></tr> <tr><td>Out Discards</td><td>0</td></tr> <tr><td>Out Errors</td><td>0</td></tr> </table> <p>A "Back" button is located at the bottom left of the window.</p> </div> <p><b>Figure 7-7 Detailed IP Tunnels Interface Statistics</b></p> <p>The detailed tunnel interface parameters are similar to the Ethernet Interface Statistics. Please refer to <a href="#">Ethernet Statistics</a>.</p>	Name	Interface1	Alias	tunn0	MTU	1480	Operational Status	UP	In Octets	0	In Ucast Packets	0	In NUcast Packets	0	In Errors	0	Out Octets	0	Out Ucast packets	0	Out Discards	0	Out Errors	0
Name	Interface1																								
Alias	tunn0																								
MTU	1480																								
Operational Status	UP																								
In Octets	0																								
In Ucast Packets	0																								
In NUcast Packets	0																								
In Errors	0																								
Out Octets	0																								
Out Ucast packets	0																								
Out Discards	0																								
Out Errors	0																								

## 7.2 WORP Statistics

### 7.2.1 General Statistics

**WORP General Statistics** provides general statistics about the WORP.

To view General Statistics, navigate to **MONITOR > WORP Statistics > Interface 1 > General Statistics**. The following **WORP General Statistics** screen appears:

WORP General Statistics			
Interface Type	BSU		
WORP Protocol Version	10	<input type="button" value="Refresh"/>	<input type="button" value="Clear"/>
<b>WORP Data Messages</b>		<b>Registration details</b>	
Poll Data	631	Remote Partners	1
Poll No Data	85935	Announcements	17515
Reply Data	782	Request For Service	2
Reply More Data	0	Registration Requests	3
Reply No Data	85312	Registration Rejects	0
Poll No Replies	541	Authentication Requests	3
<b>Data Transmission Statistics</b>		Authentication Confirms	3
Send Success	624	Registration Attempts	1
Send Retries	0	Registration Incompletes	0
Send Failures	7	Registration Timeouts	0
Receive Success	771	Registration Last Reason	None
Receive Retries	0		
Receive Failures	11		

**Figure 7-8 WORP General Statistics**

Tabulated below is an explanation to each of these parameters:

Parameter	Description
Interface Type	Specifies the type of radio interface.
WORP Protocol Version	Specifies the version of the WORP Protocol used. This information is useful to the customer support team for debugging purpose only.
<b>WORP Data Messages</b>	
Specifies the sent or received data frames through wireless interface.	
Poll Data	Refers to the number of polls with data messages sent or received.
Poll No Data	Refers to the number of polls with no data messages sent or received.
Reply Data	Refers to the number of poll replies with data messages sent or received.
Reply More Data	Refers to the number of poll replies with more data messages sent or received.
Reply No Data	Refers to the number of poll replies with no data messages sent or received.
Poll No Replies	Refers to the number of times poll messages were sent by a BSU/End Point A but no reply was received by SU/End Point B. This parameter is valid only on BSU.

Parameter	Description
<b>Data Transmission Statistics</b>	
Specifies the number of transmissions occurred through the interface.	
Send Success	Refers to the number of data messages sent and acknowledged by the peer successfully.
Send Retries	Refers to the number of data messages that are re-transmitted and acknowledged by the peer successfully.
Send Failures	Refers to the number of data messages that are not acknowledged by the peer even after the specified number of retransmissions.
Receive Success	Refers to the number of data messages received and acknowledged successfully.
Receive Retries	Refers to the number of successfully received re-transmitted data messages.
Receive Failures	Refers to the number of data messages that were not received successfully.
<b>Registration Details</b>	
Specifies the status of the entire registration process.	
Remote Partners	Refers to the number of remote partners. For a SU/End Point A/End Point B, the number of remote partners is always zero or one.
Announcements	Refers to the number of Announcement messages sent or received on WORP interface.
Request For Service	Refers to the number of requests for service messages sent or received.
Registration Requests	Refers to the number of registration request messages sent or received on WORP interface.
Registration Rejects	Refers to the number of registration reject messages sent or received on WORP interface.
Authentication Requests	Refers to the number of authentication request messages sent or received on WORP interface.
Authentication Confirms	Refers to the number of authentication confirm messages sent or received on WORP interface.
Registration Attempts	Refers to the number of times a registration attempt has been initiated.
Registration Incompletes	Refers to the number of registration attempts that are not yet completed.
Registration Timeouts	Refers to the number of times the registration procedure timed out.
Registration Last Reason	Refers to the reason for the last registration getting aborted or failed.



: For better results, the Send Failure or Send Retrieve must be low in comparison to Send Success. The same applies for Receive Retries or Receive Failure.

Click **Clear** to delete existing general statistics.

Click **Refresh** to view updated WORP general statistics.

### 7.2.2 SU / End Point B Link Statistics



SU Link Statistics is applicable only to a BSU, and End Point B Link Statistics is applicable only to a End Point A device.

SU Link statistics provides information about the SUs connected to a BSU. Similarly, End Point B Link Statistics provides information about an End Point B currently connected to an End Point A device.

To view link statistics, navigate to **MONITOR > WORP Statistics > Interface 1 > SU / End Point B Link Statistics**.



Figure 7-9 An Example - SU Link Statistics

Tabulated below is an explanation to each of these parameters:

Parameter	Description				
SU Name/ End Point B Name	Represents the name of the SU/End Point B connected to a BSU/End Point A respectively.				
MAC Address	Represents the MAC address of the SU/End Point B connected to a BSU/End Point A respectively.				
Local Tx Rate (Mbps)	Represents the data transmission rate at the local (current device) end.				
Remote Tx Rate (Mbps)	Represents the data transmission rate at the remote (peer) end.				
Local Antenna Port Info	Indicates the status of the antenna ports at the local end. The following symbols indicate the status of the antenna ports. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <table border="1"> <tr> <td style="text-align: center;"></td> <td>Indicates the antenna port is disabled.</td> </tr> <tr> <td style="text-align: center;"></td> <td>Indicates the antenna port is enabled and signal is present.</td> </tr> </table> </div>		Indicates the antenna port is disabled.		Indicates the antenna port is enabled and signal is present.
	Indicates the antenna port is disabled.				
	Indicates the antenna port is enabled and signal is present.				
Local Signal (dBm)	Represents the signal level with which the device at the local end receives frames from the device at the remote end, through wireless medium.				
Local Noise (dBm)	Represents the noise measured at the local end antenna ports.				
Local SNR (dB)	Represents the SNR measured by the receiver at the local end and is based on the Local Signal and Local Noise.				

Parameter	Description
Remote Antenna Port Info	Indicates the status of the remote end antenna ports. The antenna ports status is same as explained in Local Antenna Port Info.
Remote Signal (dBm)	Represents the signal level with which the device at the remote end receives frames, through wireless medium.
Remote Noise (dBm)	Represents the noise measured at the remote end antenna ports.
Remote SNR (dB)	Represents the SNR measured by the receiver at the remote end and is based on the Remote Signal and Remote Noise.
Current Tx Power (dBm)	Applicable only when ATPC is enabled on the device. <ul style="list-style-type: none"> <li>• <b>TPC</b>: Displays the TPC value currently applied by the device to adjust the transmit power radiated by the radio antenna.</li> <li>• <b>EIRP</b>: Displays the current EIRP that a radio antenna radiates (after applying the TPC).</li> <li>• <b>Power</b>: Displays the current transmit power radiated by the radio (after applying the TPC).</li> </ul>

Click **Refresh** to view updated link statistics.


To view detailed SU/End Point B Link statistics, click **Details** icon  in the **SU/End Point B Link Statistics** screen. The following screen appears depending on your device:



Figure 7-10 SU Detailed Statistics

The detailed page displays Remote SNR information, that is, the Minimum Required SNR and the Maximum Optimal SNR value for a given data rate or modulation, to achieve optimal throughput.

To disconnect a SU/End Point B from BSU/End Point A respectively, click **Disconnect**. To view updated detailed statistics, click **Refresh**.

To view local SNR table, click [Click here for Local SNR-Table](#) on the upper-right of **SU/End Point B Link Statistics** screen (Refer [An Example - SU Link Statistics](#)). The following screen appears depending on your device:

Local SNR Information								
Wireless 1								
S.No.	MCS Index	Modulation	Number of Streams	Data Rate (Mbps)	Minimum Required SNR (dB)		Maximum Optimal SNR (dB)	
					Default	Configured	Default	Configured
1	MCS0	BPSK(1/2)	Single	6.5	6	6	86	86
2	MCS1	QPSK(1/2)	Single	13.0	9	9	86	86
3	MCS2	QPSK(3/4)	Single	19.5	11	11	84	84
4	MCS3	16QAM(1/2)	Single	26.0	14	14	82	82
5	MCS4	16QAM(3/4)	Single	39.0	18	18	80	80
6	MCS5	64QAM(2/3)	Single	52.0	22	22	78	78
7	MCS6	64QAM(3/4)	Single	58.5	25	25	77	77
8	MCS7	64QAM(5/6)	Single	65.0	28	28	77	77
9	MCS8	BPSK(1/2)	Dual	13.0	9	9	86	86
10	MCS9	QPSK(1/2)	Dual	26.0	12	12	84	84
11	MCS10	QPSK(3/4)	Dual	39.0	14	14	82	82
12	MCS11	16QAM(1/2)	Dual	52.0	16	16	80	80
13	MCS12	16QAM(3/4)	Dual	78.0	20	20	78	78
14	MCS13	64QAM(2/3)	Dual	104.0	26	26	78	78
15	MCS14	64QAM(3/4)	Dual	117.0	29	29	77	77
16	MCS15	64QAM(5/6)	Dual	130.0	30	30	76	76

**Notes:** 1. Remote device uses configured minimum required SNR values when it is enabled with DDRS feature.  
2. Remote device uses configured maximum optimal SNR values when it is enabled with ATPC feature.

Close

Figure 7-11 Local SNR Information

These configured values are used by ATPC and DDRS to derive TPC and data rate for optimal throughput.

### 7.2.3 BSU/End Point A Link Statistics



: BSU Link Statistics is applicable only to a SU, and End Point A Link Statistics is applicable only to an End Point B device.

BSU Link statistics provides information about the BSU to which SUs are connected. Similarly, End Point A Link Statistics provides information about an End Point A currently linked to an End Point B device.



BSU Link Statistics														
BSU Name	MAC Address	Local Tx Rate (Mbps)	Remote Tx Rate (Mbps)	Local Antenna Port Info	Local Signal (dBm)	Local Noise (dBm)	Local SNR (dB)	Remote Antenna Port Info	Remote Signal (dBm)	Remote Noise (dBm)	Remote SNR (dB)	Current Tx Power Info		Details
												TPC	EIRP	
System Name	00:20:a6:d8:ca:45	78	78	A1	-15	-97	82	A1	-32	-95	63	TPC	10	🔍
				A2	-15	-99	84	A2	-33	-100	67	EIRP	27	
				A3	-	-	-	A3	-	-	-	Power	12	

[Click here for Local SNR Table](#)

**Legends**  
 Antenna Port Disabled  
 Antenna Port Enabled and Signal Present

Figure 7-12 An Example - BSU Link Statistics

The link statistics are similar to [SU / End Point B Link Statistics](#).

### 7.2.4 QoS Statistics (BSU or End Point A Only)



This parameter is applicable only to BSU or End Point A radio modes.

To view QoS Statistics, navigate to **MONITOR > WORP Statistics > Interface 1 > QoS Statistics**. The following **QoS Summary** screen appears.

QoS Summary	
<b>Note :</b> This screen shows the total, minimum and maximum bandwidth allocated per BSU and the minimum and maximum bandwidth allocated for each SU registered with the BSU.	
<input type="button" value="Refresh"/>	
<b>ACTIVE</b>	
Uplink Bandwidth	1 Kbps
Downlink Bandwidth	9 Kbps
Uplink MIR	307200 Kbps
Downlink MIR	307200 Kbps
Uplink CIR	0 Kbps
Downlink CIR	0 Kbps
<b>PROVISIONED</b>	
Uplink MIR	307200 Kbps
Downlink MIR	307200 Kbps
Uplink CIR	0 Kbps
Downlink CIR	0 Kbps

Figure 7-13 QoS Summary

This screen shows the total, minimum and maximum bandwidth allocated per BSU/End Point A, and the minimum and maximum bandwidth allocated for each SU/End Point B registered with the BSU/End Point A respectively.

## 7.3 Active VLAN



: This parameter is applicable only to a device in SU mode.

The Active VLAN page enables you to identify the VLAN Configuration mode applied on a device in SU mode.

To view active VLAN applied on the device in SU mode, navigate to **MONITOR > Active VLAN**. The **Active VLAN** page appears:

Active VLAN	
Active VLAN Config	Local
VLAN Status	Disable
Management VLAN Id	-1
Management VLAN Priority	0
Double VLAN (Q in Q) Status	Disable

Refresh

**Figure 7-14 Active VLAN**

The **Active VLAN Config** parameter helps you to identify the current VLAN configuration applied on the device in SU mode.

- **Local:** VLAN configuration is done locally from the device.
- **Remote:** VLAN configuration is done through RADIUS Server.

This page also displays the VLAN parameters and their values that are configured either locally or remotely.

To view active VLAN Ethernet Configuration, navigate to **MONITOR > Active VLAN > Ethernet**. The **Active VLAN Ethernet Configuration** page appears:

Active VLAN Ethernet Configuration	
Ethernet 1	
Interface	eth1
VLAN Mode	Access
Access VLAN Id	-1
Access VLAN Priority	0

Refresh

**Figure 7-15 Active VLAN Ethernet Configuration**

This page displays the VLAN Ethernet parameters and their values that are configured either locally or remotely.



: Please note that the number of Ethernets vary depending on the device.

## 7.4 Bridge

### 7.4.1 Bridge Statistics

The Bridge Statistics allows you to monitor the statistics of the Bridge.

To view the **Bridge Statistics**, navigate to **MONITOR > Bridge > Bridge Statistics**. The following **Bridge Statistics** screen appears:

Description	Bridge
MTU	1500
MAC Address	00:20:a6:11:22:4b
Operational Status	UP
In Octets	2853697
In Unicast Packets	19737
In Non-unicast Packets	28
In Errors	0
Out Octets	14745820
Out Unicast Packets	27199
Out Discards	0
Out Errors	0

**Figure 7-16 Bridge Statistics**

The following table lists the parameters and their description:

Parameter	Description
Description	This parameter provides a description about the bridge.
MTU	Represents the largest size of the data packet sent on the bridge.
MAC Address	Represents the MAC address at the bridge protocol layer.
Operational Status	Represents the current operational status of the bridge: <b>UP</b> (ready to pass packets) or <b>DOWN</b> (not ready to pass packets).
In Octets	Represents the total number of octets received on the bridge interface, including the framing characters.
In Unicast Packets	Represents the number of unicast subnetwork packets delivered to the higher level protocol.
In Non-unicast Packets	Represents the number of non-unicast subnetwork packets delivered to the higher level protocol.

Parameter	Description
In Errors	Represents the number of inbound packets with errors and that are restricted from being delivered.
Out Octets	Represents the total number of octets transmitted out of the bridge, including the framing characters.
Out Unicast Packets	Represents the total number of packets requested by higher-level protocols to be transmitted out of the bridge interface to a subnetwork-unicast address, including those that were discarded or not sent.
Out Discards	Represents the number of error-free outbound packets which are discarded to prevent them from being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Out Errors	Represents the number of outbound packets that could not be transmitted because of errors.

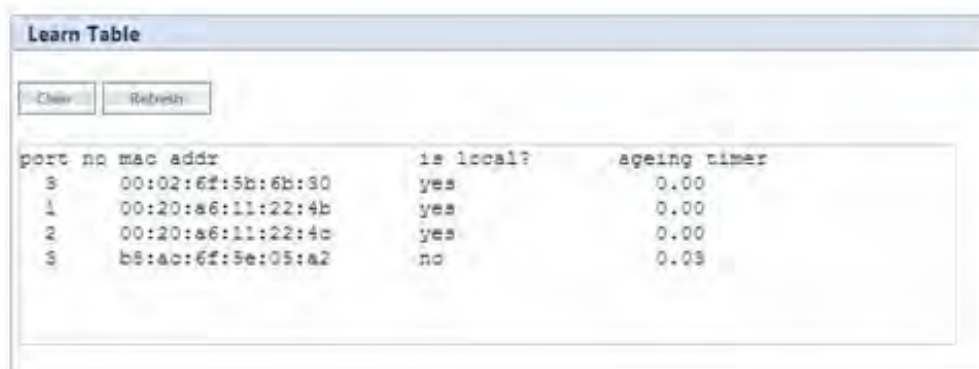
To view updated Bridge statistics, click **Refresh**.

To clear the Bridge statistics, click **Clear**.

## 7.4.2 Learn Table

Learn Table allows you to view all the MAC addresses that the device has learnt on all of its interfaces.

To view Learn Table statistics, navigate to **MONITOR > Bridge > Learn Table**. The **Learn Table** screen appears.



port no	mac addr	is local?	ageing timer
3	00:02:6f:5b:6b:30	yes	0.00
1	00:20:a6:11:22:4b	yes	0.00
2	00:20:a6:11:22:4c	yes	0.00
3	b8:ac:6f:5e:05:a2	no	0.03

**Figure 7-17 Learn Table**

The Learn Table displays the MAC address of the learnt device, the bridge port number, aging timer for each device learnt on an interface, and the local (DUT's local interfaces)/remote (learned entries through bridging) status of the learnt device.

To view updated learn table statistics, click **Refresh**.

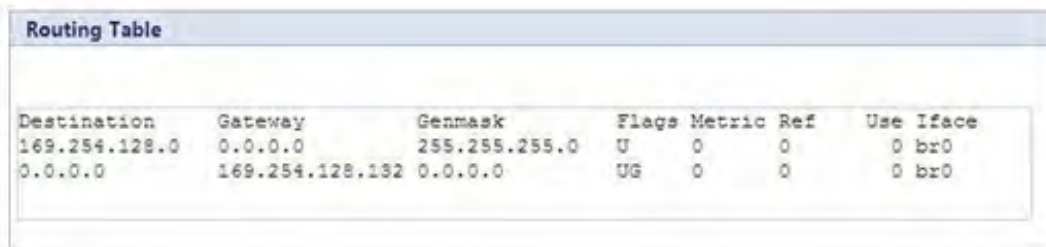
To clear learn table statistics, click **Clear**.

## 7.5 Network Layer

### 7.5.1 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, navigate to **MONITOR > Network Layer > Routing Table**. The **Routing Table** screen appears:



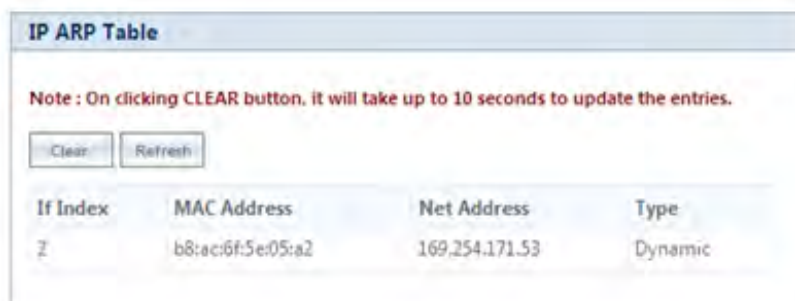
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
169.254.128.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
0.0.0.0	169.254.128.132	0.0.0.0	UG	0	0	0	br0

Figure 7-18 Routing Table

### 7.5.2 IP ARP

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical address on the network. The IP ARP table is used to maintain a correlation between each IP address and its corresponding MAC address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

To view IP Address Resolution Protocol (ARP) statistics, navigate to **MONITOR > Network Layer > IP ARP**. The **IP ARP Table** screen appears.



Note: On clicking CLEAR button, it will take up to 10 seconds to update the entries.

Clear Refresh

If Index	MAC Address	Net Address	Type
Z	b8:ac:6f:5e:05:a2	169.254.171.53	Dynamic

Figure 7-19 IP ARP Table

The **IP ARP Table** contains the following information:

- **Index:** Represents the interface type.
- **MAC Address:** Represents the MAC address of a node on the network.
- **Net Address:** This parameter represents the corresponding IP address of a node on the network.
- **Type:** This parameter represents the type of mapping, that is, Dynamic or Static.

To view updated IP ARP entries, click **Refresh**.

To clear the IP ARP entries, click **Clear**.

### 7.5.3 ICMP Statistics

The ICMP Statistics attributes enable you to monitor the message traffic that is received and transmitted by the device.

To view ICMP statistics, navigate to **MONITOR > Network Layer > ICMP Statistics**. The **ICMP Statistics** screen appears.

ICMP Statistics			
In Msgs	12	Out Msgs	12
In Errors	0	Out Errors	0
In Dest Unreachs	12	Out Dest Unreachs	12
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 7-20 ICMP Statistics**

The following table lists the ICMP Statistics parameters and their description:

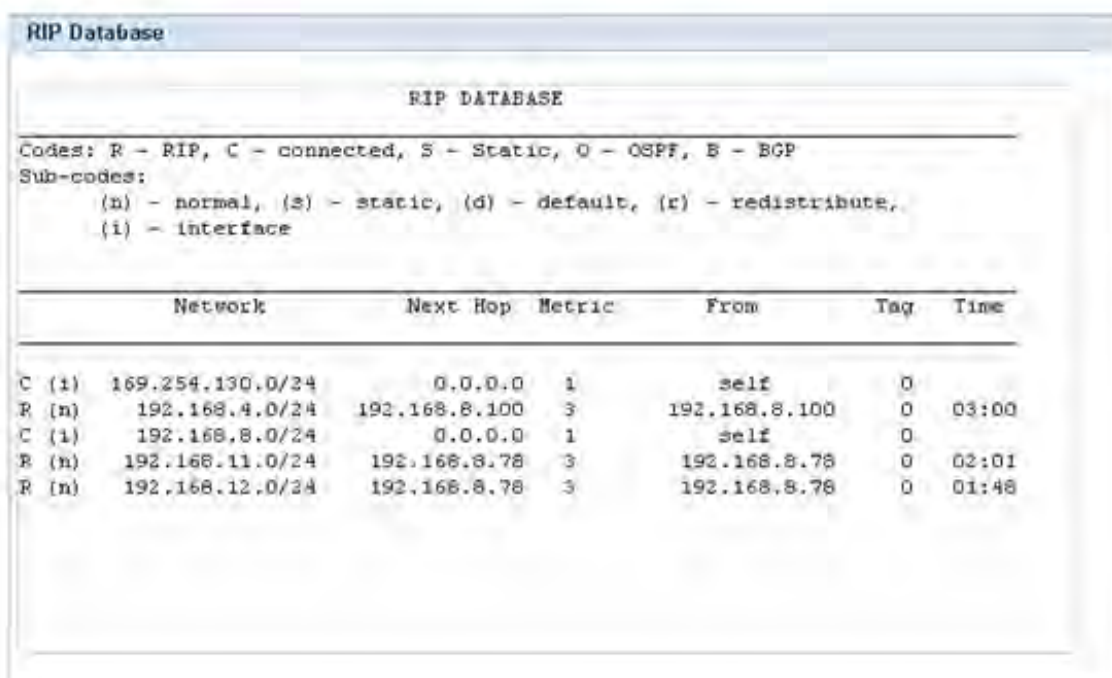
Parameter	Description
In Msgs or Out Msgs	Represents the number of ICMP messages that are received/transmitted by the device.
In Errors or Out Errors	Represents the number of ICMP messages that are received/transmitted by the device but determined as having ICMP-specific errors such as Bad ICMP checksums, bad length and so on.
In Dest Unreachs or Out Dest Unreachs	Represents the number of ICMP destination unreachable messages that are received/transmitted by the device.
In Time Excds or Out Time Excds	Represents the number of ICMP time exceeded messages that are received/transmitted by the device.
In Parm Probs or Out Parm Probs	Represents the number of ICMP parameter problem messages that are received/transmitted by the device.
In Srec Quenchs or Out Srec Quenchs	Represents the number of ICMP source quench messages that are received/transmitted by the device.
In Redirects or Out Redirects	Represents the rate at which the ICMP redirect messages are received/transmitted by the device.
In Echos	Represents the rate at which the ICMP echo messages are received.
In EchoReps or Out EchoReps	Represents the rate at which the ICMP echo reply messages are received/transmitted by the device.

Parameter	Description
In Timestamps or Out Timestamps	Represents the rate at which the ICMP timestamp (request) messages are received/transmitted by the device.
In Timestamps Repls or Out Timestamps Repls	Represents the rate at which the ICMP timestamp reply messages are received/transmitted by the device.
In Addr Masks or Out Addr Masks	Represents the number of ICMP address mask request messages that are received/transmitted by the device.
In Addr Mask Repls or Out Addr Mask Repls	Represents the number of ICMP address mask reply messages that are received/transmitted by the device.

To view updated ICMP Statistics, click **Refresh**.

#### 7.5.4 RIP Database

The **RIP Database** screen contains routes (Routing Information Protocol updates) 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	Tag	Time
C (i)	169.254.130.0/24	0.0.0.0	1	self	0	
R (n)	192.168.4.0/24	192.168.8.100	3	192.168.8.100	0	03:00
C (i)	192.168.8.0/24	0.0.0.0	1	self	0	
R (n)	192.168.11.0/24	192.168.8.78	3	192.168.8.78	0	02:01
R (n)	192.168.12.0/24	192.168.8.78	3	192.168.8.78	0	01:48

Figure 7-21 RIP Database

## 7.6 RADIUS (BSU or End Point A only)



: RADIUS is applicable only to a BSU or an End Point A device.

### 7.6.1 Authentication Statistics

Authentication Statistics provides information on RADIUS Authentication for both the primary and backup servers for each RADIUS server profile.

To view Authentication statistics, navigate to **MONITOR > RADIUS > Authentication Statistics**. The **RADIUS Client Authentication Statistics** screen appears:

S.No.	Round Trip Time	Reqs	RTMS	Accepts	Rejects	Resp	Mal Resp	Bad Auths	Timeouts	Un Known Types	Pkts Dropped
1	0	1	3	0	0	0	0	0	3	0	0

Refresh

**Notes**

S.No. : Server Index  
 Reqs: Access Requests  
 RTMS: Access Retransmissions  
 Accepts: Access Accepts  
 Rejects : Access Rejects  
 Resp: Stats Responses  
 Mal Resp: Malformed Responses  
 Bad Auths : Bad Authenticators  
 Time outs: Timeouts  
 Pkts Dropped : Packets Dropped

Figure 7-22 Radius Client Authentication Statistics

The following table lists the Authentication Statistics parameters and their description:

Parameter	Description
Round Trip Time	Represents the round trip time for messages exchanged between RADIUS client and authentication server since the client startup.
Reqs	Represents the number of RADIUS access request messages transmitted from the RADIUS client to the authentication server since client startup.
RTMS	This parameter represents the number of times the RADIUS access requests are being transmitted to the server from the device since the client startup.
Accepts	Represents the number of RADIUS access accept messages received by the device since client startup.
Rejects	Represents the number of RADIUS access reject messages received by the device since client startup.
Resp	Represents the number of RADIUS response packets received by the device since client startup.



Parameter	Description
Mal Resp	Represents the number of malformed RADIUS access response messages received by the device since client startup.
Bad Auths	Represents the number of malformed RADIUS access response messages containing invalid authenticators received by the device since client startup.
Time Outs	Represents the total number of timeouts for RADIUS access request messages since client startup.
UnKnown Types	This parameter specifies the number of messages with unknown RADIUS message code since client startup.
Packets Dropped	Represents the number of RADIUS packets dropped by the device.

To view updated RADIUS Client Authentication statistics, click **Refresh**.

## 7.7 IGMP



: Applicable in Bridge mode only.

To view IGMP statistics, navigate to **MONITOR > IGMP > IGMP Snooping Stats**. The **Ethernet or Wireless Multicast List** screen appears:

S.No.	Group IP	MAC Address	Time Elapsed
1	239.255.255.250	01:00:5e:7f:ff:fa	00:00:00.43

Figure 7-23 Ethernet1 Multicast List

### 7.7.1 Ethernet or Wireless Multicast List

The Multicast List table contains the IGMP Multicast IP and Multicast MAC address details for the Ethernet or Wireless interfaces. The following table lists the parameters and their description.

Parameter	Description
Group IP	Represents the IP address of the multicast group for Ethernet or Wireless interface learned by IGMP snooping.
MAC Address	Represents the MAC address of the multicast group for Ethernet or Wireless interface learned by IGMP snooping.

Parameter	Description
Time Elapsed	Represents the time elapsed since the multicast entry has been created for the Ethernet or Wireless interface.

To view updated IGMP statistics, click **Refresh**.

### 7.7.2 Router Port List

The Router Port List displays the list of ports on which multicast routers are attached.

To view Router Port List, navigate to **MONITOR > IGMP > Router Port List**. The **Router Port List** screen appears:

S.No.	Port Number	Time Elapsed (dd:hh:mm:ss)
1	2	00:00:00:00
2	1	00:00:00:00

**Figure 7-24 Router Port List**

The following table lists the parameters and their description.

Parameter	Description
Port Number	Represents the port number on which multicast router is attached (on which IGMP Query has been received).
Time Elapsed	Represents the time elapsed since the port is marked as the router port.

To view updated Router Port list, click **Refresh**.

## 7.8 DHCP

**DHCP Leases** file stores the DHCP client database 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, navigate to **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";
}

```

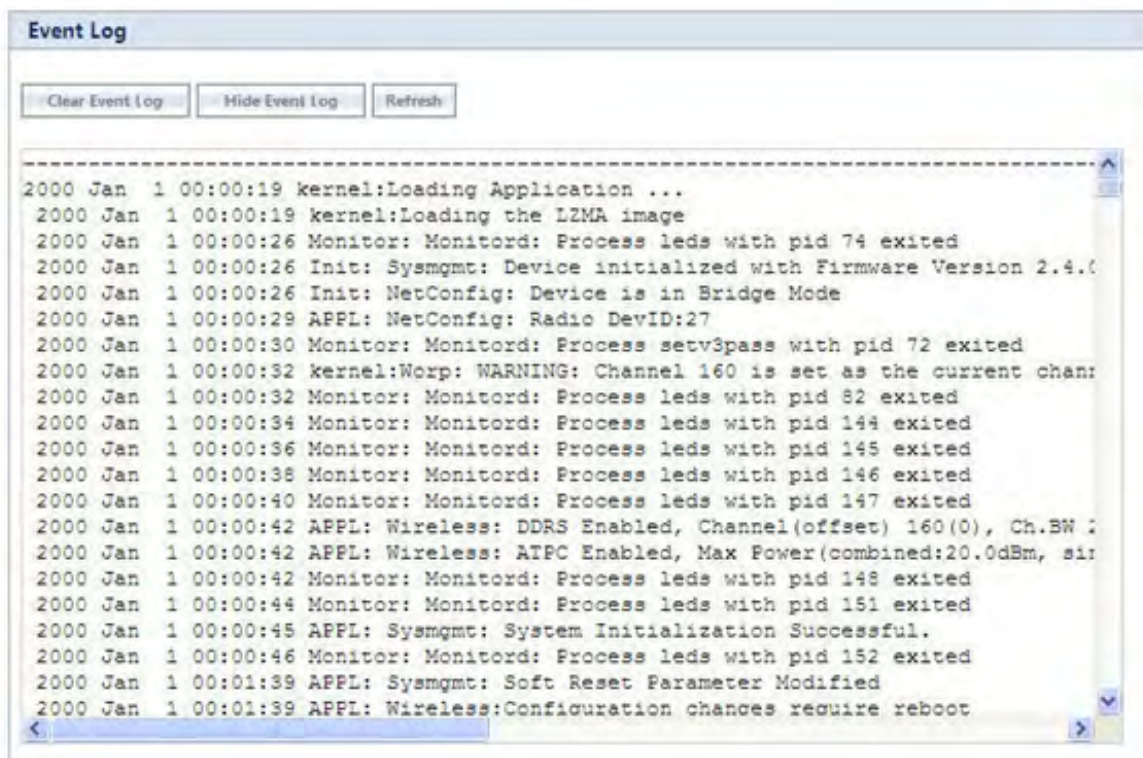
Figure 7-25 DHCP Leases

## 7.9 Logs

### 7.9.1 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 log priority is set under **MANAGEMENT > Services > Logs**), the event details are logged and can be used for any future reference or troubleshooting.

To view the Event Log, navigate to **MONITOR > Logs > Event Log**. The following **Event Log** screen appears:



```

Event Log

[Clear Event Log] [Hide Event Log] [Refresh]

-----
2000 Jan 1 00:00:19 kernel:Loading Application ...
2000 Jan 1 00:00:19 kernel:Loading the LZMA image
2000 Jan 1 00:00:26 Monitor: Monitor: Process leds with pid 74 exited
2000 Jan 1 00:00:26 Init: Sysmgmt: Device initialized with Firmware Version 2.4.(
2000 Jan 1 00:00:26 Init: NetConfig: Device is in Bridge Mode
2000 Jan 1 00:00:29 APPL: NetConfig: Radio DevID:27
2000 Jan 1 00:00:30 Monitor: Monitor: Process setv3pass with pid 72 exited
2000 Jan 1 00:00:32 kernel:Worp: WARNING: Channel 160 is set as the current chan:
2000 Jan 1 00:00:32 Monitor: Monitor: Process leds with pid 82 exited
2000 Jan 1 00:00:34 Monitor: Monitor: Process leds with pid 144 exited
2000 Jan 1 00:00:36 Monitor: Monitor: Process leds with pid 145 exited
2000 Jan 1 00:00:38 Monitor: Monitor: Process leds with pid 146 exited
2000 Jan 1 00:00:40 Monitor: Monitor: Process leds with pid 147 exited
2000 Jan 1 00:00:42 APPL: Wireless: DDRS Enabled, Channel(offset) 160(0), Ch.BW :
2000 Jan 1 00:00:42 APPL: Wireless: ATPC Enabled, Max Power(combined:20.0dBm, sir
2000 Jan 1 00:00:42 Monitor: Monitor: Process leds with pid 148 exited
2000 Jan 1 00:00:44 Monitor: Monitor: Process leds with pid 151 exited
2000 Jan 1 00:00:45 APPL: Sysmgmt: System Initialization Successful.
2000 Jan 1 00:00:46 Monitor: Monitor: Process leds with pid 152 exited
2000 Jan 1 00:01:39 APPL: Sysmgmt: Soft Reset Parameter Modified
2000 Jan 1 00:01:39 APPL: Wireless:Configuration changes require reboot

```

Figure 7-26 Event Logs

To hide the event logs, click **Hide Event Log**.

To clear the event logs, click **Clear Event Log**.

To view updated event logs, click **Refresh**.



: The recent event logs are stored in the flash memory.

## 7.9.2 Syslog

System log messages are generated by the system by sending requests at various instances to the system log server. To view System Logs, navigate to **MONITOR > Logs > Syslog**. The **Syslog** screen appears.

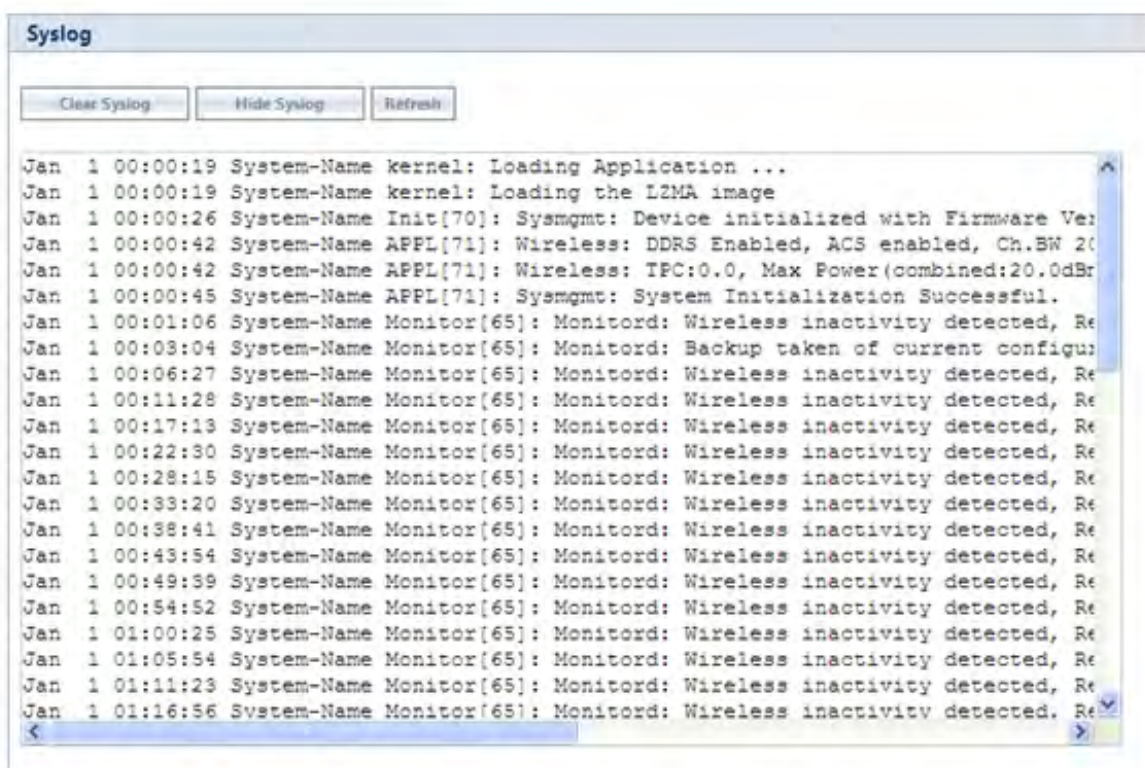


Figure 7-27 System Log

To clear Syslog information, click **Clear Syslog**.

To hide Syslog information, click **Hide Syslog**.

To refresh Syslog messages, click **Refresh**.

## 7.9.3 Debug Log

Debug Log helps you to debug issues related to important features of the device. Currently, this feature supports only DDRS and DFS. This feature helps the engineering team to get valuable information from the field to analyze the issues and provide faster solution. This feature should be used only in consultation with the Proxim Customer Support team. Once logging is enabled, the Debug Log file can be retrieved via HTTP or TFTP.

To enable Debug Log, navigate to **MONITOR > Logs > Debug Log**. The **Debug Log** screen appears:

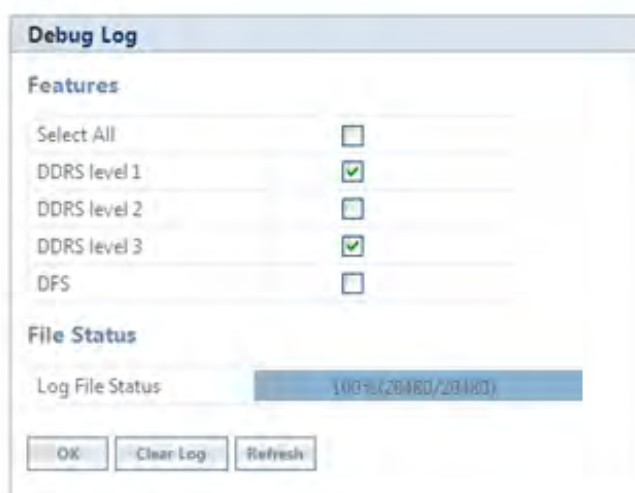


Figure 7-28 Debug Log

**Features:** Select the appropriate features to be logged. The available features are Select All, DDRS Level 1, DDRS Level 2, DDRS Level 3 and DFS.

**File Status:** This parameter displays the current size of the Debug Log file.

After selecting the **DDRS level**, click **OK**.

To delete the **Debug Log**, click **Clear Log**.

To get the updated status of the **Debug Log** File, Click **Refresh**.

## 7.9.4 Temperature Log



: Temperature Log are not applicable to Tsunami® MP-8150-CPE, Tsunami® MP-8160-CPE and Tsunami® QB-8150-EPR-12/50 devices.

Temperature Log feature reports and logs the internal temperature of the device. When the internal temperature value reaches the minimum threshold value of  $-40^{\circ}\text{C}$  or the maximum threshold temperature of  $60^{\circ}\text{C}$ , the internal temperature is logged and an SNMP trap is sent (At 5 Degrees before each limit, the device issues a warning trap). These threshold temperature values may be reconfigured but the values cannot exceed beyond the default values.



: A recording interval from one to sixty minutes with 5-minute increments can be selected. If we configure the logging interval as "0", temperature logs will be disabled.

To view and configure threshold values, and the logging interval, navigate to **MONITOR > Logs > Temperature Log**.

The threshold values of temperature are configured in Centigrade (Celsius) scale. The **Temperature Log** screen displays the **Current Device Temperature** in Celsius, along with **High Temperature** and **Low Temperature Threshold** values and **Temperature Logging Interval**. The temperature log can have a maximum size of 65 Kb; and once the limit is reached, only the last 576 logs are available. (Log storage is up to six days with the refresh time of 5 minutes).

**Temperature**

Current Unit Temperature: noSuchInstance Celsius

High Temperature Threshold: 60 (-40 to 60) in Celsius

Low Temperature Threshold: -40 (-40 to 60) in Celsius

Temperature Logging Interval: 5 (0-60) in Minutes

**Note : Set Log Interval as "0" to disable Temperature Log.**

Clear Temp Log Show Temp Log Refresh OK

Figure 7-29 Temperature Log

After configuring the parameters, click **OK**.

To view the Temperature Log, click **Show Temp Log**.

To delete all the Temperature Logs, click **Clear Temp Log**.

Click **Refresh**, to get the updated Temperature Log.

## 7.10 Tools

### 7.10.1 Wireless Site Survey



: Applicable only to a device in SU or End Point B mode.

**Wireless Site Survey** is done by the SU or End Point B only. This feature scans all the available channels according to the current Channel Bandwidth, and collects information about all BSUs or Endpoint A configured with the same network name as SUs or End Point B.

**Wireless Site Survey**

BSU Name	MAC Address	Max SUs Allowed	SUs Registered	Channel Number	Channel Bandwidth (MHz)	Rx Rate (Mbps)	Local Antenna Port Info	Local Signal (dBm)	Local Noise (dBm)	Local SNR (dB)	Registration Status
System Name	00:21:86:51:e5:0d	100	1	160	20	6.5	A1 <span style="color: green;">●</span>	-61	-100	39	Registered
							A2 <span style="color: gray;">○</span>	-	-	-	
							A3 <span style="color: green;">●</span>	-67	-100	33	

**Legends**

- Antenna Port Disabled
- Antenna Port Enabled and Singal Present

**Note: Performing Site Survey may effect the Wireless Connectivity to the BSU**

Start Refresh

Figure 7-30 Wireless Site Survey - SU Mode

To initialize the survey process, click **Start**. This process list the details of all the available BSUs or End Point A. To stop the site survey process, click **Stop**. Click **Refresh**, to get the updated Wireless Site Survey.

### 7.10.2 Scan Tool

With Scan Tool, you can scan all the devices available in your network.

To scan the devices, navigate to **MONITOR > Tools > Scan Tool**. The **Scan Tool** screen appears.

S.No.	Name	Description	MACAddress	IP Address	Subnet Mask	Default Gateway	IP Type	UP Time
1	System-Name	Tsunami MP-8100-BSU-WD v2.4.0(409070) SN-11P115010031 BL-V1.3.1	00:20:a6:11:22:31	<u>169.254.128.132</u>	255.255.255.0	169.254.128.132	Static	00:03:10:40
2	System-Name	Tsunami MP-8100-SUA-WD v2.4.0(409070) SN-11P116010026 BL-V1.3.1	00:20:a6:11:22:4b	<u>169.254.128.133</u>	255.255.255.0	169.254.128.132	Static	00:03:14:05

Figure 7-31 Scanned Devices

Click **Scan** to scan and refresh the devices on the network.

### 7.10.3 sFlow®

Proxim’s point-to-multipoint and point-to-point devices support sFlow® technology, developed by InMon Corporation. The sFlow® technology provides the ability to measure network traffic on all interfaces simultaneously by collecting, storing, and analyzing traffic data.

Depicted below is the sFlow architecture that consists of a sFlow Agent and a sFlow Receiver.

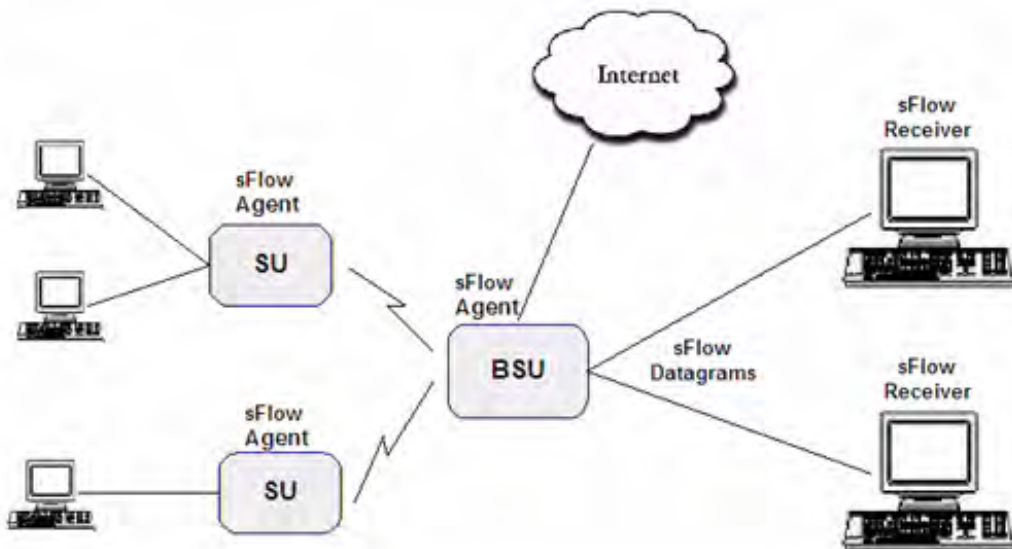


Figure 7-32 sFlow Architecture - An Example with a BSU and SUs

The **sFlow Agent**, which is running on devices, captures traffic information received on all the Ethernet interfaces, and sends sampled packets to the **sFlow Receiver** for analysis.

The sampling mechanism used to sample data are as follows:

- **Packet Flow Sampling:** In this sampling, the data packets received on the ethernet interface of the device are sampled based on a counter. With each packet received, the counter is decremented. When the counter reaches zero, the packet is packaged and sent to the sFlow Receiver for analysis. These packets are referred to as Packet Flow Samples.
- **Counter Polling Sampling:** In this sampling, the sFlow Agent sends counters periodically to the sFlow Receiver based on the set polling interval. If polling interval is set to 5 seconds then the sFlow Agent sends counters to sFlow Receiver every 5 seconds. These packets are referred to as Counter Polling Samples.

The Packet Flow Samples and Counter Polling Samples are collectively sent to the sFlow Receiver as sFlow Datagrams. It is possible to enable either or both types of sampling.

sFlow Sampling effects the system performance and hence care must be taken in configuring the sFlow parameters. To configure sFlow, navigate to **MONITOR > Tools > sFlow**. The following **sFlow®** screen appears:

**sFlow®**

Version: 1.3;Proxim Wireless Corp.,v6.4  
 Address Type: IPv4  
 Agent Address: 127.0.0.1

Receiver Configuration | Sampling Configuration | Counter Polling Configuration

S.No.	Owner	Time Out (in secs)	Max Datagram Size (200-1400)	Address Type	Receiver Address	Receiver Port (0-65535)	Datagram Version
1	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="1400"/>	ipv4	<input type="text" value="0.0.0.0"/>	<input type="text" value="6343"/>	5
2	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="1400"/>	ipv4	<input type="text" value="0.0.0.0"/>	<input type="text" value="6343"/>	5

Notes: 1. Valid Receiver IP Address and Time-out are required before configuring the owner.  
 2. Clearing the owner stops the flow sampling / counter polling.  
 3. Valid range for Time Out is 30 to 31536000 secs(365 days).

sFlow® is a registered trademark of InMon Corp.

Figure 7-33 sFLOW

This screen displays the following information about the sFlow Agent:

- **Version:** The version displayed is **1.3;Proxim Wireless Corp.; v6.4**. The version comprises the following information:
  1. **sFlow MIB Version:** Indicates the agent's MIB version. The MIB specifies how the agent extracts and bundles sampled data, and the sFlow receiver must support the agent's MIB. The sFlow MIB version is 1.3. so the sFlow Receiver's version must also be at least 1.3.
  2. **Organization:** Specifies the organization implementing sFlow Agent functionality on the device, that is, **Proxim Wireless Corp.**
  3. **Revision:** Specifies the sFlow Agent version, that is, **v6.4**.
- **Address Type:** Specifies the protocol version for IP addresses.
- **Agent Address:** Specifies the sFlow Agent's IP address.




### 7.10.3.1 sFlow Receiver Configuration

The Receiver Configuration page allows you to configure sFlow Receiver(s), which receives samples from all agents on the network, combines and analyzes the samples to produce a report of network activity.

To configure sFlow Receiver, navigate to **MONITOR > Tools > sFlow** and select **Receiver Configuration** tab.

Tabulated below is the table which explains sFlow parameters and the method to configure the configurable parameter(s):

Parameter	Description
S.No.	Represents the Receiver index number. Please note that the number of indexes depends on the ethernet interfaces your device supports.
Owner	Enter a string, which uniquely identifies the sFlow Receiver.
Time Out	Enter a value ranging from 30 to 31536000 seconds (365 days) in the <b>Time Out</b> box.  The sFlow Agent sends sampled packets to the specified sFlow Receiver till it reaches zero. At zero, all the Receiver parameters are set to default values.
Max Datagram Size	Enter the maximum size of a sFlow datagram (in bytes), which the Receiver can receive, in the <b>Max Datagram Size</b> box. By default, the maximum datagram size is set to 1400 bytes. It can range from 200 to 1400 bytes.
Address Type	The address type supported by sFlow Receiver is ipv4, which is by default selected.   : Only IPv4 is currently supported.
Receiver Address	Enter the sFlow Receiver's IP address in the <b>Receiver Address</b> box.
Receiver Port	By default, the sFlow Receiver listens to the sFlow datagrams on 6343 port. To change the port, enter a valid port ranging from 0 to 65535 in the <b>Receiver Port</b> box.
Datagram Version	The sFlow datagram version used is 5.

Click **Apply**, to save the sFlow Receiver configuration parameters.

Once the Receiver configurations are done, either Packet Flow sampling or Counter Polling Sampling or both can be started.

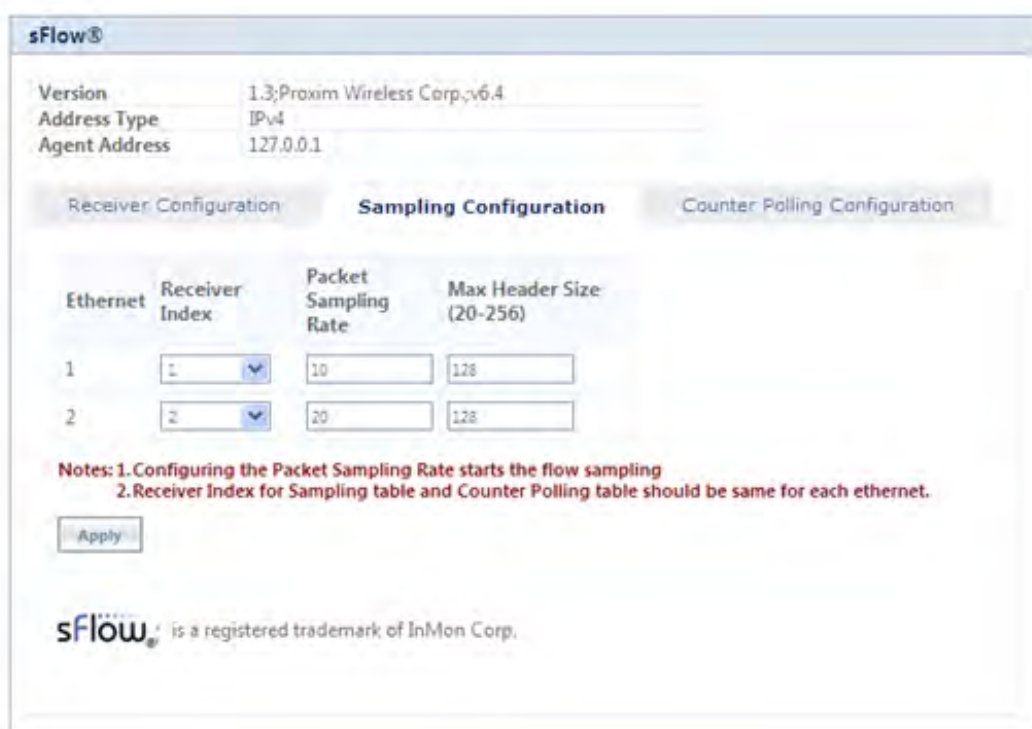


- Enabling sampling effects the system performance and hence care should be taken in setting the right values for Timeout and Max Datagram Size.
- When the Owner string is cleared, the Flow Sampling and Counter Polling stops.

### 7.10.3.2 Sampling Configuration

To configure and start packet flow sampling, do the following:

1. Navigate to **MONITOR > Tools > sFlow** and select **Sampling Configuration** tab.



Version 1.3; Proxim Wireless Corp., v6.4  
Address Type IPv4  
Agent Address 127.0.0.1

Receiver Configuration **Sampling Configuration** Counter Polling Configuration

Ethernet	Receiver Index	Packet Sampling Rate	Max Header Size (20-256)
1	1	10	128
2	2	20	128

Notes: 1. Configuring the Packet Sampling Rate starts the flow sampling  
2. Receiver Index for Sampling table and Counter Polling table should be same for each ethernet.

Apply

sflow® is a registered trademark of InMon Corp.

Figure 7-34 sFlow Sampling Configuration

- From the **Receiver Index** drop-down box, select the receiver index number associated with the sFlow Receiver to which the sFlow Agent should send the sFlow Datagrams.



: If device has two ethernet interfaces, then configure different Receiver indexes for each of the interface.

- Type a value in the **Packet Sampling Rate** box. This value determines the number of packets the sFlow Agent samples from the total number of packets passing through the ethernet interface of the device.
- Type a value in the **Maximum Header Size** box, to set the amount of data (in bytes) to be included in the sFlow datagram. The sFlow Agent samples the specified number of bytes. For example, if you set the Maximum Header Size to 100, the sFlow Agent places the first 100 bytes of every sampled frame in the datagram. The value should match the size of the frame and packet header so that the entire header is forwarded. The default size is 128 bytes. The header size can range from 20 to 256 bytes.
- Next, click **Apply** to start packet flow sampling. Once it starts, the **Time Out** parameter (see [sFlow Receiver Configuration](#)) keeps decrementing till it reaches a zero value. On reaching zero, the corresponding Receiver and Sampling values are set to default values.



- Enabling sFlow packet sampling effects the system performance, and hence care must be taken when choosing the right value for Packet Sampling Rate and Maximum Header Size.
- Receiver Index for packet Sampling table and Counter Polling table should be same for each Ethernet interface.

### 7.10.3.3 Counter Polling Configuration

To configure and start Counter Polling sampling, do the following:

1. Navigate to **MONITOR > Tools > sFlow** and select **Counter Polling Configuration** tab.

Figure 7-35 Counter Polling Configuration

2. From the **Receiver Index** drop-down box, choose the receiver index number associated with the sFlow Receiver to which the sFlow Agent sends the counters.



If Packet Flow Sampling is already configured and running, then you should configure the Receiver index same as configured in the Packet Flow Sampling for each ethernet interface.

3. Set the polling interval by typing a value in the **Interval** box. Lets say, the polling interval is set to 30 seconds. So for every 30 seconds, the counters are collected and send to the sFlow Receiver. The valid range for polling interval is 0 to  $2^{31} - 1$  seconds.
4. Next, click **Apply** to start Counter Polling Sampling. Once it starts, the **Time Out** parameter (see [sFlow Receiver Configuration](#)) keeps decrementing till it reaches a zero value. On reaching zero, the corresponding Receiver and Counter Polling values are set to default values.



- Enabling sFlow counter sampling effects the system performance, and hence care must be taken when choosing the right value sampling interval.
- Receiver Index for packet Sampling table and Counter Polling table should be same for each Ethernet interface.
- If a sampling starts and there is already another sampling running then we consider the time out value of the current/already running sampling.

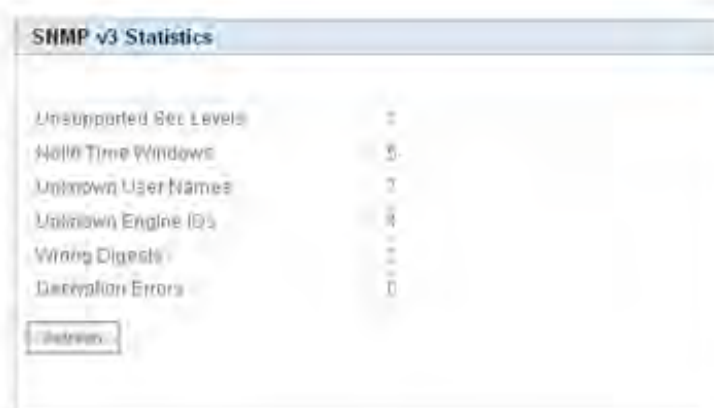
## 7.10.4 Console Commands

The **Console Commands** feature helps Proxim's Technical Support team to debug field issues.

## 7.11 SNMP v3 Statistics

SNMP v3 statistics can be viewed only when SNMPv3 feature is enabled on the device. See [SNMP](#).

To view the **SNMPv3 Statistics**, navigate to **MONITOR > SNMPV3 Statistics**. The following **SNMP v3 Statistics** screen appears:



**Figure 7-36 SNMP v3 Statistics**

The following table lists the SNMP v3 parameters and their description:

Parameter	Description
Unsupported Sec Levels	This parameter specifies the total number of packets received by the SNMP engine, which were dropped because they requested a security level that was unknown to the SNMP engine or otherwise unavailable.
Not In Time Windows	This parameter specifies the total number of packets received by the SNMP engine which were dropped because they appeared outside of the authoritative SNMP engine's window.
Unknown User Names	This parameter specifies the total number of packets received by the SNMP engine which were dropped because they correspond to an unknown user to the SNMP engine.
Unknown Engine IDs	This parameter specifies the total number of packets received by the SNMP engine which were dropped because they correspond an SNMP Engine ID that was unknown to the SNMP engine.
Wrong Digests	This parameter specifies the total number of packets received by the SNMP engine which were dropped because they did not contain the expected digest value.
Decryption Errors	This parameter specifies the total number of packets received by the SNMP engine which were dropped because they could not be decrypted.

---

# Troubleshooting



This chapter helps you to address the problems that might arise while using our device. If the procedures discussed in this chapter does not provide a solution, or the solution does not solve your problem, check our support site at <http://support.proxim.com> which stores all resolved problems in its solution database. Alternatively, you can post a question on the support site, to a technical person who will reply to your email.

Before you start troubleshooting, check the details in the product documentation available on the support site. For details about RADIUS, TFTP, Terminal and Telnet programs, and Web Browsers, refer to their appropriate documentation.

In some cases, rebooting the device solves the problem. If nothing else helps, consider a [Soft Reset to Factory Defaults](#) or a [Forced Reload](#). The Forced Reload option requires you to download a new firmware onto the device.

This chapter provides information on the following:

- [PoE Injector](#)
- [Connectivity Issues](#)
- [Surge or Lightning Issues \(For Connectorized devices\)](#)
- [Setup and Configuration Issues](#)
- [Application Specific Troubleshooting](#)
- [Wireless Link Issues](#)
- [Wired \(Ethernet\) Interface Validation](#)
- [Wireless Interface Validation](#)
- [Recovery Procedures](#)
- [Spectrum Analyzer](#)
- [Miscellaneous](#)



## 8.1 PoE Injector

Problem	Solution
The Device Does Not Work	<ul style="list-style-type: none"> <li>• Make sure that you are using a standard UTP                             <ul style="list-style-type: none"> <li>- Category 5e/6 cable in case of MP-8100-BSU, MP-8100-SUA, MP-8150-SUR, MP-8160-BSU, MP-8160-SUA, QB-8100-EPA and QB-8150-EPR devices</li> <li>- Category 5 cable in case of MP-8150-CPE, MP-8160-CPE, QB-8150-EPR-12/50</li> </ul> </li> <li>• Try a different port on the same PoE Injector hub (remember to move the input port accordingly) - if it works then there is a problem in the previous RJ45 port or a bad RJ45 port connection.</li> <li>• Try to connect the device to a different PoE Injector hub.</li> <li>• Try using a different Ethernet cable - if it works, there is probably a fault in the cable or its connection.</li> <li>• Check the power plug and hub.</li> <li>• If the ethernet link goes down, check the cable, cable type, switch and hub.</li> </ul>
There is No Data Link	<ul style="list-style-type: none"> <li>• Verify that the indicator on the device port is "ON."</li> <li>• Verify that the Ethernet cable from PoE Injector hub to the Ethernet port of the device is properly connected.</li> <li>• Make sure that you are using a standard UTP                             <ul style="list-style-type: none"> <li>- Category 5e/6 cable in case of MP-8100-BSU, MP-8100-SUA, MP-8150-SUR, MP-8160-BSU, MP-8160-SUA, QB-8100-EPA and QB-8150-EPR devices</li> <li>- Category 5 cable in case of MP-8150-CPE, MP-8160-CPE, QB-8150-EPR-12/50 devices</li> </ul> </li> <li>• The length of the cable from the Ethernet port of the device to the PoE should be less than 100 meters (approximately 325 feet).</li> <li>• Try to connect a different device to the same port on the PoE Injector hub - if it works and a link is established then there is probably a fault in the data link of the device.</li> <li>• Try to re-connect the cable to a different output port (remember to move the input port accordingly) - if it works then there is a fault probably in the output or input port of the PoE Injector hub or a bad RJ45 connection.</li> </ul>
Overload Indications	<ul style="list-style-type: none"> <li>• Connect the device to a PoE Injector.</li> <li>• Ensure that there is no short over on any of the connected cables.</li> <li>• Move the device into a different output port (remember to move the input port accordingly) - if it works then there is a fault probably in the previous RJ45 port or bad RJ45 port connection.</li> </ul>

## 8.2 Connectivity Issues

Connectivity issues include any problem that prevents from powering or connecting to the device.

Problem	Solution
Does Not Boot - No LED Activity	<ul style="list-style-type: none"> <li>• Make sure your power source is ON.</li> <li>• Make sure all the cables to the device are connected properly.</li> </ul>

Problem	Solution
Ethernet Link Does Not Work	<p>Check the Ethernet LED</p> <ul style="list-style-type: none"> <li>• <b>Solid Green:</b> The Ethernet link is up.</li> <li>• <b>Blinking Green:</b> The Ethernet link is down.</li> </ul>
Serial Link Does Not Work	<ul style="list-style-type: none"> <li>• Double-check the physical network connections.</li> <li>• Make sure your PC terminal program (such as HyperTerminal) is active and configured to the following values: <ul style="list-style-type: none"> <li>- Com Port: (COM1, COM2 and so on depending on your computer);</li> <li>- Baud rate: 115200; Data bits: 8; Stop bits: 1; Flow Control: None; Parity: None;</li> <li>- Line Feeds with Carriage Returns</li> </ul> </li> <li>• (In HyperTerminal select: <b>File &gt; Properties &gt; Settings &gt; ASCII Setup &gt; Send Line Ends with Line Feeds</b>)</li> </ul> <p> : Not applicable to Tsunami® MP-8160-CPE as it does not support serial interface.</p>
Cannot Access the Web Interface	<ul style="list-style-type: none"> <li>• Open a command prompt window and type the Ping command along with the IP address of the device. For example, <b>ping 10.0.0.1</b>. If the device does not respond, check if you have the correct IP address. If the device responds then it means the Ethernet connection is working properly.</li> <li>• Ensure that you are using Microsoft Internet Explorer 7.0 (or later) or Mozilla Firefox 3.0 (or later).</li> <li>• Ensure that you are not using a proxy server for the network connection with your Web browser.</li> <li>• Ensure that you have not exceeded the maximum number of Web Interfaces or CLI sessions.</li> <li>• Double-check the physical network connections. Use a well-known device to ensure the network connection is functioning properly.</li> <li>• Troubleshoot the network infrastructure (check switches, routers, and so on).</li> </ul> <p> : At any point of time, if the device is unable to connect to your network, reset the device by unplugging and plugging the cables from the PoE.</p>

### 8.3 Surge or Lightning Issues (For Connectorized devices)

Problem	Solution
Surge or Lighting Problem	<p>In case of any lightning or surge occurrence, check for the conditions specified below:</p> <ul style="list-style-type: none"> <li>• Check the RF signals by referring to RSSI statistics and if the signal strength has been lowered considerably, replace the Surge Arrestor.</li> <li>• Unscrew the N-Type connector at the top and visually inspect the Surge Arrestor for electrical burns. If any, replace it.</li> </ul>

## 8.4 Setup and Configuration Issues

Problem	Solution
Device Reboots Continuously	One of the reason for the device to reboot continuously is that the radio card is not properly placed in the mini-PCI slot. When you power on the device and you do not see the <b>“WIRELESS NETWORK1 PASSED”</b> in the POST message in the Serial Console, please contact Proxim’s support site at <a href="http://support.proxim.com">http://support.proxim.com</a> .
Lost Telnet or SNMP Password	Perform <a href="#">Soft Reset to Factory Defaults</a> procedure. This procedure resets system and network parameters, but does not affect the image of the device. The default HTTP, Telnet, and SNMP username is <b>admin</b> and password is <b>public</b> .
Device Responds Slowly	<p>If the device takes a long time to respond, it could mean that:</p> <ul style="list-style-type: none"> <li>• No DHCP server is available.</li> <li>• The IP address of the device is already in use. Verify that the IP address is assigned only to the device you are using. Do this by switching off the device 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 device uses a static IP address, switching to DHCP mode could solve this problem.</li> <li>• The network traffic is more.</li> </ul>
Incorrect Device IP Address	<ul style="list-style-type: none"> <li>• The default IP address assignment mode is Static and the default IP address of the device is 169.254.128.132.</li> <li>• If the IP address assignment mode is set to Dynamic, then the DHCP Server will assign an IP address automatically to the device. If the DHCP server is not available on your network, then the fall back IP address (169.254.128.132) of the device is used.</li> <li>• Use ScanTool, to find the current IP address of the device. Once you have the current IP address, use Web Interface or CLI Interface to change the device IP settings, if necessary.</li> <li>• If you are using static IP address assignment, and cannot access the device over Ethernet, refer to <a href="#">Initializing the IP Address using CLI</a>.</li> <li>• Perform <a href="#">Soft Reset to Factory Defaults</a> procedure. This will reset the device to static mode.</li> </ul>
HTTP Interface or Telnet Does Not Work	<ul style="list-style-type: none"> <li>• Make sure you are using a compatible browser: <ul style="list-style-type: none"> <li>- Microsoft Internet Explorer 7.0 or later</li> <li>- Mozilla Firefox 3.0 or later</li> </ul> </li> <li>• Make sure you have the correct IP address of the device. Enter the device IP address in the address bar of the browser, for example <b>http://169.254.128.132</b>.</li> <li>• When the <b>Enter Network Password</b> window appears, enter the User Name and and Password. The default HTTP username is <b>admin</b> and password is <b>public</b>.</li> <li>• Use CLI, to check the IP Access Table which can restrict access to Telnet and HTTP.</li> </ul>
Telnet CLI Does Not Work	<ul style="list-style-type: none"> <li>• Make sure you have the correct IP address. Enter the device IP address in the Telnet connection dialog, from a DOS prompt: <b>C:\&gt; telnet &lt;Device IP Address&gt;</b></li> <li>• Use HTTP, to check the IP Access Table which can restrict access to Telnet and HTTP.</li> <li>• Enable Telnet in Vista or Windows 7 as it is by default disabled.</li> </ul>



Problem	Solution
TFTP Server Does Not Work	<ul style="list-style-type: none"> <li>• The TFTP server is not properly configured and running</li> <li>• The IP address of the TFTP server is invalid</li> <li>• The upload or download directory is not correctly set</li> <li>• The file name is not correct</li> </ul>
Changes in Web Interface Do Not Take Effect	<ol style="list-style-type: none"> <li>1. Restart your Web browser.</li> <li>2. Log on to the device again and make changes.</li> <li>3. Reboot the device.</li> <li>4. Click <b>Commit</b> for the changes to take effect.</li> <li>5. Wait until the device reboots before accessing the device again.</li> </ol>

## 8.5 Application Specific Troubleshooting

Problem	Solution
RADIUS Authentication Server Services unavailable	<p>If RADIUS Authentication is enabled on the device, then make sure that your network's RADIUS servers are operational. Otherwise, clients will not be able to log onto the device.</p> <p>There are several reasons for the authentication server's services to be unavailable. To make it available,</p> <ul style="list-style-type: none"> <li>• Make sure you have the proper RADIUS authentication server information setup configured on the device. Check the RADIUS Authentication Server's Shared Secret and Destination Port number (default is 1812; for RADIUS Accounting, the default is 1813).</li> <li>• Make sure the RADIUS authentication server RAS setup matches the device.</li> </ul>
TFTP Server	<p>If a TFTP server is not configured and running, you will not be able to download and upload images and configuration files to or from the device. Remember that the TFTP server need not be local, as 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.</p> <p>After the TFTP server is installed:</p> <ul style="list-style-type: none"> <li>• Check to see that TFTP is configured to point to the directory containing the device Image.</li> <li>• Make sure you have the proper TFTP server IP Address, the proper device image file name, and that the TFTP server is connected.</li> <li>• Make sure the TFTP server is configured to both Transmit and Receive files (on the TFTP server's <b>Security</b> tab), with no automatic shutdown or time-out (on the <b>Auto Close</b> tab).</li> </ul>

## 8.6 Wireless Link Issues

Tabulated below are the possible reasons for a wireless link not getting established and the relevant observations.

Reason(s)	Observation
Mismatch in network name	<ul style="list-style-type: none"> <li>The Wireless Interface Statistics (In Octets, In Non-Unicast Packets) are incremented in BSU/End Point A and SU/End Point B.</li> <li>The WORP counters are not affected.</li> <li>The remote device is not listed in the Site Survey.</li> </ul>
Incorrect or invalid configured BSU/End Point A name	<ul style="list-style-type: none"> <li>The Wireless Interface Statistics (In Octets, In Non-Unicast Packets) are incremented in SU/End Point B.</li> <li>The WORP counters are not affected.</li> <li>The remote device is not listed in the Site Survey.</li> </ul>
Mismatch in network secret	<ul style="list-style-type: none"> <li>The Wireless Interface Statistics (In Octets, In Non-Unicast Packets) are incremented in BSU/End Point A and SU/End Point B.</li> <li>The WORP counters are incremented (Req for Serv, Reg Req, Auth Req, Reg Attempts, Reg LastReason: Incorrect Parameter) on both ends.</li> </ul>
Encryption set to <b>No Encryption</b> in BSU/End Point A and <b>AES Encryption</b> in SU/End Point B	<ul style="list-style-type: none"> <li>The Wireless Interface Statistics (In Octets, In Non-Unicast Packets) are incremented in BSU/End Point A; No decrypt errors are observed in SU/End Point B.</li> <li>In SU/End Point B, the WORP counters (Announcements, Req for Serv, Reg Attempts, Reg incomplete, Reg timeout, Reg Last Reason: Timeout) are incremented. In BSU/End Point A, no WORP counters are incremented except announcements.</li> <li>The remote device is not listed in the Site Survey.</li> </ul>
Encryption set to <b>AES Encryption</b> in BSU/End Point A and <b>No Encryption</b> in SU/End Point B	<ul style="list-style-type: none"> <li>The Wireless Statistics counters and WORP counters are not incremented in SU/End Point B.</li> <li>The remote device is not listed in the Site Survey.</li> </ul>
Encryption set to <b>AES Encryption</b> in both BSU/End Point A and SU/End Point B. A mismatch in Encryption key	<ul style="list-style-type: none"> <li>The Wireless Interface Statistics (In Octets, In Non-Unicast Packets) are incremented only in SU/End Point B.</li> <li>The remote device is not listed in the Site Survey.</li> </ul>
BSU exceeds the maximum SU limit	<ul style="list-style-type: none"> <li>The Wireless Interface Statistics (In Octets, In Non-Unicast Packets) are incremented in SU/End Point B but fails to authenticate.</li> <li>The WORP counters (Announcements, Req for Serv, Reg Attempts, Reg Incompletes, Reg Timeouts, Reg Last Reason: Timeout) are incremented in SU/End Point B.</li> <li>The remote device is listed in the Site Survey.</li> </ul>

## 8.7 Wired (Ethernet) Interface Validation

Problem	Solution
Wired (Ethernet) Interface Validation	Run iperf commands <ul style="list-style-type: none"> <li>• Use iperf commands with -w option as 202k. The throughput is expected to be equal in both directions and should be comparable from laptop to laptop or desktop to desktop performance</li> </ul> If the above throughput value is not in the expected range, <ul style="list-style-type: none"> <li>• Check speed and duplex settings between the device and Personal Computer or switch or router connected</li> <li>• Make sure the connection established is of same speed and full duplex is as expected (10 or 100 or 1000)</li> <li>• With auto negotiation, if you notice this issue, then try manually setting the speed and duplex</li> <li>• Update the Ethernet driver in the Personal Computer to the latest one</li> </ul>

## 8.8 Wireless Interface Validation

Problem	Solution
<p>Wireless Interface Validation</p>	<p><b>Run iperf commands</b> (You can run Embedded iperf commands only through Telnet.)</p> <ul style="list-style-type: none"> <li>• iperf -s -w 202k (command for iperf server)</li> <li>• Iperf -c ipaddress -w 202k -t time Period -l &lt;intermediateResultInterval&gt; -P &lt;4 or 6&gt; (command to run iperf client) <ul style="list-style-type: none"> <li>- Ipaddress -&gt; of the SU/End Point B or BSU/End Point A device where the iperf server is running</li> <li>- P -&gt; No of pairs (Streams)</li> </ul> </li> <li>• Use -d option to run bidirectional throughput</li> <li>• Use -r option to run unidirectional throughput one after another without changing the server and SU ends</li> </ul> <p>If the expected throughput is not achieved, then check the following:</p> <ul style="list-style-type: none"> <li>• <b>Antenna Alignment</b> <ul style="list-style-type: none"> <li>- Note whether the antenna ports are balanced - SNR/RSSI provided for Local and Remote in the BSU/SU Link Statistics page or by using “aad” command</li> <li>- Signal difference of &lt;=5 dBm is considered as balanced and recommended</li> <li>- If the chains are not balanced, then look at the alignment and connectors of RF cables, used between antenna and device</li> <li>- If in RMA (Returned from Customer), check the RF cable to radio port connectivity</li> <li>- Avoid nearby metal surfaces, if you are using Omni antenna</li> </ul> </li> <li>• <b>Data Streams</b> <ul style="list-style-type: none"> <li>- Select “Single” stream instead of “Dual” stream mode</li> <li>- DDRS - with single stream data rate or with Auto mode</li> </ul> <p>Dual stream data rates can be used only when the signal in both antenna ports is balanced</p> </li> <li>• <b>Antenna Port Selection</b> <ul style="list-style-type: none"> <li>- For MP81x0-BSU/SU or QB81x0 devices, make sure you are either enabling all antenna ports for 3*3 MIMO or using A1 and A3 antenna ports for 2*2 MIMO mode</li> <li>- For MP8160-BSU/SU use A1 and A2 antenna ports for 2*2 MIMO</li> <li>- For using single stream, it is mandatory to select antenna port A1</li> <li>- Enabling all antenna port will not cause any issue even if it is not in use.</li> </ul> </li> <li>• <b>Bad Channel</b> <ul style="list-style-type: none"> <li>- Check for CRC errors, PHY errors, WOPR Retries and WOPR Failures in Monitor Interface Statistics page. If this count increments steadily (Refreshing the web page is required) then <ul style="list-style-type: none"> <li>• Either change the channel and check for a better channel</li> <li>• Use Wi-Spy or similar tool and check the environment for better channel</li> </ul> </li> </ul> </li> <li>• <b>Data Rate Issues</b> <ul style="list-style-type: none"> <li>- Ensure same data rates are selected if you are using fixed data rate between BSU/SU and End Point A/End Point B to have predictable throughput and link</li> <li>- Alternative, use DDRS with Auto mode enabled</li> </ul> </li> </ul>

Problem	Solution
Wireless Interface Validation	<ul style="list-style-type: none"> <li>• <b>Performance and Stability Issues</b> <ul style="list-style-type: none"> <li>- Check the distance between two co-locating devices. The distance between two co-locating devices should be minimum 3 meters, in order to achieve good throughput and maintain link stability. The operating channels should maintain 5MHz spacing if managed by a single administrator.</li> <li>- When DDRS is disabled, check the Minimum Required SNR for the current data rate by navigating to <b>MONITOR --&gt; WORP Statistics --&gt; Interface 1 --&gt; Link Statistics Page --&gt; Click here for Local SNR-Table</b>. If the current SNR is not meeting the minimum required SNR criteria for the current data rate, then accordingly reduce the data rate.</li> <li>- If SNR is more than the maximum optimal SNR limit (<b>MONITOR --&gt; WORP Statistics --&gt; Interface 1 --&gt; Link Statistics Page --&gt; Click here for Local SNR-Table</b>) then it causes radio receiver saturation thus impacting the performance of the link. To overcome this situation, set the TPC appropriately or enable ATPC to adjust the signal level automatically. Also, enabling DDRS can help in choosing right data rate automatically.</li> </ul> </li> </ul>

## 8.9 Recovery Procedures

### 8.9.1 Soft Reset to Factory Defaults

Use this procedure to reset the network configuration values, including the Password, IP Address, and Subnet Mask. This procedure resets configuration settings, but does not change the current device Image.

To use this procedure, in the web interface navigate to **MANAGEMENT > Reset to Factory**.

The device gets the default IP address (169.254.128.132). You can change the IP address using Web Interface or CLI. If you do not have access to the HTTP or CLI interfaces, use [Hard Reset to Factory Defaults](#) procedure.

### 8.9.2 Hard Reset to Factory Defaults

If you cannot access the device or you have lost its password, you can reset the device to its factory default settings by using the Reload button available on the PoE injector. With Reload, the configuration settings are deleted from the device and the device reboots, using a factory default configuration.



- Please note that if the PoE supplied with the Product Package is not equipped with the Reload functionality then you will have to use a PoE which is equipped with the Reload functionality to reset the device to its factory defaults.
- You need to use a pin or the end of a paperclip to press the Reload button.



**If you hold the Reload button for longer than 10 seconds, the device may go into Forced Reload mode, which erases the device embedded software. This software must be reloaded through an ethernet connection with access to a TFTP Server. See [Forced Reload](#) for instructions.**

### 8.9.3 Forced Reload

With Forced Reload, you bring the device into bootloader mode which erases the embedded software. Use this procedure only as a last option if the device does not boot, and the Soft and Hard to Factory Defaults procedure does not help.



**: With Forced Reload, the embedded software in the device will be erased. You will need to reload the software before the device is operational.**

The device will try to load the image 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 image to the device:

- [Download a New Image Using Proxim's ScanTool](#)
- [Download a New Image Using the Bootloader CLI](#)

As the CLI requires a physical connection to the device serial port, Proxim recommends you to use the ScanTool option.



**: You cannot download a new image using Bootloader CLI onto Tsunami® MP-8160-CPE as it does not provide serial interface support to the user.**

#### 8.9.3.1 Download a New Image Using Proxim's ScanTool

To download the device image, 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 automatically detects the device that does not have a valid software image. The **TFTP Server** and **Image File Name** parameters are enabled in the ScanTool's **Change** screen so that you can download a new image to the device. (These fields are disabled, if ScanTool does not detect a software image problem). See [Initialization](#).

#### Preparing to Download the Device Image

Before starting the download process, you need to know the device IP Address, Subnet Mask, the TFTP Server IP Address, and the Image file name. Make sure the TFTP server is running and properly configured to point to the folder containing the image to be downloaded.

#### Download Procedure

Follow these steps to download a software image to the device by using ScanTool:

1. Download the latest software from <http://support.proxim.com>.
2. Copy the latest software updates to your TFTP server.
3. Launch Proxim's ScanTool.
4. Highlight the entry for the device that you want to update and click **Change**.
5. Set **IP Address Type** to **Static**.



**: You need to assign static IP information temporarily to the device since its DHCP client functionality is not available when no image is installed on the device.**

6. 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.
7. Enter the network's **Subnet Mask**.

8. Enter the network's **Gateway IP Address**, if necessary. You may need to contact your Network Administrator to get this address. You need to enter the default gateway address (169.254.128.133) only if the device and the TFTP server are separated by a router.
9. By default, the IP address of the TFTP server is provided.
10. By default, the image file name is provided.
11. Click **OK**. The device will reboot and the download starts automatically.
12. Click **OK** when prompted to return to the **Scan List** screen after the device has been updated successfully.
13. Click **Cancel** to close the ScanTool.

When the download process is complete, start configuring the device.

### 8.9.3.2 Download a New Image Using the Bootloader CLI

To download the new device image, 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 an Ethernet cable.

You must also connect the device to a computer with a standard serial cable and use a terminal client. From the terminal, enter the CLI commands to set the IP address of the device and to download the device image.

#### Preparing to Download the device image

Before starting, you need to know the device IP Address, Subnet Mask, the TFTP Server IP Address, and the device image file name. Make sure the TFTP server is running and configured to point to the default directory containing the image to be downloaded.

#### 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. Connect the device serial port to your computer's serial port.
4. Open your terminal emulator program and set the following connection properties:
  - **Com Port:** COM1, COM2 and so on, 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.

Terminal Emulator program sends a line return at the end of each line of code.

The terminal display shows Power On Self Tests (POST) activity. After approximately 30 seconds, a message indicates: **Starting ScanTool interface, press any key to enter CLI 5**". After this message appears, press any key. Now the bootloader prompt appears as below:

```
Bootloader=>
```

6. Enter the following commands:

```
Bootloader=> show (to view configuration parameters and values)
Bootloader=> set ipaddr <Access Point IP Address>
Bootloader=> set serverip <TFTP Server IP Address>
Bootloader=> set filename <Device 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 169.254.128.133
Bootloader=> set filename image_proxim.sei
Bootloader=> set gatewayip 169.254.128.133
Bootloader=> set netmask 255.255.255.0
Bootloader=> set ipaddrtype static
Bootloader=> show
Bootloader=> reboot
```

The device will reboot and then download the image file. When the download process is complete, configure the device.

### 8.9.4 Setting IP Address using Serial Port

If the ScanTool fails to scan the device and users knows the login credentials then you can set the IP address for the device using serial port.

#### 8.9.4.1 Hardware and Software Requirements

- Standard serial (RS-232) cable
- ASCII Terminal software

#### 8.9.4.2 Attach the Serial Port Cable

1. Connect one end of the serial cable to the device and the other end to a serial port on your computer.
2. Power on the computer and the device.

#### 8.9.4.3 Initializing the IP Address using CLI

After connecting the cable to the serial port, you can use the CLI to communicate with the device. CLI supports the most-generic terminal emulation programs. In addition, many web sites offer shareware or commercial terminal programs that you can download. Once the IP address has been assigned, you can use the HTTP interface or the Telnet to complete the configuration.

Follow these steps to assign an IP address to the device:

1. Open your terminal emulation program and set the following connection properties:
  - **Com Port:** COM1, COM2, and so on depending on your computer
  - **Baud Rate:** 115200
  - **Data Bits:** 8
  - **Stop Bits:** 1
  - **Flow Control:** None
  - **Parity:** None

The terminal display shows Power On Self Tests (POST) activity, and then displays the software version. It prompts you to enter the CLI username and password. The commands to enter the username and password are as follows:

```
##### |
# +---+---+---+---+---+
# |p| |r| |o| |x| |i| |m|
# +---+---+---+---+---+
# Version: 1.0.0 B208100
```



```
# Architecture: MIPS 7660
# Creation: 10-Aug-2009 (IST) 08:16:14 PM
#####|
Username: admin
Password:
```

This process may take up to 90 seconds.

2. Enter the CLI Username and password. By default username is **admin** and password is **public**. The terminal displays a welcome message and then the CLI Prompt. Enter 'show ip' as shown below:

```
System Name> show ip
```

The following Ethernet IP information is displayed:

```
// Ethernet IP CONFIGURATION //
INDEX 1
IP Address : 10.0.0.1
Mask : 255.255.255.0
Address Type : static

// IP Gateway Configuration //
Gateway IP Address : 169.254.128.1
```

3. Change the IP address and other network values using the following CLI commands (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)# rowedit 1 ipaddress <ipaddress>
System Name(config-net-ip-etherip)# rowedit 1 mask <subnet mask>
System Name(config-net-ip-etherip)# rowedit 1 address-type <Address Type>
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
```

4. After the device reboots, verify the new IP address by reconnecting to the CLI. Alternatively, you can ping the device from a network computer to confirm that the new IP address has taken effect.

When a proper IP address is set, use HTTP interface or Telnet to configure the rest of the operating parameters of the device.

## 8.10 Spectrum Analyzer

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°, one can check the direction of the interference. 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.

### 8.10.1 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:

- Change the channel to a frequency that has no or least interference.
- Try changing the antenna polarization.
- 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.
- Adjusting the antenna angle/height can help to reduce the interference.

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.

### 8.10.2 Conclusion

A spectrum analyzer can be a great help to identify whether interference might be causing link problems on the device. 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.

## 8.11 Miscellaneous

### 8.11.1 Unable to Retrieve Event Logs through HTTPS

If using Internet Explorer 7 and are not able to retrieve event logs through HTTPS, do the following:

1. Open Internet Explorer
2. Navigate to **Tool > Internet Options > Advanced**
3. Go to **Security** and uncheck/unselect **Do not save encrypted pages to disk**

Alternatively, use Mozilla Firefox 3.5 or later.

# Feature Applicability



Tabulated below are the feature(s) applicable to the respective devices:

Feature Name	Bridge Mode	Routing Mode	MP-8100-BSU	MP-8160-BSU	MP-8100-SUA MP-8150-SUR	MP-8160-SUA	QB-8100-EPA QB-8150-EPR		MP-8150-CPE	MP-8160-CPE	QB-8150-EPR-12/50		Comments
							End Point A	End Point B			End Point A	End Point B	
Maximum MTU Size	Yes	Yes	No	No	No	No	No	No	Yes	Yes	Yes	Yes	
Advanced Ethernet Properties	Yes	Yes	No	No	No	No	Yes	Yes	No	No	No	No	
Sleep Mode	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No	Yes - only when configured in BSU mode.
Channel Offset	Yes	Yes	No	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	
Legacy Mode	Yes	Yes	Yes	No	No	No	No	No	No	No	No	No	Yes - only when configured in BSU mode.
ATPC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
DPS	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	No	Yes	Yes	
Manual Blacklist	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
DDRS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Wireless Security None WEP TKIP	Yes	Yes	Yes	No	No	No	No	No	No	No	No	No	
Wireless Security AES-CCM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
RADIUS Security	Yes	Yes	Yes	Yes	No	No	Yes	No	No	No	Yes	No	Yes - only when configured in BSU mode.
MAC ACL	Yes	Yes	Yes	Yes	No	No	Yes	No	No	No	Yes	No	Yes - only when configured in BSU mode.
QoS	Yes	Yes	Yes	Yes	No	No	Yes	No	No	No	Yes	No	QoS is configurable only on BSU but applied to both BSU and SU
VLAN - Transparent and Trunk Mode	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
VLAN - Access Mode	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
VLAN - QinQ	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
VLAN over RADIUS	Yes	No	No	No	Yes	Yes	No	No	Yes	Yes	No	No	VLAN configuration for SUs can be configured in the RADIUS server.
QoS over RADIUS Filtering	Yes	Yes	No	No	Yes	Yes	No	No	Yes	Yes	No	No	QoS class for each SU can be configured in the RADIUS server.
WORP Intra Cell Blocking	Yes	No	Yes	Yes	No	No	No	No	No	No	No	No	Yes - only when configured in BSU mode.
DHCP Server	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
DHCP Relay	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
IGMP Snooping	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Static Route Table	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
NAT	No	Yes	No	No	Yes	Yes	No	Yes	Yes	Yes	No	Yes	
RIP	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
PPPoE client	No	Yes	No	No	Yes	Yes	No	No	Yes	Yes	No	No	
P in P	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
SNMPv1-v2c and v3	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
SNTP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Management Access Control	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
QB-EP to SU	Yes	Yes	No	No	No	No	Yes	Yes	No	No	No	No	
Sflow	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Wireless Site Survey	Yes	Yes	No	No	Yes	Yes	No	Yes	Yes	Yes	No	Yes	
STP/LACP Passthru	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	

## Parameters Requiring Reboot

# B

Tabulated below are the device parameters that require reboot for the changes to take effect:

Parameter(s)	Web Page(s)	Applicable Device Mode*
<b>System Configuration</b>		
Radio Mode	BASIC CONFIGURATION ADVANCED CONFIGURATION -> System	All
Frequency Domain	BASIC CONFIGURATION ADVANCED CONFIGURATION -> System	All
Network Mode	ADVANCED CONFIGURATION -> System	All
Frequency Filter Lower Edge	ADVANCED CONFIGURATION -> System	All
Frequency Filter Upper Edge	ADVANCED CONFIGURATION -> System	All
<b>IP Configuration (Bridge Mode)</b>		
Ethernet	BASIC CONFIGURATION ADVANCED CONFIGURATION -> Network -> IP Configuration	All
Default Gateway IP Address		All
DNS		All
<b>IP Configuration (Routing Mode)</b>		
Ethernet	BASIC CONFIGURATION ADVANCED CONFIGURATION -> Network -> IP Configuration	All
Wireless		All
Wireless (With PPPoE)		SU Mode
Default Gateway IP Address		All
DNS (Primary and Secondary Address)		All
<b>NAT</b>		
Status	ADVANCED CONFIGURATION -> Network -> NAT	SU Mode / End Mode B mode
Dynamic Start Port	ADVANCED CONFIGURATION -> Network -> NAT	SU Mode / End Mode B mode
Dynamic End Port	ADVANCED CONFIGURATION -> Network -> NAT	SU Mode / End Mode B mode
<b>PPPoE</b>		
Status	ADVANCED CONFIGURATION -> Network -> PPPoE Client	SU Mode

## Parameters Requiring Reboot

Parameter(s)	Web Page(s)	Applicable Device Mode*
<b>Ethernet Interface Properties</b>		
Admin Status	ADVANCED CONFIGURATION -> Network -> Ethernet	
<b>Wireless Properties</b>		
Channel Bandwidth	BASIC CONFIGURATION ADVANCED CONFIGURATION -> Wireless -> Properties	
Channel Offset	ADVANCED CONFIGURATION -> Wireless -> Properties	Applicable only to, <ul style="list-style-type: none"> <li>• Tsunami® MP-8160-BSU</li> <li>• Tsunami® MP-8160-SUA</li> <li>• Tsunami® MP-8160-CPE</li> <li>• Tsunami® MP-8150-CPE</li> <li>• Tsunami® QB-8150-EPR-12/50</li> </ul>
Frequency Extension	ADVANCED CONFIGURATION -> Wireless -> MIMO Properties	All
<b>Upgrade Firmware and Configuration</b>		
Upgrade Firmware	MANAGEMENT -> File Management -> Upgrade Firmware	All
Upgrade Configuration	MANAGEMENT -> File Management -> Upgrade Configuration	All
<b>HTTP / HTTPS</b>		
Admin Password	MANAGEMENT -> Services -> HTTP / HTTPS	All
Monitor Password		All
HTTP		All
HTTP Port		All
HTTPS		All
<b>Telnet / SSH</b>		
Admin Password	MANAGEMENT -> Services -> Telnet / SSH	All
Monitor Password		All
Telnet		All
Telnet Port		All
Telnet Sessions		All
SSH		All
SSH Port		All
SSH Sessions		All
<b>SNMP (If SNMP v1-v2c is enabled)</b>		

## Parameters Requiring Reboot

Parameter(s)	Web Page(s)	Applicable Device Mode*
SNMP	MANAGEMENT -> Services -> SNMP	All
Version		All
Read Password		All
Read / Write Password		All
SNMP Trap Host Table		All
<b>SNMP (If SNMP v3 is enabled)</b>		
SNMP	MANAGEMENT -> Services -> SNMP	All
Version		All
Security Level		All
Priv Protocol		All
Priv Password		All
Auth Protocol		All
Auth Password		All
SNMP Trap Host Table		All
<b>Management Access Control</b>		
Access Table Status	MANAGEMENT -> Access Control	All
Management Access Control Table		All
<b>Reset to Factory</b>	MANAGEMENT -> Reset to Factory	All
<b>Convert QB to MP</b>	MANAGEMENT -> Convert QB to MP	Applicable only to <ul style="list-style-type: none"> <li>• Tsunami® QB-8100-EPA</li> <li>• Tsunami® QB-8150-EPR</li> </ul>

\* **BSU**: Refers to a Base Station

**SU Mode**: Refers to both SU and CPE

**End Point A Mode**: Refers to a device in End Point A mode

**End Point B Mode**: Refers to a device in End Point B mode

# Frequency Domains and Channels



## Introduction

The Tsunami® Point-to-point and Point-to-multipoint products are available in two SKUs: United States (US) and rest of the 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 following table lists all the Tsunami® products with their respective Frequency domains and SKUs supported.

Product	Supported Frequency Band	Supported SKUs
Tsunami® MP-8100-BSU	2.3 - 2.5 GHz and 4.9 - 6.0 GHz	US, World
Tsunami® MP-8100-SUA	2.3 - 2.5 GHz and 4.9 - 6.0 GHz	US, World
Tsunami® MP-8150-SUR	4.9 - 6.0 GHz	US, World
Tsunami® MP-8150-CPE	5.3 - 6.1 GHz	US, World
Tsunami® MP-8160-BSU	5.9 - 6.4 GHz	World
Tsunami® MP-8160-SUA	5.9 - 6.4 GHz	World
Tsunami® MP-8160-CPE	5.9 - 6.4 GHz	World
Tsunami® QB-8100-EPA	2.3 - 2.5 GHz and 4.9 - 6.0 GHz	US, World
Tsunami® QB-8150-EPR	4.9 - 6.0 GHz	US, World
Tsunami® QB-8150-LNK-12/50	5.3 - 6.1 GHz	US, World

The frequency domains can be easily configured using the Web Interface as it is a drop down list with all the available domains. When the device is configured with CLI or 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:

Frequency Domain	ENUM Value
<b>US SKU</b>	
United States 5.8 GHz	2
United States 2.4 GHz	3
United States2 (5.3 to 5.8 GHz)	22
<b>World SKU</b>	
United States 5 GHz	1
World 5 GHz	4
World 4.9 GHz	5
World 2.4 GHz	6

World 2.3 GHz	7
World 2.5 GHz	8
Canada 5 GHz	9
Europe 5.8 GHz	10
Europe 5.4 GHz	11
Europe 2.4 GHz	12
Russia 5 GHz	13
Taiwan 5 GHz	14
United States 5 GHz	15
Canada 5.8 GHz	16
World 6.4 GHz	17
UK 5.8 GHz	20
World 5.9 GHz	21
India 5.8 GHz	23
Brazil 5.4 GHz	24
Brazil 5.8 GHz	25
Australia 5.4 GHz	26
Australia 5.8 GHz	27

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

```
T8000-Cl:65:7E(config)# system-configure
T8000-Cl:65:7E(config-sysconfig)# network-mode bridge
Changes in Network mode requires Reboot.
T8000-Cl:65:7E(config-sysconfig)# frequency-domain ?
Possible completions:

<Use 'show supported-frequency-domains' to get supported frequency domains
list>
Frequency Domain Configuration
T8000-Cl:65:7E(config-sysconfig)# frequency-domain 4
Changes in Frequency Domain requires Reboot.
T8000-Cl:65:7E(config-sysconfig)#exit
T8000-Cl:65:7E(config)#exit
```



## 2.4 GHz Channels

2.4 GHz frequency band is supported by the following devices:

- Tsunami® MP-8100-BSU
- Tsunami® MP-8100-SUA
- Tsunami® QB-8100-EPA

Frequency Domain	Frequency Band (Start Frequency ~ End Frequency in MHz)	Allowed Channels (Center Frequency in GHz)				
		5 MHz	10 MHz	20 MHz	40 PLUS MHz	40 MINUS MHz
<b>US SKU</b>						
United States 2.4 GHz	2412 ~ 2462	1 (2412), 2 (2417), 3 (2422)... 11 (2462).	1 (2412), 2 (2417), 3 (2422)... 11 (2462).	1 (2412), 2 (2417), 3 (2422)... 11 (2462).	1 (2412), 2 (2417), 3 (2422)... 7 (2442).	5 (2432), 6 (2437), 7 (2442)... 11 (2462).
<b>World SKU</b>						
World 2.3 GHz	2277 ~ 2397	100 (2277), 101 (2282), 102 (2287), 103 (2292)... 124 (2397).	100 (2277), 101 (2282), 102 (2287), 103 (2292)... 123 (2392).	101 (2282), 102 (2287), 103(2292)... 122 (2387).	101 (2282), 102 (2287), 103 (2292)... 118 (2367).	105 (2302), 106(2307), 107(2312)... 122 (2387).
World 2.4 GHz	2412 ~ 2472	1 (2412), 2 (2417), 3 (2422)... 13 (2472).	1 (2412), 2 (2417), 3 (2422)... 13 (2472).	1 (2412), 2 (2417), 3 (2422)... 13 (2472).	1 (2412), 2 (2417), 3 (2422)... 9 (2452).	5 (2432), 6 (2437), 7 (2442)... 13 (2472).
World 2.5 GHz	2477 ~ 2507	200(2477), 201(2482), 202 (2487), 203(2492), 204(2497), 205 (2502), 206(2507).	200(2477), 201(2482), 202 (2487), 203(2492), 204(2497), 205 (2502), 206 (2507).	201(2482), 202 (2487), 203(2492), 204(2497), 205 (2502).	201(2482)	205(2502)
Europe 2.4 GHz	2412 ~ 2472	1 (2412), 2 (2417), 3 (2422)... 13 (2472).	1 (2412), 2 (2417), 3 (2422)... 13 (2472).	1 (2412), 2 (2417), 3 (2422)... 13 (2472).	1 (2412), 2 (2417), 3 (2422)... 9 (2452).	5 (2432), 6 (2437), 7 (2442)... 13 (2472).

## 5 GHz Channels

5 GHz frequency band is supported by the following devices:

- Tsunami® MP-8100-BSU
- Tsunami® MP-8100-SUA
- Tsunami® MP-8150-SUR
- Tsunami® QB-8100-EPA
- Tsunami® QB-8150-EPR
- Tsunami® MP-8150-CPE
- Tsunami® QB-8150-EPR-12/50

Frequency Domain	Frequency Band (Start Frequency ~ End Frequency in MHz)	Allowed Channels (Center Frequency in GHz)				
		5 MHz	10 MHz	20 MHz	40 PLUS MHz	40 MINUS MHz
<b>US SKU</b>						
United States 5.8 GHz	5740 ~ 5830 (Non-DFS)	148(5740), 149(5745)... 165(5825), 166(5830).	149(5745), 150(5750)... 164(5820), 165(5825).	149(5745), 150(5750)... 164(5820), 165(5825).	149(5745), 150(5750)... 160(5800), 161(5805).	153(5765), 154(5770)... 164(5820), 165(5825).
United States2 (5.3, 5.8 GHz)	5255 ~ 5325 (DFS) 5740 ~ 5830 (Non-DFS)	51(5255), 52(5260)... 64(5320), 65(5325). 148(5740), 149(5745)... 165(5825), 166(5830).	52(5260), 53(5265)... 63(5315), 64(5320). 149(5745), 150(5750)... 164(5820), 165(5825).	52(5260), 53(5265)... 63(5315), 64(5320). 149(5745), 150(5750)... 164(5820), 165(5825).	52(5260), 53(5265)... 59(5295), 60(5300). 149(5745), 150(5750)... 160(5800), 161(5805).	56(5280), 57(5285)... 63(5315), 64(5320). 153(5765), 154(5770)... 164(5820), 165(5825).
<b>World SKU</b>						
United States 5 GHz	5255 ~ 5325 (DFS) 5495 ~ 5585 (DFS) 5655 ~ 5830 (Non-DFS)	51(5255), 52(5260)... 64(5320), 65(5325). 99(5495), 100(5500)... 116(5580), 117(5585). 131(5655), 132(5660)... 140(5700), 141(5705). 148(5740), 149(5745)... 165(5825), 166(5830).	52(5260), 53(5265)... 63(5315), 64(5320). 100(5500), 101(5505)... 115(5575), 116(5580). 132(5660), 133(5665)... 139(5695), 140(5700). 149(5745), 150(5750)... 164(5820), 165(5825).	52(5260), 53(5265)... 63(5315), 64(5320). 100(5500), 101(5505)... 115(5575), 116(5580). 132(5660), 133(5665)... 139(5695), 140(5700). 149(5745), 150(5750)... 164(5820), 165(5825).	52(5260), 53(5265)... 59(5295), 60(5300). 100(5500), 101(5505)... 111(5555), 112(5560). 132(5660), 133(5665)... 135(5675), 136(5680). 149(5745), 150(5750)... 160(5800), 161(5805).	56(5280), 57(5285)... 63(5315), 64(5320). 104(5520), 105(5525)... 115(5575), 116(5580). 136(5680), 137(5685)... 139(5695), 140(5700). 153(5765), 154(5770)... 164(5820), 165(5825).

## Frequency Domains and Channels

Frequency Domain	Frequency Band (Start Frequency ~ End Frequency in MHz)	Allowed Channels (Center Frequency in GHz)				
		5 MHz	10 MHz	20 MHz	40 PLUS MHz	40 MINUS MHz
World 5 GHz	5155 ~ 6075 (Non-DFS)	31(5155), 32(5160)... 214(6070), 215(6075).	31(5155), 32(5160)... 214(6070), 215(6075).	32(5160), 33(5165)... 213(6065), 214(6070).	32(5160), 33(5165)... 209(6045), 210(6050).	36(5180), 37(5185)... 213(6065), 214(6070).
WORLD 4.9 GHz*	4905 ~ 4995 (Non-DFS)	181(4905), 182(4910)... 188(4940). 10(4945), 20(4950)... 110(4995)	181(4905), 182(4910)... 188(4940). 10(4945), 20(4950)... 110(4995)	182(4910), 183(4915)... 188(4940). 10(4945), 20(4950)... 100(4990)	182(4910), 183(4915)... 188(4940). 10(4945), 20(4950)... 60(4970)	186(4930), 187(4935), 188(4940), 10(4945), 20(4950)... 100(4990)
WORLD 5.9 GHz*	5880 ~ 5920 (Non-DFS)	176(5880), 177(5885)... 183(5915), 184(5920).	176(5880), 177(5885)... 183(5915), 184(5920).	177(5885), 178(5890)... 182(5910), 183(5915).	177(5885), 178(5890), 179(5895).	181(5905), 182(5910), 183(5915).
CANADA 5 GHz	5255 ~ 5325 (DFS) 5495 ~ 5585 (DFS) 5655 ~ 5705 (DFS)	51(5255), 52(5260)... 64(5320), 65(5325). 99(5495), 100(5500)... 116(5580) 117(5585). 131(5655), 132(5660)... 140(5700), 141(5705).	52(5260), 53(5265)... 63(5315), 64(5320). 100(5500), 101(5505)... 115(5575), 116(5580). 132(5660), 133(5665)... 139(5695), 140(5700).	52(5260), 53(5265)... 63(5315), 64(5320). 100(5500), 101(5505)... 115(5575), 116(5580). 132(5660), 133(5665)... 139(5695), 140(5700).	52(5260), 53(5265)... 59(5295), 60(5300). 100(5500), 101(5505)... 111(5555), 112(5560). 132(5660), 133(5665)... 135(5675), 136(5680).	56(5280), 57(5285)... 63(5315), 64(5320). 104(5520), 105(5525)... 115(5575), 116(5580). 136(5680), 137(5685)... 139(5695), 140(5700).
EUROPE 5.4 GHz	5495 ~ 5585 (DFS) 5655 ~ 5705 (DFS)	99(5495), 100(5500)... 116(5580), 117(5585). 131(5655), 132(5660)... 140(5700), 141(5705).	100(5500), 101(5505)... 115(5575), 116(5580). 132(5660), 133(5665)... 139(5695), 140(5700).	100(5500), 101(5505)... 115(5575), 116(5580). 132(5660), 133(5665)... 139(5695), 140(5700).	100(5500), 101(5505)... 111(5555), 112(5560). 132(5660), 133(5665)... 135(5675), 136(5680).	104(5520), 105(5525)... 115(5575), 116(5580). 136(5680), 137(5685)... 139(5695), 140(5700).
EUROPE 5.8 GHz	5735 ~ 5870 (DFS)	147(5735), 148(5740)... 173(5865), 174(5870).	147(5735), 148(5740)... 173(5865), 174(5870).	149(5745), 150(5750)... 172(5860), 173(5865).	149(5745), 150(5750)... 168(5840), 169(5845).	153(5765), 154(5770)... 172(5860), 173(5865).

## Frequency Domains and Channels

Frequency Domain	Frequency Band (Start Frequency ~ End Frequency in MHz)	Allowed Channels (Center Frequency in GHz)				
		5 MHz	10 MHz	20 MHz	40 PLUS MHz	40 MINUS MHz
RUSSIA 5 GHz	5155 ~ 6075 (Non-DFS)	31(5155), 32(5160)... 214(6070), 215(6075).	31(5155), 32(5160)... 214(6070), 215(6075).	32(5160), 33(5165)... 213(6065), 214(6070).	32(5160), 33(5165)... 219(6045), 210(6050).	36(5180), 37(5185)... 213(6065), 214(6070).
Taiwan 5 GHz	5495 ~ 5705 (DFS) 5740 ~ 5810 (Non-DFS)	99(5495), 100(5500)... 140(5700), 141(5705). 148(5740), 149(5745)... 161(5805), 162(5810).	100(5500), 101(5505)... 139(5695), 140(5700). 149(5745), 150(5750)... 160(5800), 161(5805).	100(5500), 101(5505)... 139(5695), 140(5700). 149(5745), 150(5750)... 160(5800), 161(5805).	100(5500), 101(5505)... 135(5675), 136(5680). 149(5745), 150(5750)... 156(5780), 157(5785).	104(5520), 105(5525)... 139(5695), 140(5700). 153(5765), 154(5770)... 160(5800), 161(5805).
India 5.8 GHz	5830 ~ 5870 (Non-DFS)	166(5830), 167(5835)... 173(5865), 174(5870).	166(5830), 167(5835)... 173(5865), 174(5870).	167(5835), 168(5840)... 172(5860), 173(5865).	167(5835), 168(5840), 169(5845).	171(5855), 172(5860), 173(5865).
CANADA 5.8 GHz	5735 ~ 5855 (Non-DFS)	147(5735), 148(5740)... 170(5850), 171(5855).	147(5735), 148(5740)... 170(5850), 171(5855).	148(5740), 149(5745)... 169(5845), 170(5850).	148(5740), 149(5745)... 165(5825), 166(5830).	152(5760), 153(5765)... 169(5845), 170(5850).
U.K 5.8 GHz	5730 ~ 5790 (DFS) 5820 ~ 5845 (DFS)	146(5730), 147(5735)... 157(5785), 158(5790), 164(5820)... 169(5845).	147(5735), 148(5740)... 156(5780), 157(5785), 167(5835).	147(5735), 148(5740)... 156(5780), 157(5785), 167(5835).	147(5735), 148(5740)... 152(5760), 153(5765).	151(5755), 152(5760)... 156(5780), 157(5785).
Australia 5.4 GHz	5475 ~ 5595 (DFS) 5655 ~ 5720 (DFS)	95(5475), 96(5480) 97(5485)... 119(5595). 131(5655) 132(5660) 133(5665)... 144(5720).	95(5475), 96(5480)... 118(5590), 119(5595). 131(5655) 132(5660) 133(5665)... 144(5720).	96(5480), 97(5485)... 117(5585), 118(5590). 132(5660), 133(5665)... 143(5715).	96(5480), 97(5485)... 114(5570), 132(5660), 133(5665)... 139(5695)	100(5500), 101(5505)... 118(5590), 136(5680), 137(5685)... 143(5715).
Australia 5.8 GHz	5730 ~ 5845 (Non-DFS)	146(5730), 147(5735)... 169(5845).	146(5730), 147(5735), 148(5740)... 169(5845).	147(5735), 148(5740)... 168(5840).	147(5735), 148(5740)... 164(5820).	151(5755), 152(5760)... 168(5840).

## Frequency Domains and Channels

Frequency Domain	Frequency Band (Start Frequency ~ End Frequency in MHz)	Allowed Channels (Center Frequency in GHz)				
		5 MHz	10 MHz	20 MHz	40 PLUS MHz	40 MINUS MHz
Brazil 5.4 GHz	5475 ~ 5720 (DFS)	95(5475), 96(5480), 97(5485)... 144(5720).	95(5475), 96(5480), 97(5485)... 144(5720).	96(5480), 97(5485)... 142(5710), 143(5715).	96(5480), 97(5485)... 138(5690)... 139(5695).	100(5500), 101(5505)... 142(5710), 143(5715).
Brazil 5.8 GHz	5730-5845 (Non-DFS)	146(5730), 147(5735)... 169(5845).	146(5730), 147(5735), 148(5740)... 169(5845).	147(5735), 148(5740)... 168(5840).	147(5735), 148(5740)... 164(5820).	151(5755), 152(5760)... 168(5840).

\* Not applicable for MP-8150-CPE and QB-8150-EPR-12/50 products.

## 6.4 GHz Channels

6.4 GHz frequency band is supported by the following devices:

- Tsunami® MP-8160-BSU
- Tsunami® MP-8160-SUA
- Tsunami® MP-8160-CPE

Frequency Domain	Frequency Band (Start Frequency ~ End Frequency in MHz)	Allowed Channels (Center Frequency)				
		5 MHz	10 MHz	20 MHz	40 PLUS MHz	40 MINUS MHz
World 6.4 GHz	5905 ~ 6420	181 (5905), 182 (5910), 183 (5915)... 284 (6420).	181 (5905), 182 (5910), 183 (5915)... 284 (6420).	182 (5910), 183 (5915), 184 (5920)... 283 (6415).	182 (5910), 183 (5915), 184 (5920)... 279 (6395).	186 (5930), 187 (5935), 188 (5940)... 283 (6415).



: The center frequency listed in the above tables are based on channel offset set to '0'. If channel offset is set to any value other than '0' then the center frequency will be shifted accordingly. You can set the channel offset ranging from -2 to +2 MHz in the following devices: Tsunami® MP-8150-CPE; Tsunami® QB-8150-EPR-12/50; Tsunami® MP-8160-BSU; Tsunami® MP-8160-SUA and Tsunami® MP-8160-CPE.

### Details for 40MHz Bandwidth

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

For 40 PLUS

- 2.4GHz ->
  - Channel 1 = 2412 MHz
  - Bandwidth starts from 2403 MHz and ends at 2442 MHz
- 5GHz ->
  - Channel 52 = 5260 MHz
  - Bandwidth starts from 5251 MHz and ends at 5290 MHz

For 40 MINUS

- 2.4GHz ->
  - Channel 5 = 2432 MHz
  - Bandwidth starts from 2403 MHz and ends at 2442 MHz
- 5GHz ->
  - Channel 56 = 5280 MHz
  - Bandwidth starts from 5251 MHz and ends at 5290 MHz

# SNR Information



Tabulated below are the SNR values for the following devices:

- Tsunami® MP-8100-BSU
- Tsunami® MP-8100-SUA
- Tsunami® MP-8150-SUR
- Tsunami® QB-8100-EPA
- Tsunami® QB-8150-EPR

MCS Index	Modulation	No of Streams	2.4 GHz											
			5 MHz			10 MHz			20 MHz			40 MHz		
			Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR
MCS0	BPSK 1/2	Single	1.6	10	86	3.3	10	86	6.5	12	86	13.5	26	80
MCS1	QPSK 1/2	Single	3.3	15	86	6.5	16	86	13	21	86	27	26	80
MCS2	QPSK 3/4	Single	4.9	21	84	9.7	21	84	19.5	21	84	40.5	26	79
MCS3	16 QAM 1/2	Single	6.5	23	82	13	23	82	26	23	82	54	30	77
MCS4	16 QAM 3/4	Single	9.7	26	80	19.5	26	80	39	25	80	81	33	77
MCS5	64 QAM 2/3	Single	13	29	79	26	29	79	52	27	78	108	37	76
MCS6	64 QAM 3/4	Single	14.6	30	79	29.3	31	78	58.5	30	77	121.5	40	75
MCS7	64 QAM 5/6	Single	16.2	32	78	32.5	32	78	65	32	77	135	42	75
MCS8	BPSK 1/2	Dual	3.3	12	86	6.5	14	86	13	14	86	27	16	80
MCS9	QPSK 1/2	Dual	6.5	20	84	13	21	84	26	21	84	54	26	80
MCS10	QPSK 3/4	Dual	9.7	22	82	19.5	23	82	39	22	82	81	28	79
MCS11	16 QAM 1/2	Dual	13	23	80	26	23	80	52	24	80	108	32	77
MCS12	16 QAM 3/4	Dual	19.5	27	80	39	27	80	78	30	78	162	35	77
MCS13	64 QAM 2/3	Dual	26	30	79	52	30	79	104	34	78	216	37	76
MCS14	64 QAM 3/4	Dual	29.3	36	78	58.5	35	77	117	37	77	243	43	75
MCS15	64 QAM 5/6	Dual	32.5	39	78	65	38	77	130	39	76	270	45	75

MCS Index	Modulation	No of Streams	5 GHz											
			5 MHz			10 MHz			20 MHz			40 MHz		
			Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR
MCS0	BPSK 1/2	Single	1.6	6	86	3.3	7	86	6.5	6	86	13.5	9	80

## SNR Information

MCS Index	Modulation	No of Streams	5 GHz											
			5 MHz			10 MHz			20 MHz			40 MHz		
			Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR
MCS1	QPSK 1/2	Single	3.3	8	86	6.5	8	86	13	9	86	27	11	80
MCS2	QPSK 3/4	Single	4.9	10	84	9.7	13	84	19.5	11	84	40.5	15	79
MCS3	16 QAM 1/2	Single	6.5	14	82	13	16	82	26	14	82	54	16	77
MCS4	16 QAM 3/4	Single	9.7	17	80	19.5	20	80	39	18	80	81	20	77
MCS5	64 QAM 2/3	Single	13	22	79	26	24	79	52	22	78	108	24	76
MCS6	64 QAM 3/4	Single	14.6	25	79	29.3	26	78	58.5	25	77	121.5	27	75
MCS7	64 QAM 5/6	Single	16.2	28	78	32.5	29	78	65	28	77	135	30	75
MCS8	BPSK 1/2	Dual	3.3	8	86	6.5	9	86	13	9	86	27	9	80
MCS9	QPSK 1/2	Dual	6.5	12	84	13	12	84	26	12	84	54	13	80
MCS10	QPSK 3/4	Dual	9.7	14	82	19.5	15	82	39	14	82	81	17	79
MCS11	16 QAM 1/2	Dual	13	16	80	26	16	80	52	16	80	108	22	77
MCS12	16 QAM 3/4	Dual	19.5	20	80	39	21	80	78	20	78	162	25	77
MCS13	64 QAM 2/3	Dual	26	25	79	52	26	79	104	26	78	216	27	76
MCS14	64 QAM 3/4	Dual	29.3	29	78	58.5	29	77	117	29	77	243	30	75
MCS15	64 QAM 5/6	Dual	32.5	30	78	65	30	77	130	30	76	270	33	75

Tabulated below are the SNR values for the following device(s) in legacy mode:

- Tsunami® MP-8100-BSU

Modulation	2.4 GHz									5 GHz					
	5 MHz			10 MHz			20 MHz			5 MHz		10 MHz		20 MHz	
	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Min SNR	Max SNR	Min SNR	Max SNR	Min SNR	Max SNR
BPSK 1/2	1.5	10	84	3	10	84	6	13	84	8	84	8	84	7	81
BPSK 3/4	2.25	10	84	4.5	11	84	9	13	84	9	84	9	84	8	81
QPSK 1/2	3	12	84	6	11	84	12	15	84	10	82	10	82	9	81
QPSK 3/4	4.5	14	84	9	13	84	18	15	84	12	82	11	82	12	81
16QAM 1/2	6	17	82	12	17	80	24	22	80	16	82	16	82	15	80
16QAM 3/4	9	20	82	18	23	78	36	25	73	18	82	18	80	18	80
64QAM 2/3	12	27	81	24	29	76	48	28	73	24	80	24	80	24	78
64QAM 3/4	13.5	29	80	27	30	74	54	29	72	27	80	27	80	27	76



## SNR Information

Tabulated below are the SNR values for the following devices:

- Tsunami® MP-8150-CPE
- Tsunami® QB-8150-EPR-12/50

MCS Index	Modulation	No of Streams	5 GHz											
			5 MHz			10 MHz			20 MHz			40 MHz		
			Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR
MCS0	BPSK 1/2	Single	1.6	8	82	3.3	8	82	6.5	8	82	13.5	8	82
MCS1	QPSK 1/2	Single	3.3	8	82	6.5	9	82	13	9	82	27	9	82
MCS2	QPSK 3/4	Single	4.9	10	82	9.7	11	82	19.5	11	82	40.5	11	80
MCS3	16 QAM 1/2	Single	6.5	13	82	13	15	82	26	17	82	54	16	80
MCS4	16 QAM 3/4	Single	9.7	16	82	19.5	19	82	39	19	82	81	18	80
MCS5	64 QAM 2/3	Single	13	20	81	26	22	81	52	23	81	108	23	79
MCS6	64 QAM 3/4	Single	14.6	22	80	29.3	24	80	58.5	25	80	121.5	24	79
MCS7	64 QAM 5/6	Single	16.2	24	80	32.5	26	80	65	26	80	135	26	79
MCS8	BPSK 1/2	Dual	3.3	9	82	6.5	8	82	13	9	82	27	9	82
MCS9	QPSK 1/2	Dual	6.5	10	82	13	10	82	26	12	82	54	11	80
MCS10	QPSK 3/4	Dual	9.7	12	82	19.5	12	82	39	13	82	81	13	80
MCS11	16 QAM 1/2	Dual	13	16	82	26	16	82	52	18	82	108	15	78
MCS12	16 QAM 3/4	Dual	19.5	19	80	39	20	82	78	19	82	162	20	68
MCS13	64 QAM 2/3	Dual	26	24	80	52	24	80	104	24	80	216	24	60
MCS14	64 QAM 3/4	Dual	29.3	29	80	58.5	30	78	117	27	78	243	29	58
MCS15	64 QAM 5/6	Dual	32.5	33	80	65	33	78	130	32	78	270	32	56

Tabulated below are the SNR values for the following devices:

- Tsunami® MP-8160-BSU
- Tsunami® MP-8160-SUA
- Tsunami® MP-8160-CPE

MCS Index	Modulation	No of Streams	6.4 GHz											
			5 MHz			10 MHz			20 MHz			40 MHz		
			Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR
MCS0	BPSK 1/2	Single	1.6	6	87	3.3	6	87	6.5	6	87	13.5	7	87
MCS1	QPSK 1/2	Single	3.3	8	87	6.5	8	87	13	7	87	27	8	86

## SNR Information

MCS Index	Modulation	No of Streams	6.4 GHz											
			5 MHz			10 MHz			20 MHz			40 MHz		
			Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR
MCS2	QPSK 3/4	Single	4.9	10	86	9.7	10	84	19.5	10	86	40.5	12	82
MCS3	16 QAM 1/2	Single	6.5	13	84	13	14	84	26	13	82	54	13	74
MCS4	16 QAM 3/4	Single	9.7	16	80	19.5	16	78	39	16	76	81	19	70
MCS5	64 QAM 2/3	Single	13	21	74	26	21	70	52	20	70	108	21	62
MCS6	64 QAM 3/4	Single	14.6	22	70	29.3	23	67	58.5	22	67	121.5	24	56
MCS7	64 QAM 5/6	Single	16.2	24	67	32.5	24	65	65	24	65	135	27	55
MCS8	BPSK 1/2	Dual	3.3	8	87	6.5	8	87	13	7	86	27	10	86
MCS9	QPSK 1/2	Dual	6.5	10	87	13	10	87	26	11	84	54	12	82
MCS10	QPSK 3/4	Dual	9.7	15	84	19.5	13	84	39	13	82	81	15	75
MCS11	16 QAM 1/2	Dual	13	16	80	26	17	80	52	17	78	108	18	74
MCS12	16 QAM 3/4	Dual	19.5	20	74	39	23	74	78	20	71	162	22	56
MCS13	64 QAM 2/3	Dual	26	25	70	52	24	66	104	24	65	216	25	55
MCS14	64 QAM 3/4	Dual	29.3	27	66	58.5	27	62	117	27	62	243	27	53
MCS15	64 QAM 5/6	Dual	32.5	28	64	65	29	62	130	29	62	270	30	52

---

# Bootloader CLI and ScanTool



## Bootloader CLI

The Bootloader CLI is a minimal subset of the normal CLI used to perform initial configuration of the device. The Bootloader CLI is available when the device 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 Bootloader CLI provides the ability to configure the initial setup parameters; and depending on this configuration, a software file is downloaded to the device during startup.

The Bootloader 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 Bootloader 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 Bootloader fails to load the firmware from flash, it tries to get the firmware from the network. While trying to get firmware from the network, the device should be powered on using Ethernet 1 interface of the device. The default configuration of the Bootloader 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	imagenname
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 parameter value.

**To Get the IP Parameters Dynamically for Loading the Firmware**

1. Set the `ipaddrtype` to dynamic
2. Run the BOOTP and TFTP Servers followed by reboot of the device

When the device reboots, the device gets the IP Address and Boot filename from the BOOTP server. You need not change any of the default Bootloader 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 followed by reboot of the device

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 as "serverip". In this case, the TFTP Server should be reachable to the device.

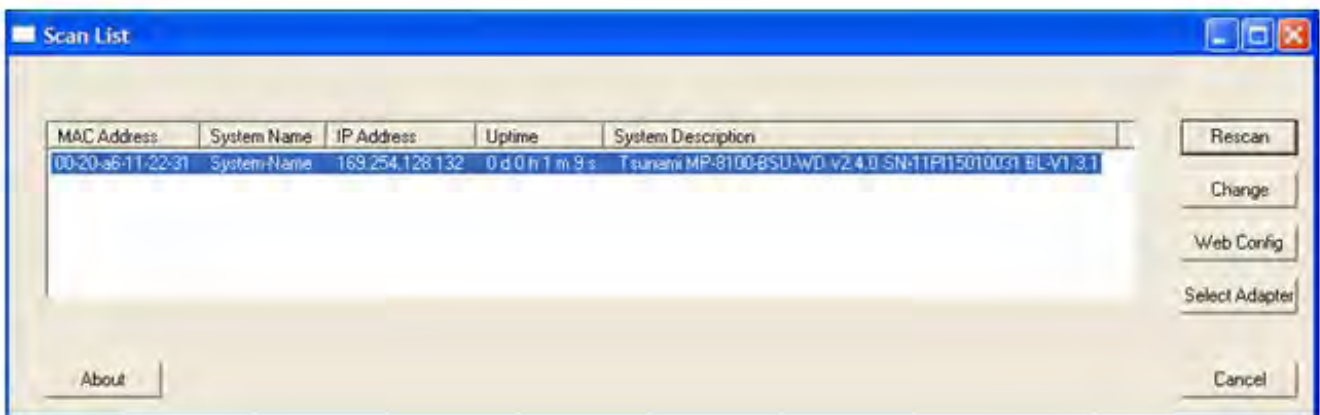
**ScanTool**

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 Bootloader 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 Bootloader mode.

For example:

- Tsunami MP-8100-BSU-WD - Description of the device
- v2.4.0 - Firmware Version
- SN-11P115010031 - Serial Number
- BL-v1.3.1 - Bootloader version



**Figure E-1 Scan Tool View of a Device in Bootloader Mode (An Example)**

---

## Lightning Protection

# F

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 5/Cat5e/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® series products. Contact your reseller or distributor for more information.

---

## Abbreviations

# G

<b>A</b>	
ACL	Access Control List
ACS	Automatic Channel Selection
AES	Advanced Encryption Standard
ALG	Application Level Gateway
ARP	Address Resolution Protocol
ATPC	Adaptive Transmit Power Control
<b>B</b>	
BSU	Base Station Unit
<b>C</b>	
CCP	Compression Control Protocol
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface
CIR	Committed Information Rate
CPE	Customer Premises Equipment
CRC	Cyclic Redundancy Check
<b>D</b>	
DDRS	Dynamic Data Rate Selection
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSL	Digital Subscriber Line
<b>E</b>	
EIRP	Equivalent Isotropically Radiated Power
ETSI	European Telecommunications Standards Institute
<b>F</b>	

FCC	Federal Communications Commission
FCS	Frame Check Sequence
<b>G</b>	
Gbps	Gigabit Per Second
GPL	General Public License
GRE	Generic Routing Encapsulation
<b>H</b>	
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
<b>I</b>	
IANA	Internet Assigned Numbers Authority (IANA)
IC	Industry Canada
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
ISP	Internet Service Provider
ITS	Intelligent Transportation System
<b>L</b>	
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LCP	Link Configuration Protocol
LED	Light Emitting Diode
LGPL	Lesser General Public License
<b>M</b>	
MAN	Metropolitan Area Networks
Mbps	Megabits Per Second
MD5	Message-Digest algorithm
MIB	Management Information Base
MIMO	Multiple-input and multiple-output
MIR	Maximum Information Rate
MP	Multipoint
MPPE	Microsoft Point-to-Point Encryption

MSCHAP v2	Microsoft Challenge-Handshake Authentication Protocol
MTU	Maximum Transmission Unit
<b>N</b>	
NAPT	Network Address Port Translation
NAT	Network Address Translation
NCP	Network Control Protocol
NMS	Network Management System
NOP	Non Occupancy Period
<b>P</b>	
PAP	Password Authentication Protocol
PC	Personal Computer
PoE	Power Over Ethernet
PPPoE	Point-to-point Protocol over Ethernet
PTMP	Point-to-multipoint
PTP	Point-to-point
PVES	ProximVision ES
<b>Q</b>	
QB	Quick Bridge
QoS	Quality of Service
<b>R</b>	
RADIUS	Remote Authentication Dial In User Service
RAS	Remote Access Services
RF	Radio Frequency
RIP	Routing Information Protocol
RMA	Return Material Authorization
RSSI	Received Signal Strength Indicator
<b>S</b>	
SHA	Secure Hash Algorithm
SKU	Stock Keeping Unit
SNMP	Simple Network Management Protocol
SNR	Signal-to-noise Ratio



Sntp	Simple Network Time Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
SU	Subscriber Unit
<b>T</b>	
TBC	Text Based Configuration
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TPC	Transmit Power Control
TPID	Tag Protocol Identifier
TTL	Time to Live
<b>U</b>	
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair
<b>V</b>	
VLAN	Virtual Local Area Network
<b>W</b>	
WEP	Wired Equivalent Privacy
WORP	Wireless Outdoor Router Protocol

---

# 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 where the 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 (vi) 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 and 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 team:

- Product information
  - Part number and serial number of the suspected faulty device
- 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 and location where you purchased the product



: 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 online 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	24x7Enhanced (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](mailto:servpak@proxim.com).

# **FCC Statement**

## **Federal Communication Commission Interference Statement**

This equipment has been tested and found to comply with the limits for a Class A 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.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

FCC NOTICE: To comply with FCC part 15 rules in the United States, the system must be professionally installed to ensure compliance with the Part 15 certification. It is the responsibility of the operator and professional installer to ensure that only certified systems are deployed in the United States. The use of the system in any other combination (such as co-located antennas transmitting the same information) is expressly forbidden.

## **IMPORTANT NOTE:**

### **FCC 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 50cm between the radiator & your body.