

Tsunami® 800 & 8000 Series **(Point-to-point and Point-to-multipoint Products)** **Software Management Guide**

Products Covered

--> Tsunami® Multipoint

- MP-820-BSU-100
- MP-8100-BSU
- MP-8200-BSU; MP-8250-BS9; MP-8250-BS1
 - MP-820-SUA-50+
 - MP-825-SUR-50+
 - MP-825-CPE-50
 - MP-8100-SUA
 - MP-8150-SUR
 - MP-8150-SUR-100
 - MP-8150-CPE
 - MP-8200-SUA
 - MP-8250-SUR
- MP-8160-BSU and MP-8160-BS9
 - MP-8160-SUA
 - MP-8160-CPE

--> Tsunami Quickbridge®

- QB-8100-EPA / LNK
- QB-8150-EPR / LNK
- QB-8150-LNK-100
- QB-8150-LNK-12/50
- QB-8151-EPR / LNK
- QB-8200-EPA / LNK
- QB-8250-EPR / LNK
- QB-825-EPR / LNK-50
- QB-825-EPR / LNK-50+



Copyright

© 2013 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 guide at any time. When using these devices, 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, in part, some free software that is developed by Free Software Foundation. A user is granted license to this software under the terms of either the GNU General Public License or GNU Lesser General Public License (See <http://www.gnu.org/licenses/licenses.html>). This license allows the user to freely copy, modify and redistribute this software and no other statement or documentation from us. To get a copy of this software, or for any other information, please contact our customer support team Telephone Support).

OpenSSL License Note

Tsunami® products contains software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>) and that is subject to the following copyright and conditions:

Copyright (c) 1998-2002 The OpenSSL Project. All rights reserved.

The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to refer to, endorse, or promote the products or for any other purpose related to the products without prior written permission. For written permission, please contact openssl-core@openssl.org.

This software is provided by the OpenSSL Project "as is" and any expressed or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the OpenSSL Project or its contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

Tsunami® 800 and 8000 Series - Software Management Guide

Documentation Version: 5.2
P/N 765-00131, February 2014

Preface	10
1 Overview	13
About Tsunami® 800 and 8000 Products	13
Wireless Network Topology	18
Point-to-Multipoint (PTMP).....	18
Point-to-Point Link	22
Multiple-Input-Multiple-Output (MIMO)	25
Wireless Outdoor Router Protocol (WORP)	25
2 Management and Monitoring Capabilities	27
Web (HTTP/HTTPS) Interface	27
Command Line Interface	27
HyperTerminal	27
Telnet	28
Secure Shell (SSH)	28
Simple Network Management Protocol (SNMP) Management	28
ProximVision NMS	29
3 Device Initialization	30
Initialization	30
ScanTool	30
Initialize Device by using ScanTool	31
Modifying the IP Address of the Device by using ScanTool.....	32
Logging onto the Web Interface	33
Home Page	35
COMMIT.....	36
REBOOT	37
Factory Default Configuration	37
4 Basic Configuration	40
5 Advanced Configuration	47
System	48
Network	51
IP Configuration	51
Bridge Mode	52
Routing Mode	56
Routing Mode with PPPoE Client Enabled	59
Static Route Table	63
Adding Static Route Entries	64
Network Address Translation (NAT).....	64

Supported Session Protocols	67
RIP	67
PPPoE End Point (SU Only)	69
IP over IP Tunneling	74
Create a Tunnel	76
View Existing Tunnels	78
Ethernet	78
Basic Ethernet Configuration	78
Advanced Configuration	80
Wireless	81
Link Profiles	82
Add a Link Profile	83
Edit a Link Profile	83
Wireless Outdoor Router Protocol (WORP)	90
Wireless Interface Properties	96
Dynamic Frequency Selection (DFS) / Dynamic Channel Selection (DCS)	106
Dynamic Frequency Selection (DFS):	106
Dynamic Channel Selection (DCS)	107
Blacklist Information	111
Manual Blacklist	112
Roaming	112
Definition(s)	113
Roaming Types	113
Configurable Parameters on a BSU	114
Configurable Parameters on an SU	117
BSU / SU Profiles	119
Add a Profile	119
Edit a Mapped Profile	121
Security	122
Wireless Security	122
Creating a New Security Profile	123
Editing an existing Security Profile	125
RADIUS	125
MAC ACL	127
Add SUs/End Point B to MAC Access Control Table	128
Edit the existing SUs/End Point B from MAC Access Control Table	128
Quality of Service (QoS)	129
QoS Concepts and Definitions	129
Packet Identification Rule (PIR)	129
Service Flow Class (SFC)	131
QoS Class	134
QoS Configuration	135

QoS PIR Configuration	138
QoS Service Flow Configuration (SFC)	148
QoS Class Configuration	150
QoS SU or End Point B List Configuration	153
QoS Configuration for a Management Station	154
RADIUS Based SU QoS Configuration	158
VLAN (Bridge Mode Only)	159
System-Level VLAN Configuration.	159
Ethernet VLAN Configuration.	161
Transparent Mode.	161
Access Mode	162
Trunk Mode	163
RADIUS Based SU VLAN Configuration	166
Filtering (Bridge Only)	168
Protocol Filter.	169
Protocol Filter Table	171
Add User-defined Protocols to the Filter Table	172
Static MAC Address Filter	172
Static MAC Address Filter Configuration.	174
Advanced Filtering	175
Edit Advanced Filtering Table Entries	176
TCP/UDP Port Filter.	177
TCP/UDP Port Filter Table	178
Adding User-defined TCP/UDP Port Filter Entries	179
Storm Threshold Filter	179
WORP Intra Cell Blocking	180
WORP Intra Cell Blocking Group Table	182
WORP Intra Cell Blocking MAC Table	183
DHCP	185
DHCP Pool.	185
Adding a New Pool Entry	185
DHCP Server	186
DHCP Relay (Routing Mode only)	188
IGMP Snooping	190
6 Management	192
System	192
System Information	192
Inventory Management	193
Licensed Features	194
License Upgrade Procedure	195
File Management	195

TFTP Server	196
Text Based Configuration (TBC) File Management	196
Generating TBC File	196
Editing the TBC File	197
Loading the TBC file	198
Upgrade Firmware	198
Upgrade Firmware via HTTP	198
Upgrade Firmware via TFTP	199
Upgrade Configuration	200
Upgrade Configuration via HTTP	200
Upgrade Configuration via TFTP	201
Upgrade License	202
Upgrade License via HTTP	202
Upgrade License via TFTP	203
Retrieve From Device	204
Retrieve from Device via HTTP	204
TFTP Retrieve	206
Services	207
HTTP/HTTPS	207
Telnet/SSH	209
SNMP	211
SNMP Trap Host Table	214
Edit SNMP Trap Host Table	214
Logs	215
Configure a Remote Syslog host	216
Simple Network Time Protocol (SNTP)	217
Access Control	219
Add Host(s) to Management Access Control Table	220
Edit Management Access Control Table Entries	220
Reset to Factory	221
Convert QB to MP	221
7 Monitor	223
System	223
Interface Statistics	224
Ethernet Statistics	224
Wireless Statistics	226
PPPoE Statistics	227
IP Tunnels	229
WORP Statistics	230
General Statistics	230
Basic Statistics	232

Advanced Statistics	233
Link Statistics	234
SU / End Point B Link Statistics	234
BSU/End Point A Link Statistics	238
QoS Statistics (BSU or End Point A Only)	239
Active VLAN	240
Bridge	241
Bridge Statistics	241
Learn Table	243
Network Layer	243
Routing Table	243
IP ARP	244
ICMP Statistics	245
IP Address Table	246
DNS Addresses	246
Neighbour Table	247
RIP Database	247
RADIUS (BSU or End Point A only)	248
Authentication Statistics	248
IGMP	249
Ethernet or Wireless Multicast List	249
Router Port List	249
DHCP	250
Logs	251
Event Log	251
View Event Log	251
Hide Event Log	251
Clear Event Log	252
Debug Log	252
Temperature Log	252
View Temperature Log	254
Hide Temperature Log	255
Clear Temperature Log	255
Tools	255
Wireless Site Survey	255
Scan Tool	256
sFlow®	256
sFlow Receiver Configuration	258
Sampling Configuration	259
Counter Polling Configuration	260
Console Commands	261
Spectrum Analyzer	262

Radio Link Test Tool	266
Configuration Options	266
Statistics Options.	269
SNMP v3 Statistics	271
8 Troubleshooting	273
PoE Injector	274
Connectivity Issues	275
Surge or Lightning Issues (For Connectorized devices)	276
Setup and Configuration Issues	276
Application Specific Troubleshooting	278
Wireless Link Issues	279
Wired (Ethernet) Interface Validation	281
Wireless Interface Validation	282
Recovery Procedures	283
Operational Mode.	284
Bootloader Mode	285
Load a New Image.	285
Using the ScanTool.	286
Using the Bootloader CLI	286
Setting IP Address using Serial Port	287
Hardware and Software Requirements.	287
Attach the Serial Port Cable	288
Initializing the IP Address using CLI	288
Spectrum Analyzer	289
Avoiding Interference	289
Conclusion	289
Miscellaneous	290
Unable to Retrieve Event Logs through HTTPS	290
A Feature Applicability	291
B Parameters Requiring Reboot.	293
C Frequency Domains and Channels.	297
D LACP - Device Management	311
E QinQ.	313
F BSU Redundancy	315
G Bootloader CLI and ScanTool	318

H SNR Information 320

I Configuration File Cross-loading across the Products 328

J Abbreviations 330

K Lightning Protection 334

L Statement of Warranty 335

M Technical Services and Support 337

Preface

This chapter contains information on the following:

- About this Guide
- Products Covered
- Audience
- Prerequisites
- Related Documents
- Documentation Conventions

About this Guide

This guide gives a jump-start working knowledge of the Tsunami® 800 and 8000 products. It explains the step-by-step procedure to configure, manage and monitor the device by using Web Interface.

Products Covered

Given below are the products that are covered in this guide along with the latest software version supported by each of the device.

Product(s)	Supported Countries	Supported Software Version
MP-8100-BSU	US, WD, EU	2.6.1
MP-8200-BSU	US, WD, EU, JP	2.6.1
MP-8250-BS9	US, WD, EU	2.6.1
MP-8250-BS1	US, WD, EU	2.6.1
MP-8100-SUA	US, WD, EU	2.6.1
MP-8150-SUR	US, WD, EU	2.6.1
MP-8150-SUR-100	US, WD, EU	2.6.1
MP-8150-CPE	US, WD	2.6.1
MP-8200-SUA	US, WD, EU, JP	2.6.1
MP-8250-SUR	US, WD, EU, JP	2.6.1
MP-8160-BSU	WD	2.6.1
MP-8160-BS9	WD	2.6.1
MP-8160-SUA	WD	2.6.1
MP-8160-CPE-A100	WD	2.6.1
MP-820-BSU-100	US, WD, EU	2.6.2
MP-820-SUA-50+	US, WD, EU	2.6.2
MP-825-SUR-50+	US, WD, EU	2.6.2
MP-825-CPE-50	US, WD, EU	2.6.2
QB-8100-EPA/LNK	US, WD, EU	2.6.1

Product(s)	Supported Countries	Supported Software Version
QB-8150-EPR/LNK	US, WD, EU	2.6.1
QB-8150-LNK-100	US, WD, EU	2.6.1
QB-8150-LNK-12	US	2.6.1
QB-8150-LNK-50	US, WD	2.6.1
QB-8151-EPR/LNK	US, WD	2.6.1
QB-8200-EPA/LNK	US, WD, EU, JP	2.6.1
QB-8250-EPR/LNK	US, WD, EU, JP	2.6.1
QB-825-EPR/LNK-50	US, WD, EU	2.6.2
QB-825-EPR/LNK-50 ⁺	US, WD, EU	2.6.2

Audience

The intended audience for this guide is the network administrators who install and/or manage 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

Please refer to the following related documents that are available on the Proxim's support site at <http://my.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 step-by-step instructions to configure, manage and monitor the device by using Command Line Interface (CLI).
- **Antenna Guides** - A guide that gives insight on the recommended antennas and ways to align the antennas.
- **Safety and Regulatory Compliance Guide** - A guide that provides country specific safety and regulatory norms to be followed while installing the device.

Documentation Conventions

ScreenShots

This guide uses screenshots to explain the method to configure, manage and monitor the device by 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 the attention of the user.
Important		A note of significant importance that the user should be aware of.
Caution		A warning that cautions the user of a 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
MP 800 and 8000 BSU/SU in Legacy Mode	Refers to MP 800 and 8000 BSU and SU devices that can interoperate with the legacy products of the Tsunami [®] MP.11 family.



: A feature specific to a device is referred to by its name (For example, Tsunami[®] MP-8100-BSU) else by the common naming convention (For example, BSU) as tabulated above.

Overview







This chapter contains information on the following:












- About Tsunami® 800 and 8000 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® 800 and 8000 Products









Proxim's Tsunami® 800 and 8000 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
MP-8100-BSU	The 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 band. This connectorized device comes with a 3x3 MIMO radio and three N-Type connectors to connect external antennas.	
MP-8100-SUA	The MP-8100 Subscriber unit, is a flexible wireless outdoor product that operates in 2.3 – 2.5 and 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.	
MP-8150-SUR	The MP-8150 Subscriber unit comes with a 2x2 MIMO radio and 23 dBi Integrated dual-polarized panel antenna that operates in 4.900 – 5.925 GHz frequency band.	
MP-8150-SUR-100	The MP-8150 Subscriber unit comes with a 2x2 MIMO radio and 21 dBi integrated dual-polarized panel antenna that operates in 4.900 – 5.875 GHz frequency band. It provides a throughput of up to 50 Mbps (Uplink) and 50 Mbps (Downlink).	
MP-8150-CPE	The MP-8150 Customer Premises Equipment comes with a high power 2x2 MIMO radio and 16 dBi integrated dual-polarized panel antenna that operates in 5.3 – 6.1 GHz frequency band.	
MP-8200-BSU	The MP-8200 Base Station unit, is a flexible wireless outdoor product that operates in 4.900 to 5.925 GHz frequency band. This connectorized device comes with a 3x3 MIMO high power radio and three N-Type connectors to connect external antennas.	

MP-8250-BS9	The MP-8250 Base Station unit comes with a high power 2x2 MIMO radio and 16 dBi integrated 90° sector antenna that operates in 4.900 – 5.925 GHz frequency band.	
MP-8250-BS1	The MP-8250 Base Station unit comes with a high power 2x2 MIMO radio and 23 dBi integrated 10° panel antenna that operates in 4.900 – 5.925 GHz frequency band.	
MP-8200-SUA	The MP-8200 Subscriber unit, is a flexible wireless outdoor product that operates in 4.900 to 5.925 GHz frequency band. This connectorized device comes with a 3x3 MIMO high power radio and three N-Type connectors to connect external antennas.	
MP-8250-SUR	The MP-8250 Subscriber unit comes with a 2x2 MIMO high power radio and 23 dBi integrated dual-polarized panel antenna that operates in 4.900 – 5.925 GHz frequency band.	
MP-8160-BSU	The MP-8160 Base Station unit, is a flexible outdoor product that operates in 5.900 – 6.425 GHz frequency band. This connectorized device comes with a high power 2x2 MIMO radio and two N-Type connectors to connect external antennas.	
MP-8160-BS9	The MP-8160 Base Station unit comes with a 2x2 MIMO radio and 16 dBi integrated 90° sector antenna that operates in 5.900 – 6.425 GHz frequency band.	
MP-8160-SUA	The MP-8160 Subscriber unit, is a flexible outdoor product that operates in 5.900 – 6.425 GHz frequency band. This connectorized device comes with a high power 2x2 MIMO radio and two N-Type connectors to connect external antennas.	
MP-8160-CPE-A100	The MP-8160 Customer Premises Equipment comes with a single high power 2x2 MIMO radio and 15 dBi integrated dual-polarized panel antenna that operates in 5.900 – 6.425 GHz frequency band.	
MP-820-BSU-100	The MP-820 Base Station unit, is a flexible wireless outdoor product that operates in 5.150 – 5.925 GHz frequency band. This connectorized device comes with 2x2 MIMO radio and two N-Type connectors to connect external antennas. It provides an aggregate throughput of 100 Mbps.	
MP-820-SUA-50+	The MP-820 Subscriber unit, is a flexible wireless outdoor product that operates in 5.150 to 5.925 GHz frequency band. This connectorized device comes with a 2x2 MIMO radio and two N-Type connectors to connect external antennas. It provides an aggregate throughput of 50 Mbps, license upgradable to 100 Mbps.	
MP-825-SUR-50+	The MP-825 Subscriber unit comes with a 2x2 MIMO radio and 15 dBi integrated dual-polarized panel antenna that operates in 5.150 - 5.925 GHz frequency band. It provides an aggregate throughput of 50 Mbps, license upgradable to 100 Mbps.	

MP-825-CPE-50	The MP-825 Customer Premises Equipment comes with a 2x2 MIMO radio and 15 dBi integrated dual-polarized panel antenna that operates in 5.15 - 5.925 GHz frequency band with aggregate throughput of 50 Mbps.	
QB-8100-EPA	The QB-8100-EPA QuickBridge operates in 2.3 – 2.5 and 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.	
QB-8100-LNK	A pair of QB-8100-EPA devices form a link.	
QB-8150-EPR	The QB-8150-EPR QuickBridge comes with a 2x2 MIMO radio and 23 dBi integrated dual-polarized panel antenna that operates in 4.900 – 5.925 GHz frequency band.	
QB-8150-LNK	A pair of QB-8150-EPR devices form a link.	
QB-8150-LNK-100	A pair of QB-8150-EPR-100 devices form a link. The QB-8150-EPR-100 device comes with a 2x2 MIMO radio, 21 dBi integrated dual-polarized panel antenna that operates in 4.900 – 5.875 GHz frequency band. It provides a throughput of up to 50 Mbps (Uplink) and 50 Mbps (Downlink).	
QB-8150-LNK-12	A pair of QB-8150-EPR-12 devices form a link. The QB-8150-EPR-12 device comes with a high power 2x2 MIMO radio, 12 Mbps speed and 16 dBi integrated dual-polarized panel antenna that operates in 5.3 - 6.1 GHz frequency band.	
QB-8150-LNK-50	A pair of QB-8150-EPR-50 devices form a link. The QB-8150-EPR-50 device comes with a high power 2x2 MIMO radio, 50 Mbps and 16 dBi integrated dual-polarized panel antenna that operates in 5.3 – 6.1 GHz frequency band.	
QB-8151-EPR	The QB-8151-EPR device comes with a 2x2 MIMO radio, 21 dBi integrated dual-polarized panel antenna that operates in 4.900 – 5.875 GHz frequency band. It provides a throughput of up to 300 Mbps (Uplink) and 300 Mbps (Downlink).	

<p>QB-8151-LNK</p>	<p>A pair of QB-8151-EPR devices form a link.</p> <p>The QB-8151-EPR device comes with a 2x2 MIMO radio, 21 dBi integrated dual-polarized panel antenna that operates in 4.900 – 5.875 GHz frequency band. It provides a throughput of up to 300 Mbps (Uplink) and 300 Mbps (Downlink).</p>	
<p>QB-8200-EPA</p>	<p>The QB-8200-EPA QuickBridge operates in 4.900 – 5.925 GHz frequency band. This connectorized device comes with a 3x3 MIMO high power radio and three N-Type connectors to connect external antennas.</p>	
<p>QB-8200-LNK</p>	<p>A pair of QB-8200-EPA devices form a link.</p>	
<p>QB-8250-EPR</p>	<p>The QB-8250-EPR QuickBridge comes with a 2x2 MIMO high power radio and 23 dBi integrated dual-polarized panel antenna that operates in 4.900 – 5.925 GHz frequency band.</p>	
<p>QB-8250-LNK</p>	<p>A pair of QB-8250-EPR devices form a link.</p>	
<p>QB-825-EPR-50</p>	<p>The QB-825-EPR-50 device comes with a 2x2 MIMO radio and 15 dBi integrated dual-polarized panel antenna that operates in 5.15 - 5.925 GHz frequency band with aggregate throughput of 50 Mbps.</p>	
<p>QB-825-LNK-50</p>	<p>A pair of QB-825-EPR-50 devices form a link.</p>	
<p>QB-825-EPR-50+</p>	<p>The QB-825-EPR-50+ device comes with a 2x2 MIMO high power radio and 15 dBi integrated dual-polarized panel antenna that operates in 5.150 – 5.925 GHz frequency band. It provides an aggregate throughput of 50 Mbps, license upgradable to 100 Mbps.</p>	

QB-825-LNK-50+	A pair of QB-825-EPR-50+ devices form a link.	 Two white, rectangular, rack-mountable devices are shown. Each device has two circular ports on the front face. They are arranged one above the other, slightly offset to the right.
----------------	---	--

1.2 Wireless Network Topology

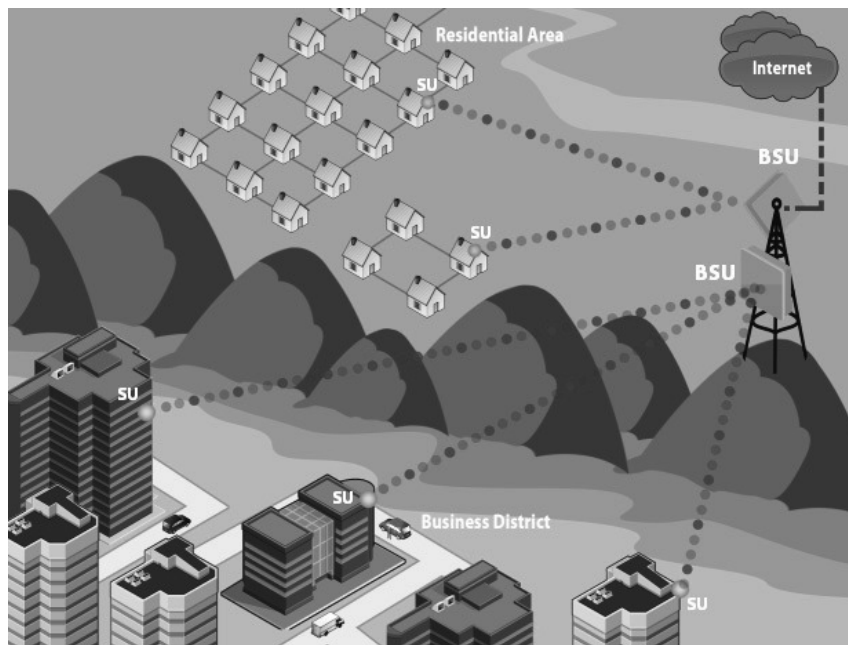
1.2.1 Point-to-Multipoint (PTMP)

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.

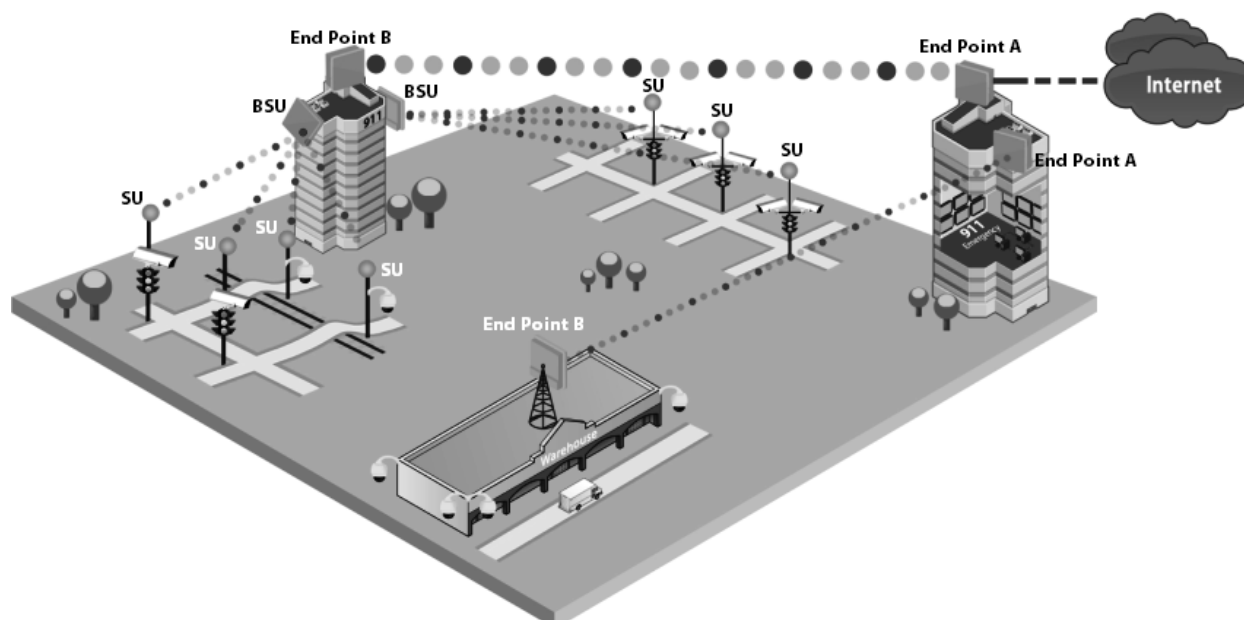
Given below are the deployment scenarios, where Proxim's point-to-multipoint devices are recommended. The Proxim devices used in the deployment images are commonly referred to as BSU (Base Station Unit) and SU (Subscriber Unit). The combinations that are used for BSU and SU multipoint devices are:

Base Station Unit (BSU)	Subscriber Unit (SU)
MP-820-BSU-100 MP-8100-BSU MP-8200-BSU MP-8250-BS9 MP-8250-BS1	MP-820-SUA-50 ⁺
	MP-825-SUR-50 ⁺
	MP-825-CPE-50
	MP-8100-SUA
	MP-8150-SUR
	MP-8150-SUR-100
	MP-8150-CPE
	MP-8200-SUA
	MP-8250-SUR
	MP-8160-BSU MP-8160-BS9
MP-8160-CPE-A100	

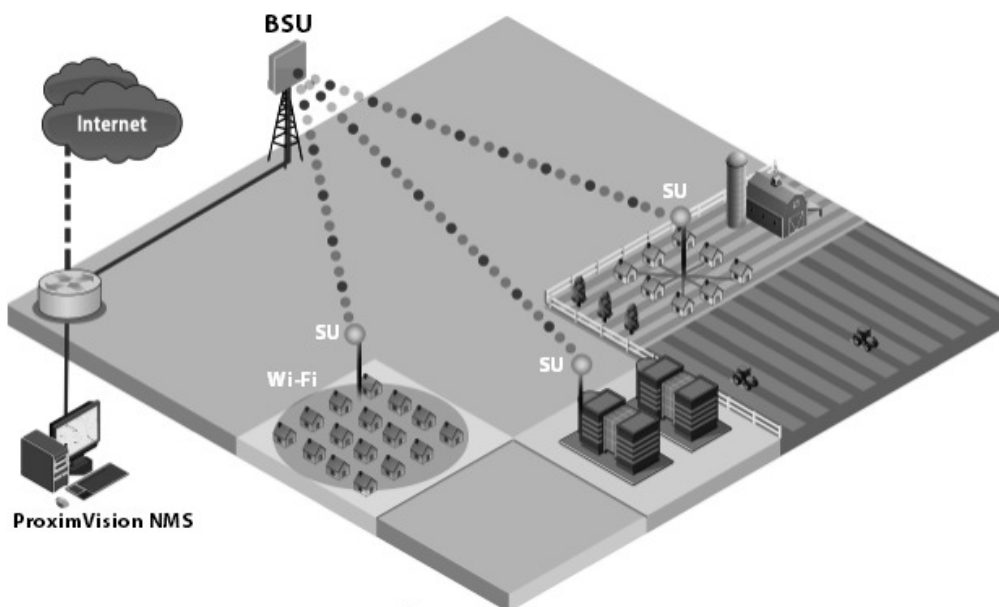
- **Last Mile Access:** Competitive broadband service access alternative to Digital Subscriber Line (DSL) or cable for residences and T1 or Ethernet for businesses.



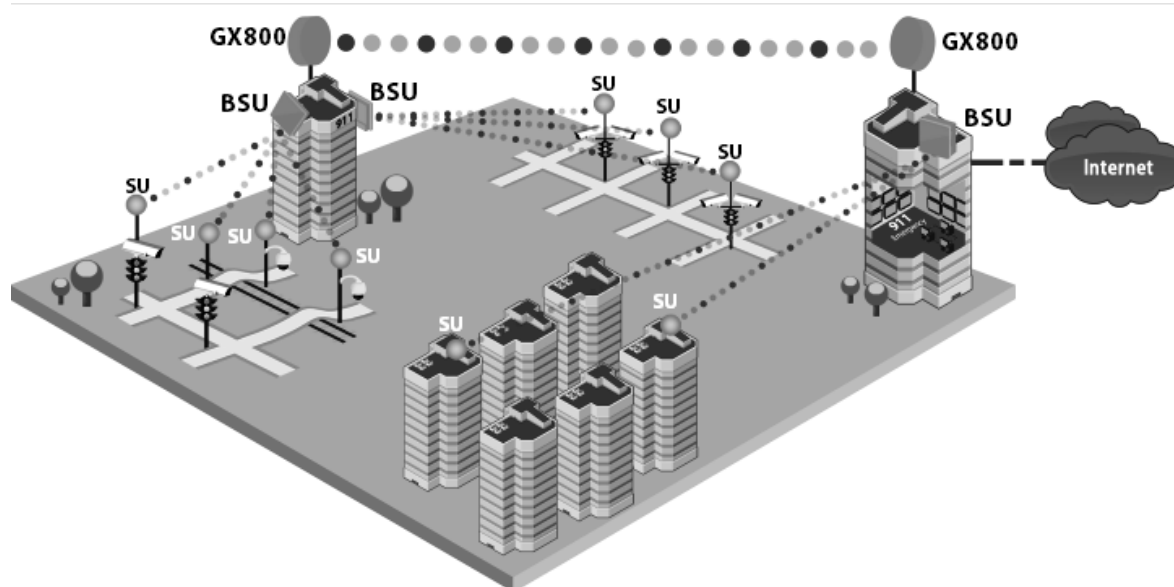
- **Security and Surveillance:** High definition IP-surveillance cameras for monitoring city streets, airports, bridges, seaports, transportation hubs, offices and warehouses.



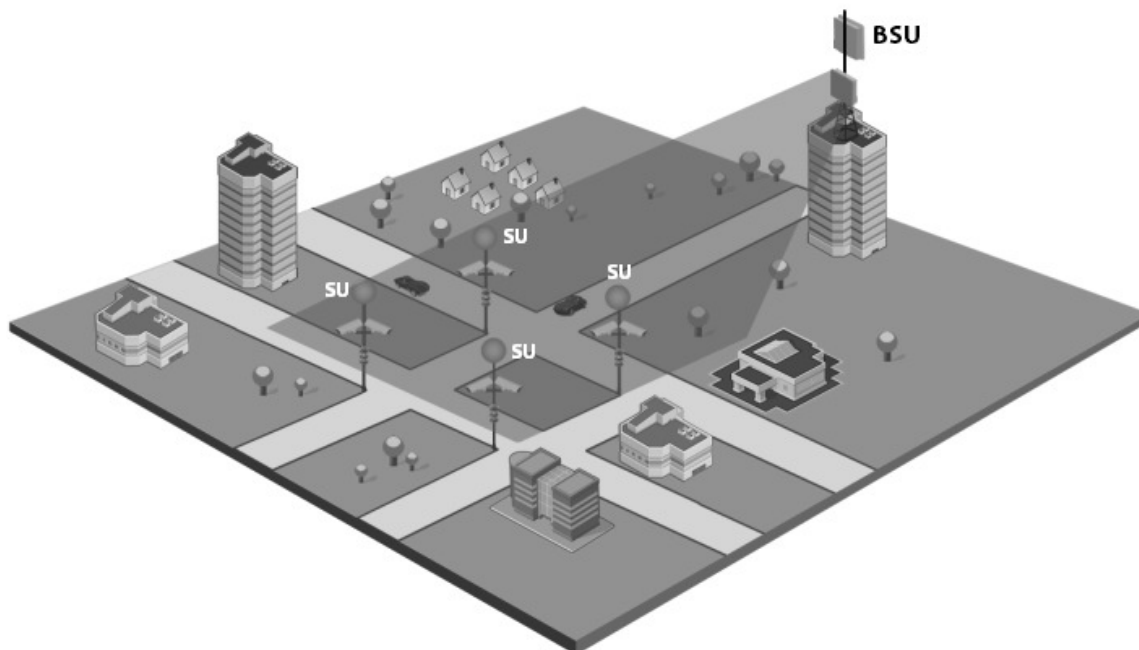
- **Metropolitan Area Network:** Secure and reliable connectivity between city buildings.



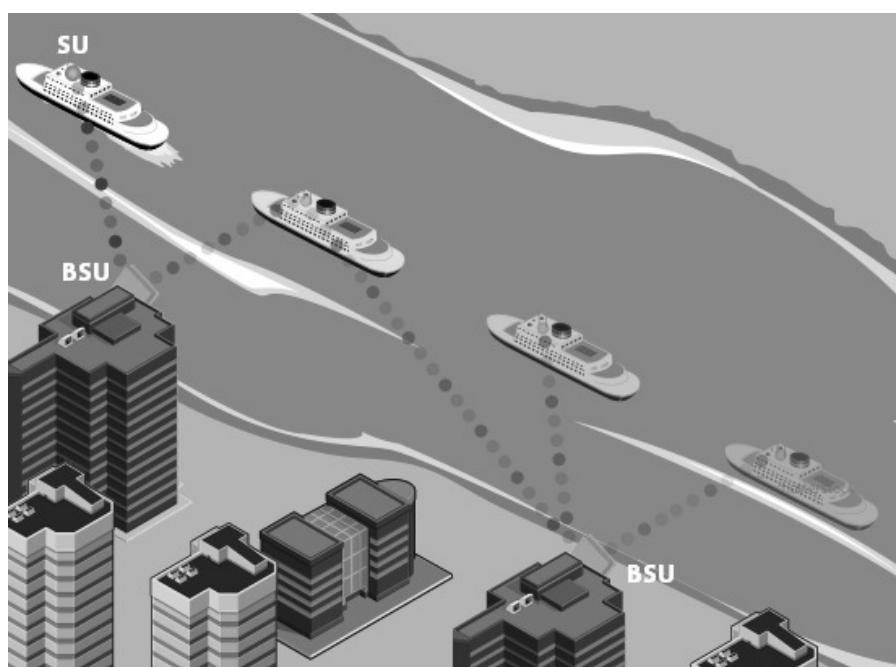
- **Enterprise Campus Connectivity:** Extend the main network to remote offices, warehouses or other buildings without leased lines.



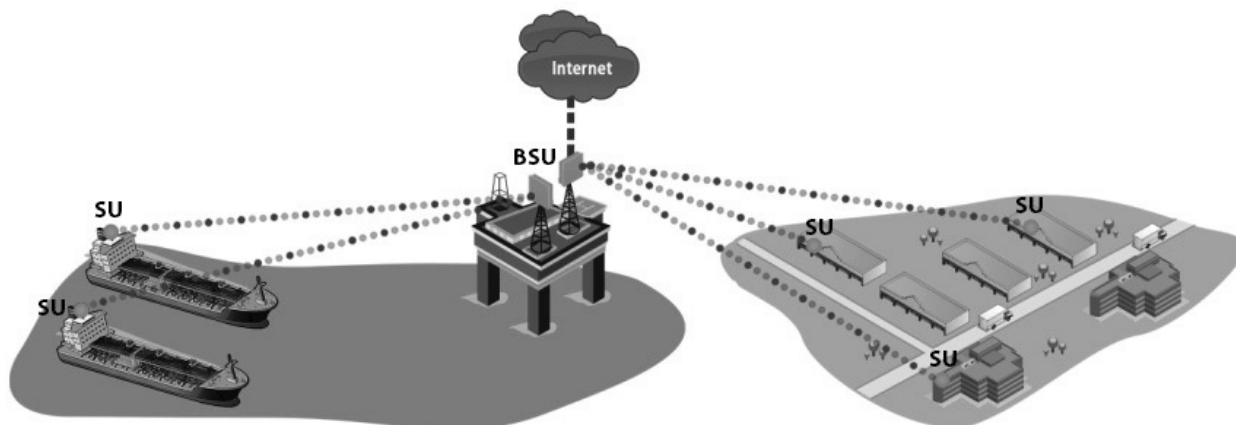
- **Wireless Intelligent Transport System (ITS):** Increases the traffic efficiency and reduces the commuting time in cities and metropolitan areas.



- **Roaming:** A mobile device (SU) provides seamless network services.



- **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.



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.

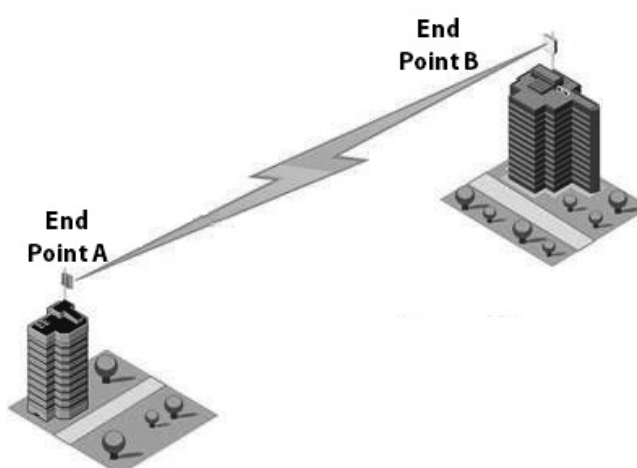


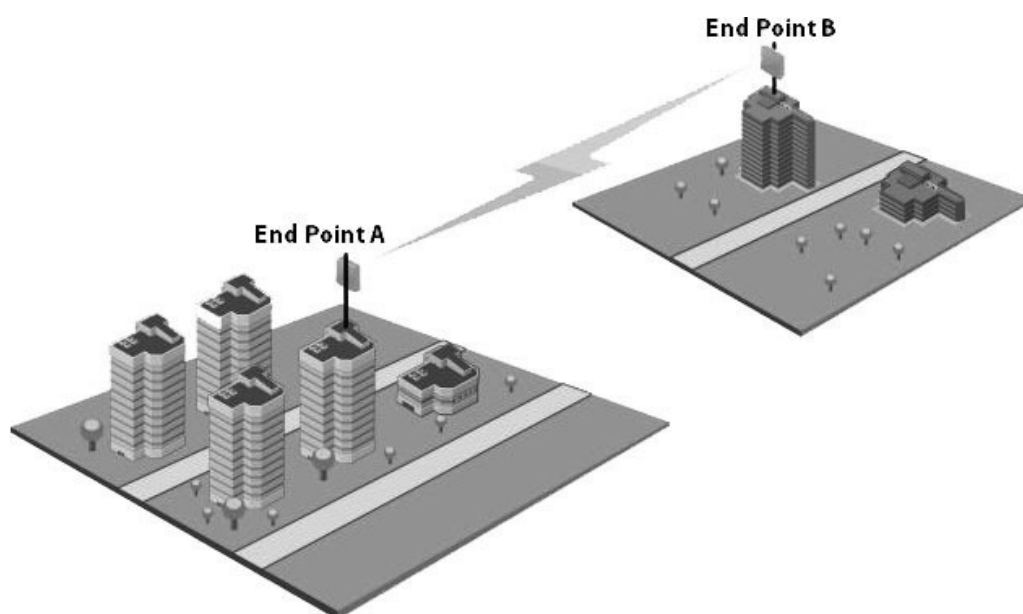
Figure 1-1 Point-to-Point-Link (An Example)

Given below are the deployment scenarios, where Proxim's point-to-point devices are recommended. The proxim devices used in the deployment images are commonly referred to as End Point A and End Point B. The combinations that are used for point-to-point devices are:

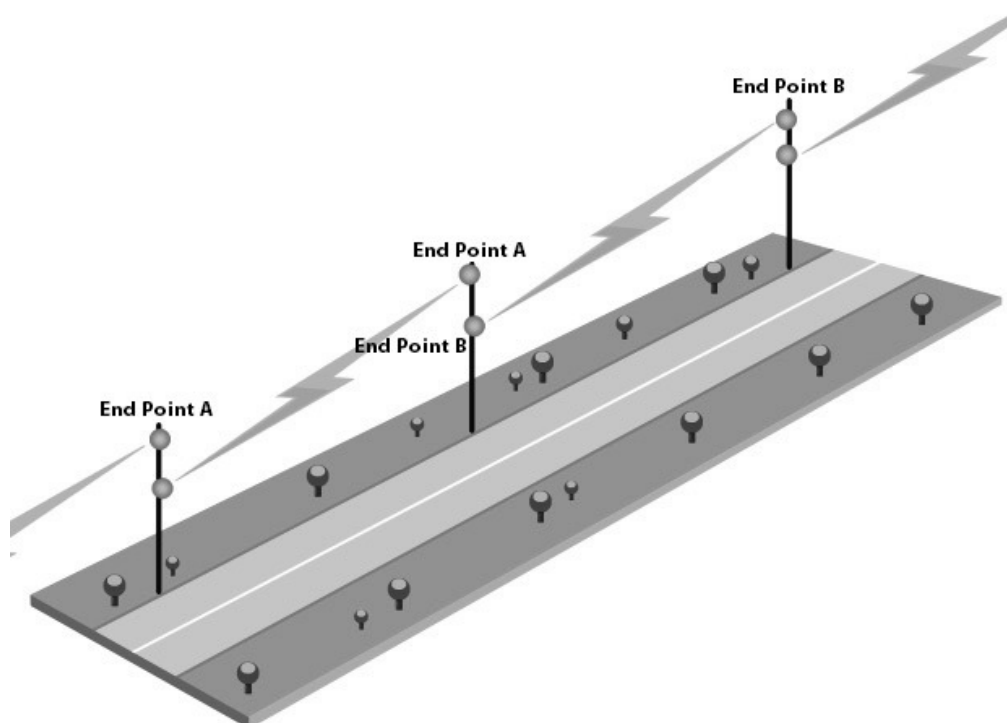
End Point A	End Point B
QB-8100-EPA	QB-8100-EPA
QB-8150-EPR	QB-8150-EPR
QB-8150-LNK-100	QB-8150-LNK-100
QB-8150-LNK-12/50	QB-8150-LNK-12/50
QB-8151-EPR	QB-8151-EPR
QB-8200-EPA	QB-8200-EPA
QB-8250-EPR	QB-8250-EPR
QB-825-EPR-50	QB-825-EPR-50
QB-825-EPR-50 ⁺	QB-825-EPR-50 ⁺

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

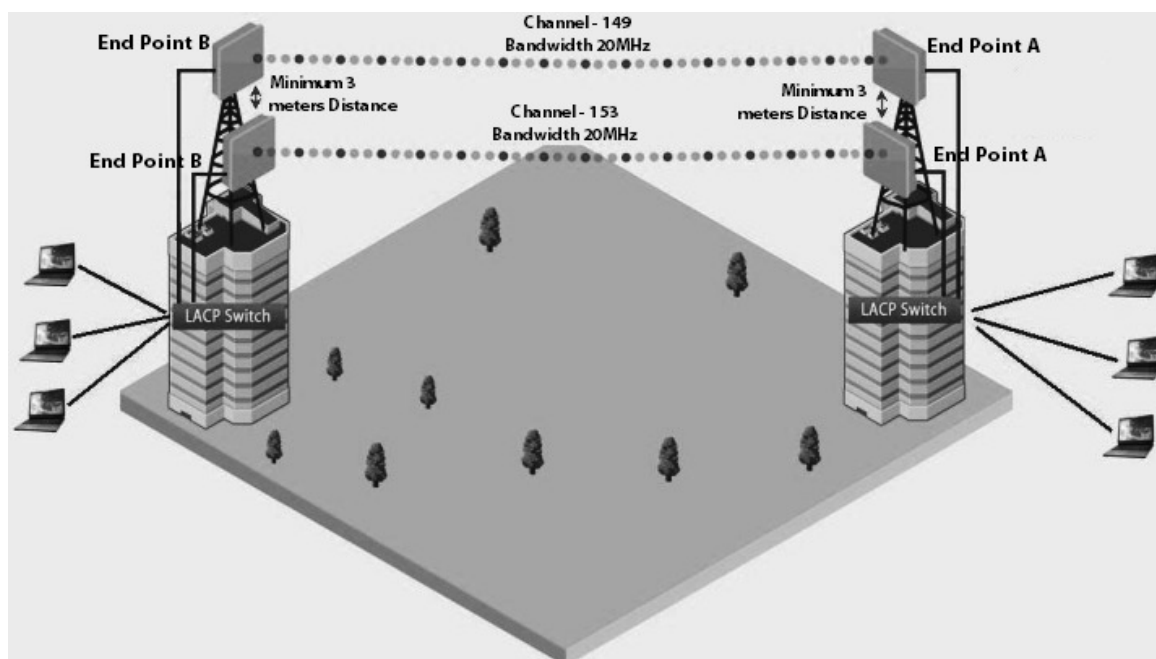
- **Backhaul to a Central POP:** Avoids expensive installation and recurring charge of a second wireline backhaul to a remote virtual POP.



- **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 to QB-8100-EPA/LNK, QB-8150-EPR/LNK, QB-8150-LNK-100, QB-8151-EPR/LNK, QB-8200-EPA/LNK, and QB-8250-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 800 & 8000 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 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 by 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 by throttling outgoing traffic in both base station and subscriber devices, thus 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 device.


- Web (HTTP/HTTPS) Interface
- Command Line Interface
- Simple Network Management Protocol (SNMP) Management
- ProximVision NMS

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. The Web interface can be accessed, through LAN (switch, hub and so on), the Internet, or with an Ethernet cable connected directly to the 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 by 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 by using the server and the client-side certificate.



- *Compatible browser for Web Interface:*
 - Microsoft Internet Explorer 7.0 or later
 - Mozilla Firefox 3.0 or later
- *When working with Internet Explorer 9 in Windows 2008 Server, navigate to **Internet Options -> Security -> Internet -> Custom Level -> Scripting -> Active Scripting** to enable active scripting.*
- *When working with Internet Explorer 10 and facing web page issues, click the **Broken Page** icon  available on the right side of the address bar.*

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. For example, when downloading a file, an administrator enters the download CLI command along with the IP address, file name, and file type parameters. Commands can be issued from the keyboard for real-time control, or from scripts that automate configuration.

2.2.1 HyperTerminal

The CLI can be accessed 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 using RS-232 cable, verify the following information in the HyperTerminal serial port setup:

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



: When using Windows 7, use a Terminal Emulator program like Teraterm Pro for serial connection.

2.2.2 Telnet

The device can be accessed through CLI by using Telnet. The device can be accessed through LAN (switch, hub and so on), the Internet, or with an Ethernet cable connected directly to the computer's Ethernet port.

2.2.3 Secure Shell (SSH)

The device can be securely accessed 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 the clients, to connect to the device. Clients need to verify that they are communicating with the correct SSH server.

2.3 Simple Network Management Protocol (SNMP) Management

The device can also be configured, managed and monitored by using 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

Before managing the device by using SNMP, compile one or more of these MIB files into your SNMP program's database.

The PXM MIB files are available on the Proxim support site at <http://my.proxim.com>. The enterprise MIB (PXM-SNMP.mib) defines the Read and Read/Write objects that can be viewed or configured by 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 NMS

ProximVision NMS is the state-of-the-art network management system to administer Proxim's devices on the network.

ProximVision NMS offers the following network management and monitoring features:

- Network Management --> Network Discovery, Geographical and Logical Maps
- Fault Management --> Event Logs and Alarms
- Performance Management --> Statistics Collection and Analysis
- Security Management --> User Provisioning
- Scheduled Bulk Operations and Task - Backup, Software Upgrade, and Bulk SNMP Parameter Configuration
- Configuration Management --> Device Configuration

For details, refer to ProximVision NMS Installation and Management Guide at <http://my.proxim.com>.



This guide explains the method to initialize and manage the device by using Web Interface only. To configure and manage the device by using Command Line Interface, please refer to the Tsunami® 800 & 8000 Series Reference Guide available on the Proxim's support site at <http://my.proxim.com>.

Device Initialization

This chapter contains information on the following:

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

3.1 Initialization

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



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

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

For all the modes of connection, the IP address of the device should be configured. As each network is different, a suitable IP address on the network must be assigned to the device. This IP address helps to configure, manage and monitor the device by using Web Interface, SNMP, or Telnet/CLI. The device can be assigned a **static/dynamic/auto** IP address. When set to **static**, the user has to set the IP address manually; 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. In case of QB-825-LNK-50, the factory configured IP address for End Point B is 169.254.128.131. If required, the end user can change it to the default IP address.



MP-8160-CPE-A100, MP-825-CPE-50, and QB-825-EPR-50 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, a user can,

- Scan devices (Proxim devices only) available on the network
- ScanTool v3.0.1 scans devices based on IPv4 or IPv6 address
- 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



- IPv6 is supported only by ScanTool v3.0.1 and higher versions.
- Network Adapter of ScanTool supports up to 16 virtual / real interfaces
- Disable Windows Firewall (or add an exception) for ScanTool to function or to detect the radio.

3.1.2 Initialize Device by 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://my.proxim.com> and search for ScanTool with (Answer ID 1735). Upon successful download, double-click the icon to start the ScanTool.
3. If there are more than one network adapter installed on the computer, then the user will be prompted to select the adapter for scanning Proxim devices. Use either an Ethernet or a Wireless Adapter. Select an adapter and click **OK**. The following **Scan List** screen appears, which displays all devices that are connected to the selected adapter.

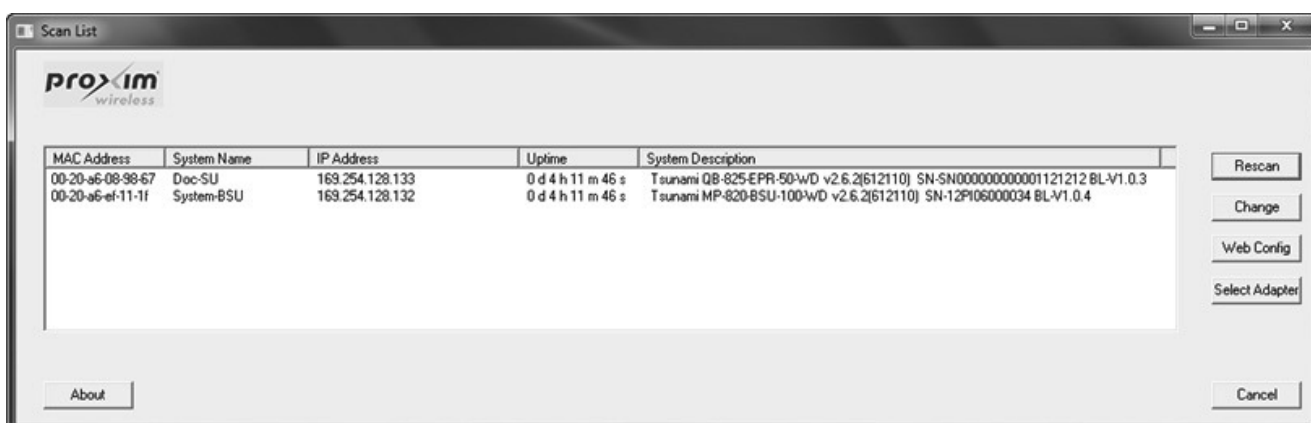


Figure 3-1 Scan List - Scanned Devices (IPv4)

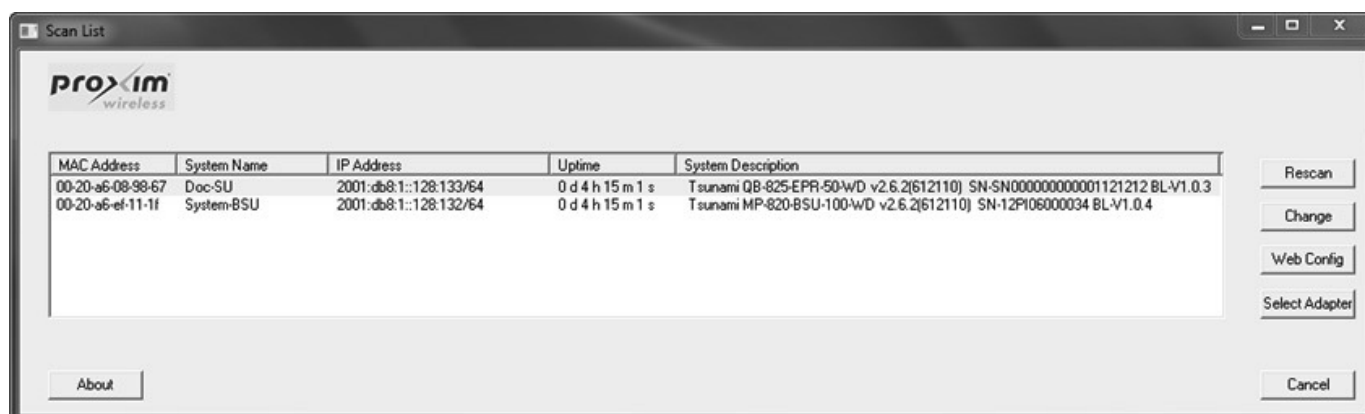


Figure 3-2 Scan List - Scanned Devices (IPv6)

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, MP-820-BSU-100-WD
 - **Firmware Version:** 2.X.Y; For example, version 2.6.2
 - **Serial Number :** For example, SN-12PI06000034
 - **Bootloader Version:** For example, BL - V1.0.4
4. Click **Select Adapter**, to change adapter settings.
 5. From the list, identify and select the MAC address of the device that needs to be initialized, and click **Web Config** to log on to the Web Interface.



*If the 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. 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 by using ScanTool

To modify the IP address of a device by using ScanTool, select the device from the scan list and click **Change**. A **Change** screen appears as shown in the following screen. 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 3-3 Modifying Device's IP Address (IPv4)

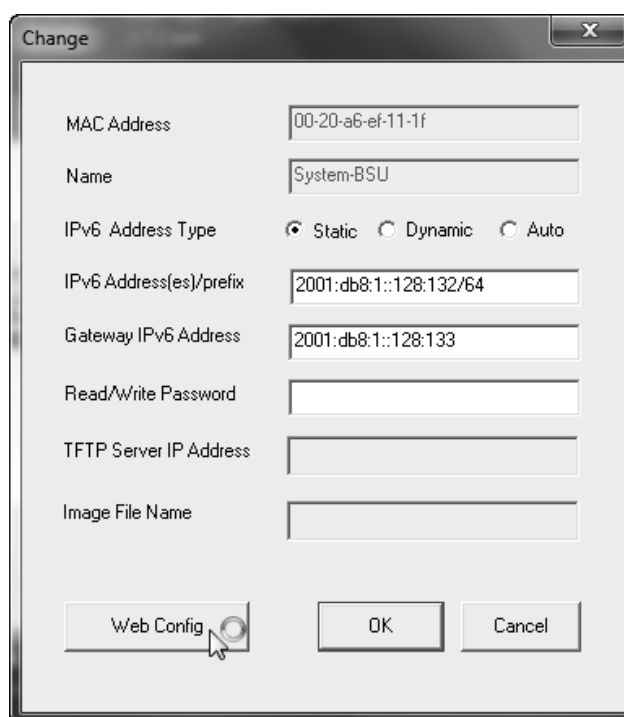


Figure 3-4 Modifying Device's IP Address (IPv6)

1. Select the **IP Address Type** as **static/dynamic** for IPv4 and as **static/dynamic/auto** for IPv6
 - **Static:** When set to static, the IP address of the device can be manually changed.
 - **Dynamic:** When set to dynamic, the IP address is dynamically generated by the DHCP server.
 - **Auto:** When set to auto, the IPv6 address is calculated by the device using the router advertisement messages.
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 logon, please see Logging onto the Web Interface.

3.2 Logging onto the Web Interface

Once the device is connected to the 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).

The user is now prompted to enter its username and password.



Figure 3-5 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 Wireless Site Survey and so on. However, the user can view the logs and statistics of the test tools.
 - Run the Spectrum Analyzer. However, the user can view the last scanned results.

The Monitor user has 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 the 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 the proxy server is not used for the connection.
- If unable to log on to the configuration pages by using default user name and password, please check with the administrator or follow Recovery Procedures.
- While using Internet Explorer, if wrong password is entered consecutively for three times, the HTTP session will get disconnected. If case of other browsers, the login screen will reset until a correct password is entered.

- 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 logon, the device home page appears.

The screenshot shows the Proxim Wireless device home page. At the top right, the user is logged in as 'Admin' and the system name is 'System-Name'. The system type is 'Tsunami MP-8200-BSU-WD-vx.Y.Z<Build Number>'. The left sidebar contains navigation buttons: COMMIT, REBOOT, HOME, BASIC CONFIGURATION, ADVANCED CONFIGURATION, MANAGEMENT, and MONITOR. The main content area is titled 'System Summary' and contains the following information:

System Name	System-Name
System Up-Time	00:00:01:14 (dd:hh:mm:ss)
IP Address	169.254.128.132
Remote Partners	1
Radio Mode	BSU
Network Mode	Bridge

Interface	Status	MAC Address	Speed/Mode
Ethernet 1	UP	00:20:a6:11:22:31	100 Mbps / Full Duplex
Ethernet 2	DOWN	00:20:a6:11:22:32	
Wireless	UP	00:20:a6:d9:dd:ae	

Below the interface table is an Event Log showing the following messages:

```

2000 Jan 1 00:00:43 kernel:Worp: WARNING: Channel Cost Histogram calculation
2000 Jan 1 00:00:43 kernel:Worp: WARNING: CACT scanning for channel 100 is st
2000 Jan 1 00:00:43 APPL: Wireless: BSU Started DFS Scanning on - Channel: 1
2000 Jan 1 00:00:45 APPL: Wireless: Channel(offset) 100(0), Ch.BW 20MHz
2000 Jan 1 00:00:48 APPL: Sysmgmt: System Initialization Successful With Debu

```

At the bottom of the event log, there are buttons for 'Clear Event Log' and 'Refresh'.

Figure 3-6 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 and build number.
- **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 a link on 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:

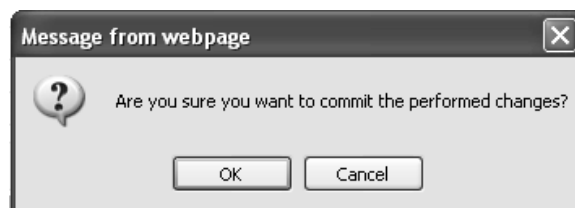


Figure 3-7 Commit

Click **OK**, to confirm the changes.

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

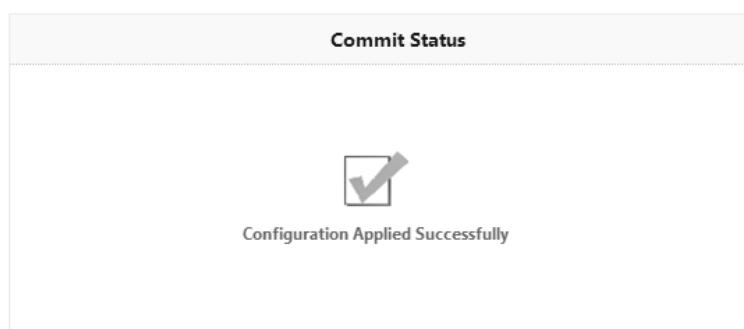


Figure 3-8 Commit Status

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

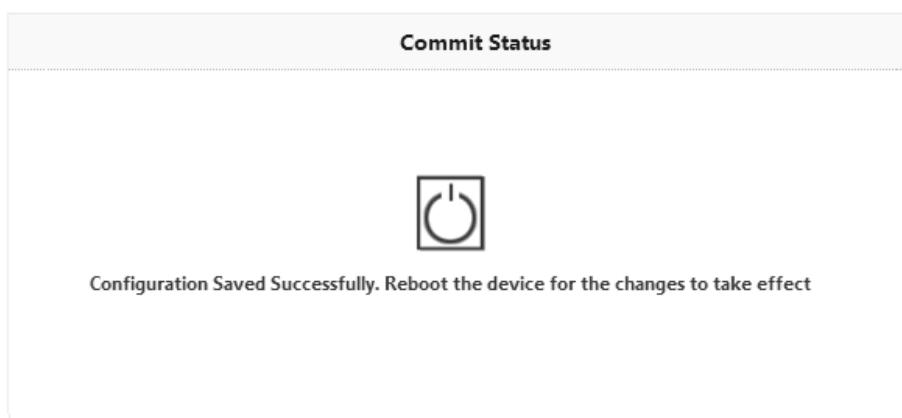


Figure 3-9 Commit Status with Reboot Message

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, Network Mode and so on, require device reboot for the changes 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.

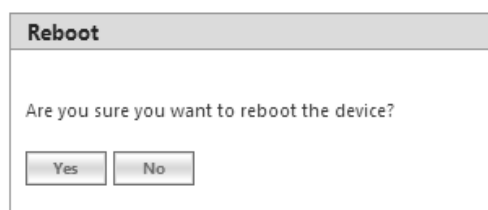


Figure 3-10 Reboot



*: 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 Mode	IPv4 Only	IPv4 Only
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
Secondary BSU Name	Not Applicable	SU - Blank (Secondary BSU name is not configured) End Point B - Not Applicable
DNS Proxy	Enabled	Enabled
Legacy Mode	BSU - Disabled End Point A - Not Applicable	SU - Disabled End Point B - Not Applicable

Parameter	BSU Mode/ End Point A	SU Mode/ End Point B
Maximum Number of SUs (per BSU)	MP-8100-BSU (rev 1 to rev 6) --> 100 MP-8100-BSU (rev 7 and above) --> 250 MP-8160-BSU --> 250 MP-8160-BS9 --> 250 MP-8200-BSU --> 250 MP-8250-BS9 --> 250 MP-8250-BS1 --> 250 MP-820-BSU-100--> 10	Not Applicable
Registration Timeout	10 Seconds	10 Seconds
Link Profiles	Default Link Profile	Default Link Profile
DDRS	Enabled	Enabled
Input Bandwidth Limit	As per license	As per license
Output Band Limit	As per license	As per license
Roaming	BSU - Disabled End Point A - Not Applicable	SU - Disabled End Point B - Not Applicable
Security Profile	Enabled with profile name "WORP Security"	Enabled with profile name "WORP Security"
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
Allow Untagged Management Access	Disabled	Disabled
Global Filtering	Disabled	Disabled
DHCP Server	Disabled	Disabled
STP/LACP	Enabled (configured as "passthru")	Enabled (configured as "passthru")
DHCP Relay	Disabled	Disabled

Parameter	BSU Mode/ End Point A	SU Mode/ End Point B
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
LED Display Status	RSSI Enabled	RSSI Enabled

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	<input type="text" value="System-Name"/>	(0-64) Characters	
Frequency Domain	<input type="text" value="World 5 GHz"/>	<input type="button" value="v"/>	*
Radio Mode	<input type="text" value="BSU"/>	<input type="button" value="v"/>	*
Channel Bandwidth	<input type="text" value="20"/>	<input type="button" value="v"/>	MHz *
Auto Channel Selection	<input type="text" value="Disable"/>	<input type="button" value="v"/>	*
Preferred Channel	<input type="text" value="160 (5.8 GHz)"/>	<input type="button" value="v"/>	
Active Channel	160 (5.8 GHz)		
Network Name	<input type="text" value="MY_NETWORK"/>	(1-32) Characters	
Legacy Mode	<input type="text" value="Disable"/>	<input type="button" value="v"/>	*
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="text" value="Static"/>
Default Gateway IP Address*			
IP Address	<input type="text" value="169.254.128.132"/>		
* Reboot is required			
Notes:			
1. Change in <i>Radio Mode</i> will reset Wireless and WORP parameters to default after reboot.			
2. Disable DHCP Server before changing the network configurations such as <i>IP Address, Subnet Mask, Address Type</i> .			
<input type="button" value="OK"/>			

Figure 4-1 Basic Configuration (BSU)

Basic Configuration

System Name	<input type="text" value="System-Name"/>	(0-64) Characters
Frequency Domain	<input type="text" value="World 5 GHz"/>	*
Radio Mode	<input type="text" value="SU"/>	*
Active Radio Mode	BSU	
Channel Bandwidth	<input type="text" value="20"/>	MHz *
Auto Channel Selection	<input type="text" value="Enable"/>	
Active Channel	160 (5.8 GHz)	
Network Name	<input type="text" value="MY_NETWORK"/>	(1-32) Characters
Primary BSU Name	<input type="text"/>	
Legacy Mode	<input type="text" value="Disable"/>	*

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="text" value="Static"/>

Default Gateway IP Address*

IP Address

* Reboot is required

Notes:

1. Change in *Radio Mode* will reset Wireless and WORP parameters to default after reboot.
2. *Auto Channel Selection* cannot be disabled when *Secondary BSU Name* is configured.
3. Disable DHCP Server before changing the network configurations such as *IP Address, Subnet Mask, Address Type*.

Figure 4-2 Basic Configuration (SU)

Basic Configuration

System Name	<input type="text" value="System-Name"/>	(0-64) Characters
Frequency Domain	<input type="text" value="World 5 GHz"/>	*
Radio Mode	<input type="text" value="End Point A"/>	*
Channel Bandwidth	<input type="text" value="20"/>	MHz *
Auto Channel Selection	<input type="text" value="Disable"/>	*
Preferred Channel	<input type="text" value="160 (5.8 GHz)"/>	
Active Channel	160 (5.8 GHz)	
Network Name	<input type="text" value="MY_NETWORK"/>	(1-32) Characters

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="text" value="Static"/>

Default Gateway IP Address*

IP Address

* Reboot is required

Notes:

- Change in *Radio Mode* will reset Wireless and WOPR parameters to default after reboot.

Figure 4-3 Basic Configuration (End Point A)


Basic Configuration			
System Name	<input type="text" value="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	71 (5.355 GHz)		
Network Name	MY_NETWORK (1-32) Characters		
End Point A Name	<input type="text"/>		
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"/>	Static
Default Gateway IP Address*			
IP Address	<input type="text" value="169.254.128.132"/>		
* Reboot is required			
Notes:			
1. Change in <i>Radio Mode</i> will reset Wireless and WORP parameters to default after reboot.			
<input type="button" value="OK"/>			




Figure 4-4 Basic Configuration (End Point B)



Below is the table which explains basic parameters and the method to configure the configurable parameter(s):




Recommended characters for the name field are A-Z a-z 0-9 - _ =: . @ \$ & and space.

Parameter	Description
System Name	<p>By default, the device name is System-Name.</p> <p>Change the default device name to the desired one, with name ranging from 0 to 64 characters.</p> <p> : The system name configured for the device shall be unique across all devices in a given WORP network.</p>

Parameter	Description
Frequency Domain	<p>This parameter specifies the country of operation, permitted frequency bands and regulatory rules for a particular country or domain. When the frequency domain is selected, the Dynamic Frequency Selection (DFS) and Automatic Transmit Power Control (ATPC) features are enabled automatically if the selected country and band has a regulatory domain that requires it. The Frequency domain selection pre-selects and displays only the allowed frequencies for the selected country or domain.</p>  <ul style="list-style-type: none"> • Devices are pre-configured to scan and display only the outdoor frequencies permitted in the respective country. No other countries, channels, or frequencies can be configured. <ul style="list-style-type: none"> — Do not exceed the maximum EIRP permitted in the particular country. — Configure the ATPC/TPC parameters by choosing the correct cable type / attenuator — It is the responsibility of the professional installer to properly install and configure the device parameters in accordance with the respective country laws. <p>For non-US device, the default frequency domain selected is World 5MHz. For more details on frequency domains, see Frequency Domains and Channels.</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 a BSU device, the radio mode can be changed from BSU to SU and vice versa. Also, in an End Point A device, the radio mode can be changed from End Point A to End Point B and vice versa.</p>  <p>: A change in radio mode will reset wireless and WORP parameters to defaults 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>  <p>: The 40 MHz frequency band is not applicable to MP 800 & 8000 BSU and SU devices, when configured in Legacy Mode.</p> <p>For more details on supported Channel Bandwidth, see Frequency Domains and Channels.</p>

Parameter	Description
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 an 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> <p> : Irrespective of the ACS status, the BSU/End Point A will automatically select a new channel upon radar detection.</p>
Preferred Channel	<p>Applicable only when the Auto Channel Selection (ACS) is disabled. This parameter enables to select a specific channel (in the specified frequency domain) for the device to operate.</p>
Active Channel	<p>Displays the current active channel of operation. 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>
Network Name	<p>Network name to identify a wireless network. The network name can be of minimum 1 or maximum 32 characters. The default network name is MY_NETWORK.</p> <p> : 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.</p>
Primary BSU Name	<p>Applicable only to an SU.</p> <p>Represents the Primary BSU name. If the primary BSU name is configured then SU establishes link with it. If a name is not configured then SU establishes link with any BSU on the same network, which meets the registration criteria.</p>
End Point A Name	<p>Applicable only to an End Point B.</p> <p>If a name is configured for End Point A then End Point B establishes a wireless link with it. If a name is not configured then End Point B establishes link with any End Point A on the same network that meets the registration criteria.</p>

Parameter	Description
Legacy Mode	<p>By default, this parameter is disabled. When enabled, the MP 800 & 8000 BSU and SU devices can interoperate with the legacy products of the Tsunami® MP.11 family.</p> <p>The MP 800 & 8000 devices that provide legacy support are,</p> <ul style="list-style-type: none"> • MP-8100-BSU • MP-8100-SUA • MP-8150-SUR • MP-8150-CPE • MP-8150-SUR-100 • MP-8200-BSU • MP-8250-BS9 • MP-8250-BS1 • MP-8200-SUA • MP-8250-SUR • MP-825-CPE-50 • MP-825-SUR-50⁺ • MP-820-BSU-100 • MP-820-SUA-50⁺ <p> : MP 800/8000 BSU device in legacy mode can connect to a MP 800/8000 SU device only when configured in legacy mode.</p>
IP Configuration, and Default Gateway IP Address	See Network.

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



: Reboot the device, if any of the parameters with an asterisk symbol are configured.

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



: Recommended characters for the name field are A-Z a-z 0-9 - _ = : . @ \$ & and space.

5.1 System

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

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

The screenshot shows the 'System' configuration window with the following fields and values:

System	
Radio Mode	BSU *
Frequency Domain	World 5 GHz *
Network Mode	Bridge *
Maximum MTU (Refer Note 2)	1500 (1500-2048) *
Frequency Filter Lower Edge	0 (0-10000) MHz *
Frequency Filter Upper Edge	10000 (0-10000) MHz *
LED Display	
LED Status	RSSI
SU Wireless MAC Address	00:00:00:00:00:00

* Reboot is required

Notes:

1. Excluding Ethernet Header(14 bytes) + VLAN Tag(4 bytes).
2. For optimal performance, *Maximum MTU* should be configured the same on both BSU and SU.
3. A valid *SU Wireless MAC Address* is required for LED Display based on RSSI.

OK


Figure 5-1 System Configuration

Given 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 SKU, the radio mode is set to either BSU, SU, End Point A or End Point B. In a BSU device, the radio mode can be changed from BSU to SU and vice versa. Also, in an End Point A device, the radio mode can be changed from End Point A to End Point B and vice versa. But note that a change in radio mode will reset wireless and WORP parameters of the device after reboot.
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 Frequency Domains and Channels.
Network Mode	The device can be configured in two network modes: Bridge and Routing . By default, the network mode is Bridge mode.

Parameter	Description
Active Network Mode	<p>A change in the network mode (either Bridge or Routing mode) is applied on the device only when the device is rebooted.</p> <p>So, when the network mode is changed and the device is not rebooted, this parameter displays the current operating network mode of the device.</p>
Frequency Filter Lower Edge, and Frequency Filter Upper Edge	<p>These parameters enables 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.</p> <p>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.</p>

Parameter	Description																																				
Maximum MTU (Maximum Transmission Unit)	<p>Given below are the devices and their corresponding MTU configurable range:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th style="text-align: center;">Devices</th> <th style="text-align: center;">MTU Configurable Range</th> </tr> </thead> <tbody> <tr> <td>MP-8150-CPE; MP-8160-CPE-A100 MP-820-BSU-100; MP-820-SUA-50+ MP-825-CPE-50; MP-825-SUR-50+ QB-8150-LNK-12/50; QB-825-EPR/LNK-50 QB-825-EPR/LNK-50+</td> <td style="text-align: center;">1500 to 2048 bytes</td> </tr> <tr> <td>MP-8100-BSU; MP-8100-SUA MP-8150-SUR; MP-8150-SUR-100 MP-8160-BSU; MP-8160-SUA; MP-8160-BS9 QB-8100-EPA/LNK; QB-8150-EPR/LNK QB-8150-LNK-100; QB-8151-EPR/LNK MP-8200-BSU/SUA; MP-8250-BS9/BS1; MP-8250-SUR QB-8200-EPA/LNK; QB-8250-EPR/LNK</td> <td style="text-align: center;">1500 to 1514 bytes</td> </tr> </tbody> </table> <p>Maximum Frame Size = Configured MTU + Ethernet Header (14 bytes) + VLAN Header (4 bytes) + Frame Check Sequence (4 bytes) Maximum Payload = Configured MTU – Feature Header</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th rowspan="2" style="text-align: center;">Feature</th> <th rowspan="2" style="text-align: center;">Feature Header (in bytes)</th> <th colspan="2" style="text-align: center;">Maximum Payload (in Bytes)</th> </tr> <tr> <th style="text-align: center;">#</th> <th style="text-align: center;">*</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td style="text-align: center;"> MP-8100-BSU MP-8100-SUA MP-8150-SUR MP-8150-SUR-100 MP-8160-BSU MP-8160-BS9 MP-8160-SUA QB-8100-EPA/LNK QB-8150-EPR/LNK QB-8150-LNK-100 QB-8151-EPR/LNK MP-8200-BSU/SUA MP-8250-BS9/BS1 MP-8250-SUR QB-8200-EPA/LNK QB-8250-EPR/LNK </td> <td style="text-align: center;"> MP-8150-CPE MP-8160-CPE-A100 MP-825-CPE-50 MP-825-SUR-50+ MP-820-BSU-100 MP-820-SUA-50+ QB-8150-LNK-12 QB-8150-LNK-50 QB-825-EPR/LNK-50 QB-825-EPR/LNK-50+ </td> </tr> <tr> <td>General or Single VLAN</td> <td style="text-align: center;">0</td> <td style="text-align: center;">1514</td> <td style="text-align: center;">2048</td> </tr> <tr> <td>QinQ</td> <td style="text-align: center;">4</td> <td style="text-align: center;">1510</td> <td style="text-align: center;">2044</td> </tr> <tr> <td>PPPoE</td> <td style="text-align: center;">8</td> <td style="text-align: center;">1506</td> <td style="text-align: center;">2040</td> </tr> <tr> <td>IP Tunneling (IP in IP Encapsulation)</td> <td style="text-align: center;">20</td> <td style="text-align: center;">1494</td> <td style="text-align: center;">2028</td> </tr> <tr> <td>IP Tunneling (GRE Encapsulation)</td> <td style="text-align: center;">24</td> <td style="text-align: center;">1490</td> <td style="text-align: center;">2024</td> </tr> </tbody> </table> <p># Assuming that MTU is configured as 1514 * Assuming that MTU is configured as 2048</p> <p>For optimal performance, MTU should be configured same on both the ends.</p>	Devices	MTU Configurable Range	MP-8150-CPE; MP-8160-CPE-A100 MP-820-BSU-100; MP-820-SUA-50+ MP-825-CPE-50; MP-825-SUR-50+ QB-8150-LNK-12/50; QB-825-EPR/LNK-50 QB-825-EPR/LNK-50+	1500 to 2048 bytes	MP-8100-BSU; MP-8100-SUA MP-8150-SUR; MP-8150-SUR-100 MP-8160-BSU; MP-8160-SUA; MP-8160-BS9 QB-8100-EPA/LNK; QB-8150-EPR/LNK QB-8150-LNK-100; QB-8151-EPR/LNK MP-8200-BSU/SUA; MP-8250-BS9/BS1; MP-8250-SUR QB-8200-EPA/LNK; QB-8250-EPR/LNK	1500 to 1514 bytes	Feature	Feature Header (in bytes)	Maximum Payload (in Bytes)		#	*			MP-8100-BSU MP-8100-SUA MP-8150-SUR MP-8150-SUR-100 MP-8160-BSU MP-8160-BS9 MP-8160-SUA QB-8100-EPA/LNK QB-8150-EPR/LNK QB-8150-LNK-100 QB-8151-EPR/LNK MP-8200-BSU/SUA MP-8250-BS9/BS1 MP-8250-SUR QB-8200-EPA/LNK QB-8250-EPR/LNK	MP-8150-CPE MP-8160-CPE-A100 MP-825-CPE-50 MP-825-SUR-50+ MP-820-BSU-100 MP-820-SUA-50+ QB-8150-LNK-12 QB-8150-LNK-50 QB-825-EPR/LNK-50 QB-825-EPR/LNK-50+	General or Single VLAN	0	1514	2048	QinQ	4	1510	2044	PPPoE	8	1506	2040	IP Tunneling (IP in IP Encapsulation)	20	1494	2028	IP Tunneling (GRE Encapsulation)	24	1490	2024
Devices	MTU Configurable Range																																				
MP-8150-CPE; MP-8160-CPE-A100 MP-820-BSU-100; MP-820-SUA-50+ MP-825-CPE-50; MP-825-SUR-50+ QB-8150-LNK-12/50; QB-825-EPR/LNK-50 QB-825-EPR/LNK-50+	1500 to 2048 bytes																																				
MP-8100-BSU; MP-8100-SUA MP-8150-SUR; MP-8150-SUR-100 MP-8160-BSU; MP-8160-SUA; MP-8160-BS9 QB-8100-EPA/LNK; QB-8150-EPR/LNK QB-8150-LNK-100; QB-8151-EPR/LNK MP-8200-BSU/SUA; MP-8250-BS9/BS1; MP-8250-SUR QB-8200-EPA/LNK; QB-8250-EPR/LNK	1500 to 1514 bytes																																				
Feature	Feature Header (in bytes)	Maximum Payload (in Bytes)																																			
		#	*																																		
		MP-8100-BSU MP-8100-SUA MP-8150-SUR MP-8150-SUR-100 MP-8160-BSU MP-8160-BS9 MP-8160-SUA QB-8100-EPA/LNK QB-8150-EPR/LNK QB-8150-LNK-100 QB-8151-EPR/LNK MP-8200-BSU/SUA MP-8250-BS9/BS1 MP-8250-SUR QB-8200-EPA/LNK QB-8250-EPR/LNK	MP-8150-CPE MP-8160-CPE-A100 MP-825-CPE-50 MP-825-SUR-50+ MP-820-BSU-100 MP-820-SUA-50+ QB-8150-LNK-12 QB-8150-LNK-50 QB-825-EPR/LNK-50 QB-825-EPR/LNK-50+																																		
General or Single VLAN	0	1514	2048																																		
QinQ	4	1510	2044																																		
PPPoE	8	1506	2040																																		
IP Tunneling (IP in IP Encapsulation)	20	1494	2028																																		
IP Tunneling (GRE Encapsulation)	24	1490	2024																																		

Parameter	Description
LED Status	<p>The Received Signal Strength Indicator (RSSI) LEDs indicates that the unit is powered on, and LEDs will glow based on RSSI value indicating link status. By default, all 5 LEDs will blink at an interval of 1 sec. When the LED Status is disabled, all LEDs will be turned off.</p> <p> : 'RSSI LED' feature is applicable only to 82x MP and QB devices.</p>
SU Wireless MAC Address	<p>This field is applicable only for a BSU. In order to monitor the SU link statistics, the user should first configure the wireless MAC address of the SU. If the configured SU is registered with the BSU, then the LEDs will glow based on the RSSI value else all the 5 LEDs will blink. To get the SU Wireless MAC Address, navigate to MONITOR > WORM Statistics > Interface 1 > SU Link Statistics.</p>

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



: For more details regarding LED display and RSSI LED behavior, refer System.

5.2 Network

The **Network** tab allows 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:

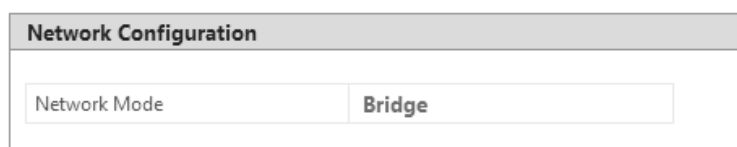


Figure 5-2 Bridge Mode

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

The IP addresses can be configured in two modes. They are:

- **IPv4**: IPv4 is the widely used version of Internet Protocol defining the IP address in 32-bit in size.
- **IPv6**: Ipv6 is the latest version of Internet Protocol with new addressing system for more IP addresses than IPv4. The IPv6 address is 128-bit in size.

 : IPv6 address is supported only in bridge mode.

5.2.1.1 Bridge Mode

5.2.1.1.1 IP Configuration (IPv4 Only)

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:

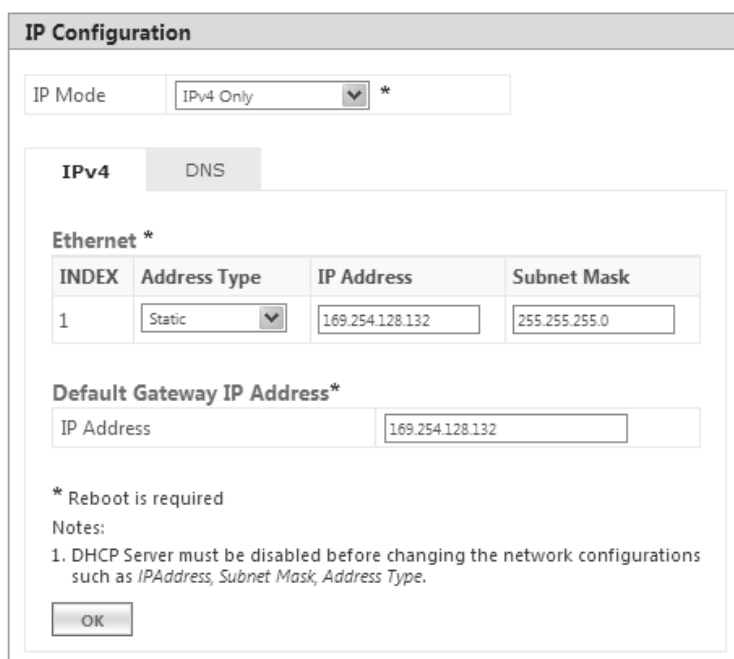



Figure 5-4 IPv4 Configuration (Bridge Mode)

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

Parameter	Description
IP Mode	Represents the IP Mode of the device. The IP Mode can be set to either IPv4 Only or Dual (IPv4 and IPv6). By default, IP Mode is set to IPv4 Only .  : A change in IP mode requires device reboot.
Ethernet (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 Static meaning which the user can manually configure the network parameters. Select Dynamic to configure the device as a DHCP client. If Dynamic is selected, the device obtains the IP parameters from a DHCP server automatically during the bootup. If a DHCP server is not available or to manually configure the device's IP settings, select Static.</p>
IP Address	<p>Represents the IP address of the Ethernet interface.</p> <p>When the address type is set to Static (default address type), the IP address can be manually configured. By default, the static IP address is set to 169.254.128.132. When the address type is set to Dynamic, this parameter is read-only and displays the device IP address obtained from the DHCP server. The device will fall back 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 Static (default address type), the subnet mask can be manually configured. By default, the subnet mask is set to 255.255.255.0. When the address type is set to Dynamic, this parameter is read-only and displays the device current subnet mask obtained from the DHCP server. The subnet mask will fall back to 255.255.255.0, if the device cannot obtain the subnet mask from the DHCP server.</p>
Default Gateway IP Address	
IP Address	<p>Represents the gateway IP address of the device.</p> <p>When the address type is set to Static (default address type), the gateway IP address can be manually configured. By default, the gateway IP address is set to 169.254.128.132. When the address type is set to Dynamic, 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 fall back to 169.254.128.132, if it cannot obtain the gateway IP address from a DHCP server.</p>

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

5.2.1.1.2 IP Configuration (IPv4 and IPv6)

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:

IP Configuration

IP Mode: IPv4 and IPv6 *

IPv4 | **IPv6** | DNS

Ethernet *

INDEX	Link Local IP Address
1	fe80::220:a6ff:fe12:8934/64

INDEX	Address Type	IP Address with Prefix
1	Static	2001:220:a6ff:fe12:8934/64

Default Gateway IP Address*


IP Address: 2001:220:a6ff:fe12:8934/64

* Reboot is required
 Notes:
 1. DHCP Server must be disabled before changing the network configurations such as IP Address, Address Type.

OK

Figure 5-5 IPv6 Configuration (Bridge Mode)

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

Parameter	Description
IP Mode	Represents the IP Mode of the device. The IP Mode can be set to either IPv4 Only or Dual (IPv4 and IPv6). By default, the IP Mode is set to IPv4 Only .  : A change in IP mode requires device reboot.
Ethernet (Please note that the number of Ethernet interfaces depend on your device.)	
Link Local IP Address	Link Local IP Address is an Internet protocol that is intended for communication within the segment of a local network or point-to-point connection that a host is connected to. During initial bootup, each system is assigned with a Link Local IP Address whose prefix is fe80::.../64 . The Link Local IP Address is a read only parameter.

Parameter	Description
Address Type	<p>Specifies whether the Ethernet interface parameters are to be configured through Dynamic Host Configuration Protocol (DHCP) or Stateless Auto Configuration or to be assigned statically.</p> <p>Select Auto (default address type) to configure the device automatically. If Auto is selected, device obtains the IPv6 address, using the prefix obtained from the router advertisement.</p> <p>Select Static to configure the device manually. If Static is selected, the user should manually configure the network parameters.</p> <p>Select Dynamic to configure the device as a DHCP client. If Dynamic is selected, device obtains the IPv6 parameters from a DHCP server automatically. If the DHCP server is not available, the device will be accessible through Link Local IP Address.</p>
IP Address with Prefix	<p>Represents the IP address of the Ethernet interface.</p> <p>For Example: The IP address is represented as 2000::220:a6ff:fe00:1/64, where "/64" is called the IP prefix or network prefix.</p> <p>When the address type is set to Auto (default address type), this parameter is read-only and displays the device IP address obtained from the router advertisements.</p> <p>When the address type is set to Dynamic, this parameter is read-only and displays the device IPv6 address obtained from the DHCP server. If device fails to get dynamic IP from DHCP server, the device will be accessible through Link Local IP Address.</p> <p>When the address type is set to Static, the IPv6 address should be manually configured along with prefix.</p>
Default Gateway IP Address	
IP Address	<p>Represents the gateway IP address of the device.</p> <p>When the address type is set to Auto (default address type), this parameter is read-only and displays the device IP address obtained from the router advertisement.</p> <p>When the address type is set to Static, the gateway IP address should be manually configured (prefix is not required).</p> <p>When the address type is set to Dynamic, the device uses the IP address obtained from DHCP server. The IP address obtained from DHCP server can be viewed in Routing Table. If IP address is not obtained from the DHCP server, then the device uses the user configured IP address.</p>

5.2.1.1.3 DNS

DNS server is used to resolve/translate a domain name into an IP address.

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

IP Configuration

IP Mode: IPv4 and IPv6 *

IPv4 | IPv6 | **DNS**

DNS *


Primary IP Address: 169.254.128.20

Secondary IP Address: 2001:db8:1:10:1

* Reboot is required

OK

Figure 5-6 DNS Configuration (Bridge Mode)

Parameter	Description
Primary and Secondary IP Address	<p>Represents the IP address of the Primary and Secondary DNS Server.</p> <p>Primary and Secondary IP Address can be configured manually irrespective of the IP mode. The DNS address obtained from the DHCP server (Dynamic mode) or from the router advertisement (Auto Mode) is given preference over the manually configured IP Addresses.</p> <p>The device lists all the IP addresses from DNS server configured manually or obtained from DHCP server/ router advertisement and only top three DNS server IP addresses will be used. To view the IP addresses refer DNS Addresses.</p> <p> : IPv4 addresses will be given preference over IPv6 addresses.</p>

5.2.1.2 Routing Mode



- A device (BSU/SU) will act as a DHCP Client only when configured in Bridge Mode.
- In Routing Mode,
 - With PPPoE Client disabled, the device (BSU/SU) IP addresses are assigned only statically.
 - With PPPoE Client enabled, the device (SU) IP addresses can be assigned both statically and dynamically. See Routing Mode with PPPoE Client Enabled

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

IP Configuration

IPv4
DNS

Ethernet *

INDEX	IP Address	Subnet Mask
1	<input type="text" value="169.254.128.132"/>	<input type="text" value="255.255.255.0"/>
2	<input type="text" value="169.254.129.132"/>	<input type="text" value="255.255.255.0"/>

Wireless*

INDEX	IP Address	Subnet Mask
1	<input type="text" value="169.254.130.132"/>	<input type="text" value="255.255.255.0"/>

Default Gateway IP Address*

IP Address	<input type="text" value="169.254.128.132"/>
------------	--

DNS Proxy

DNS Proxy Status	<input type="text" value="Enable"/>
------------------	-------------------------------------

* Reboot is required


Notes:

1. DHCP Server must be disabled before changing the network configurations such as IP Address, Subnet Mask, Address Type.

Figure 5-7 IP Configuration (Routing Mode)

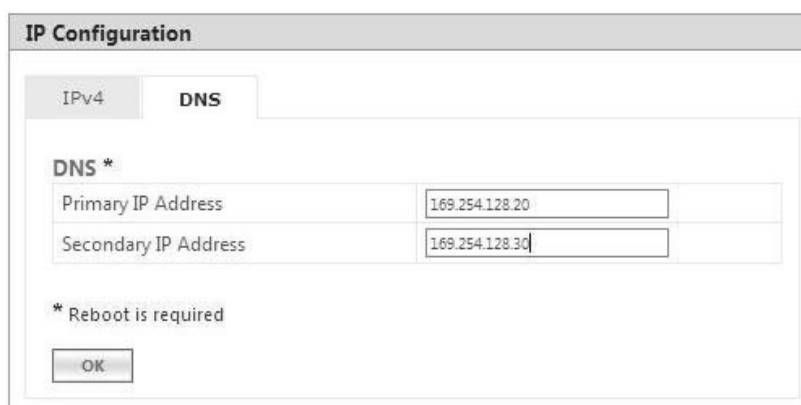
Given below is the table which explains the method to configure IP parameters in Routing mode:

Parameter	Description
Ethernet (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 for Ethernet2 it is set to 169.254.129.132. 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.
Wireless	
IP Address	Represents the IP address of the wireless interface. By default, the static IP address is set to 169.254.130.132. You can manually change the IP address.

Parameter	Description
Subnet Mask	Represents the subnet mask of the wireless interface. By default, the static subnet mask is set to 255.255.255.0. You can manually change the subnet mask.
Default Gateway IP Address	
IP Address	Represents the gateway IP address of the device. By default, the Gateway IP address is set to 169.254.128.132. You can manually change the gateway IP address.
DNS Proxy	
DNS Proxy	It is a read-only parameter, which is enabled by default. When DNS Proxy is enabled along with the DHCP server, the device will serve its own address as the Primary DNS address to the DHCP client on the Ethernet.  <ul style="list-style-type: none"> • If the DNS request from the client is destined to the device's interface address then the device acts as a DNS Proxy. • DNS Proxy is configurable through CLI/SNMP. • When DNS Proxy is disabled, you need to configure the DNS settings manually so that the end-to-end communication works properly.

5.2.1.2.1 DNS

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



IP Configuration

IPv4 **DNS**

DNS *

Primary IP Address 169.254.128.20

Secondary IP Address 169.254.128.30

* Reboot is required

OK

Figure 5-8 DNS Configuration (Routing Mode)

Parameter	Description
Primary IP Address	Represents the IP Address of the Primary DNS Server.
Secondary IP Address	Represents the IP Address of the Secondary DNS Server.



: In routing mode, the Primary and Secondary IP Address cannot be configured as IPv6 addresses.

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



- To obtain dynamic IP address of the SU over WORP,
 - **Scenario 1:** When BSU and SU are in Bridge Mode with DHCP Client enabled in SU, and if external DHCP server is running behind BSU, then SU will get the IP Address over WORP.
 - **Scenario 2:** When BSU and SU are in Bridge mode with DHCP client enabled in SU, and if BSU has an embedded DHCP server running on the wireless interface, then SU will get the IP address from BSU.
 - **Scenario 3:** When BSU is in Routing Mode and SU is in Bridge mode, and DHCP server is in a different network than SU, then configure DHCP relay in BSU to get the IP for SU over WORP.
 - **Scenario 4:** When BSU is in Routing mode and SU in Bridge mode, and if BSU has an embedded DHCP server running on the wireless interface, then SU will get the IP address from BSU.

5.2.1.3 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

IPv4

DNS

Ethernet *

INDEX	IP Address	Subnet Mask
1	<input type="text" value="169.254.128.13"/>	<input type="text" value="255.255.255.0"/>
2	<input type="text" value="169.254.129.132"/>	<input type="text" value="255.255.255.0"/>

Wireless* (PPPoE)

INDEX	IP Address	Subnet Mask	Address Type
1	<input type="text" value="169.254.130.132"/>	<input type="text" value="255.255.255.0"/>	Static <input type="button" value="v"/>

PPPoE Secondary IP*

INDEX	IP Address	Subnet Mask
1	<input type="text"/>	<input type="text" value="0.0.0.0"/>

Default Gateway IP Address*

IP Address	<input type="text" value="169.254.128.13"/>
------------	---

DNS Proxy

DNS Proxy Status	Enable
------------------	--------

* Reboot is required

Notes:


1. DHCP Server must be disabled before changing the network configurations such as *IP Address*, *Subnet Mask*, *Address Type*.
2. Only Wireless interface Address Type is configurable, and that too only when PPPoE status is enabled.

Figure 5-9 IP Configuration (Routing Mode with PPPoE Client Enabled)

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

Parameter	Description
Ethernet (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
Wireless (PPPoE)	
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 PPPoE-ipcp 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 Static.</p>
IP Address	<p>Represents the Primary IP address of the wireless interface.</p> <p>When the address type is set to PPPoE-ipcp, 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 Static, 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 PPPoE-ipcp, 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 Static, the subnet mask by default is set to 255.255.255.0. You can manually change the subnet mask.</p>
PPPoE Secondary IP	
IP Address	<p>Represents the Secondary IP address of the wireless interface.</p> <p>The Secondary IP serves as an alternate source to access/manage the device irrespective of the PPPoE link is up or down, as long as the WORP link is up. By using Secondary IP address, only management access to the device is allowed.</p> <p>Configure Secondary IP address manually. When PPPoE is disabled, the Secondary IP address is not applicable.</p>
Subnet Mask	<p>Represents the subnet mask of the Secondary IP address.</p> <p>The subnet mask by default is set to 0.0.0.0. You can manually change the subnet mask. The subnet mask of the Secondary IP address should be different from other subnets.</p>

Parameter	Description
Default Gateway IP Address	
IP Address	<p>Represents the gateway IP address of the device.</p> <p>When the address type is set to PPPoE-ipcp, 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 Static, the gateway IP address by default is set to 169.254.128.132. You can manually change the gateway IP address.</p>
DNS Proxy	
DNS Proxy	<p>It is a read-only parameter, which is enabled by default.</p> <p>When DNS Proxy is enabled along with the DHCP server, the device will serve its own address as the Primary DNS address to the DHCP client on the Ethernet.</p>  <ul style="list-style-type: none"> • If the DNS request from the client is destined to the device's interface address then the device acts as a DNS Proxy. • DNS Proxy is mostly applicable in scenarios where PPPoE Client is enabled on a device and obtains its IP addresses dynamically from the PPPoE Server; And at the same time, the device acts as a DHCP Server for a client.

5.2.1.3.1 DNS

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



Figure 5-10 DNS Configuration (Routing Mode)

Parameter	Description
Primary and Secondary IP Address	Represents the IP address of the Primary and Secondary DNS Server. Primary and Secondary IP address can be configured manually. The DNS address obtained from the PPPoE-ipcp is given preference over manually configured IP addresses.

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

5.2.2 Static Route Table



: Applicable only in routing mode.

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.

Static Route Table

Static Route Status: Disable

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 5-11 Static Route Table

Given 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.

5.2.2.1 Adding Static Route Entries

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

Static Route Table Add Row	
Destination Address	<input type="text" value="169.254.150.0"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Route Next Hop	<input type="text" value="169.254.130.101"/>
Metric	<input type="text" value="5"/> (0-16)
Entry Status	Enable <input type="button" value="v"/>
<input type="button" value="Add"/> <input type="button" value="Back"/>	

Figure 5-12 Static Route Table Add Row

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



- You can add a maximum of 256 routes 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.

5.2.3 Network Address Translation (NAT)



! : NAT is applicable only to an SU and an End Point B, in routing mode.

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	Enable <input type="button" value="v"/>	*
Dynamic Start Port	1 <input type="button" value="x"/>	(1-65535) *
Dynamic End Port	65535 <input type="button" value="x"/>	(1-65535) *
Port Forwarding Status	Disable <input type="button" value="v"/>	*

* Reboot is required

Notes:

1. To enable NAT status, RIP status must be disabled.
2. To enable NAT status, 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.

Figure 5-13 NAT

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

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 5-14 NAT Port Bind Table Add Row

Given 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: TCP , UDP , or Both .
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**.

5.2.3.1 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
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

5.2.4 RIP



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

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.

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

RIP

RIP Status: Enable

INDEX	Name	Status	Authorization Type	Authorization Key	Version Number	Direction
1	Ethernet 1	Disable	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 status, NAT status must be disabled.
2. Authorization Type & Key are valid for V2 version only.
3. If Authorization Type is "None" Authorization Key is ignored.

OK

Figure 5-15 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 Ethernet 1 , Ethernet 2 , or Wireless .
Status	Enables you to either enable or disable RIP for a particular network interface.
Authorization Type	Enables you to select the appropriate Authorization Type. This parameter is not applicable if RIP v1 is selected as the Version number .
Authorization Key	Enter the authorization key. This parameter is not applicable if RIP v1 is selected as the Version number . It is not applicable when the Authorization Type is set to None .
Version Number	Select RIP Version number from the Version Number list. Available options are V1 , V2 and both . The default is V2 .
Direction	You can enable RIP for both receiving and transmitting the data. To enable RIP only for Receiving, select Rx Only . To enable RIP for both receiving and transmitting, select Rx and Tx .

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.
- When RIP is enabled with Simple Authentication, MP 82x/8000 SUs/BSUs will not exchange RIP packets with 5012 or 5054 SUs/BSUs.

5.2.5 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**.

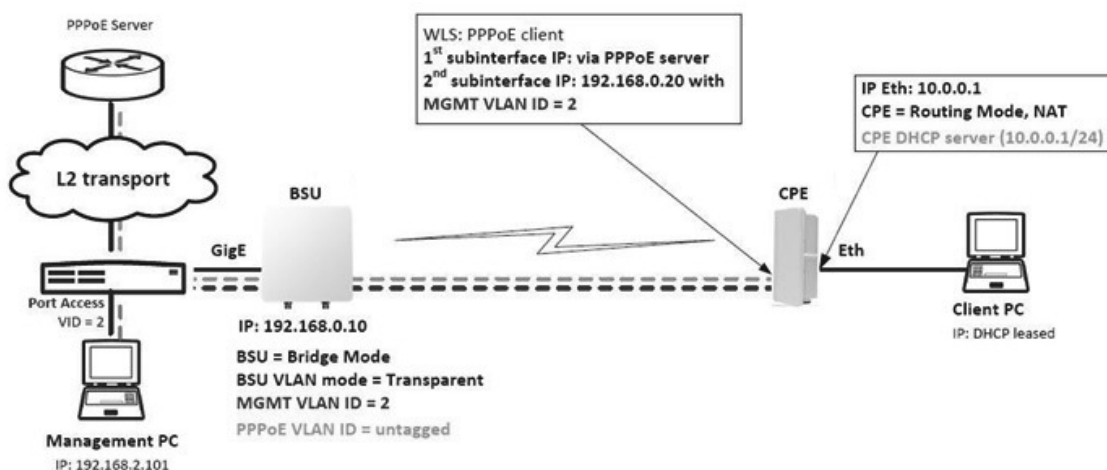


Figure 5-16 PPPoE Architecture

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:

PPPoE Client

Status: *

* Reboot is required

Notes:
1. To enable PPPoE status, NAT status must be enabled.

Figure 5-17 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	<input type="text" value="Enable"/> *
Authentication Protocol	<input type="text" value="MSCHAP v2"/>
LCP Echo Interval	<input type="text" value="30"/> (5-300) secs
LCP Echo Failure	<input type="text" value="5"/> (1-25)
Preferred Service Name	<input type="text"/> (0-32) Characters
Access Concentrator Name	<input type="text"/> (0-32) Characters
User Name	<input type="text" value="guestuser"/> (4-32) Characters
Password	<input type="password" value="*****"/> (6-32) Characters
MPPE Status	<input type="text" value="Mandatory"/>
Stateless Encryption Mode	<input type="text" value="Disable"/>
MPPE Key Length	<input type="text" value="128 Bit"/>
Link Status	<input type="text" value="Connecting..."/>


* Reboot is required




Notes:
1. To enable PPPoE status, NAT status must be enabled.
2. 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.
3. PPPoE Client Authentication Protocol is not negotiable. If PPPoE server doesn't support it, then tunnel will not established.
4. MPPE parameters are only configurable when the authentication protocol selected is MSCHAPv2.
5. 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 5-18 PPPoE Client Configuration

5. Given 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"> • None: Represents that no authentication is required for transferring PPP frames over Ethernet between PPPoE client and server. • Password Authentication Protocol (PAP): 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. • Challenge Handshake Authentication Protocol (CHAP): 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. • Microsoft Challenge-Handshake Authentication Protocol version 2 (MSCHAP v2): 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 mostly used in windows servers and client. • EAP-MD5: 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. <p>By default, the authentication protocol is set to CHAP. You can configure the authentication protocol to the desired one and click OK.</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 30 seconds.</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 User Name and Password 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	<p>: <i>MPPE Status parameter is applicable only when the Authentication Protocol is configured as "MSCHAP v2".</i></p> <p>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.</p> <p>The MPPE Status can be configured as following:</p> <ul style="list-style-type: none"> • Mandatory: When the MPPE status is configured as Mandatory, 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. • Optional: When the MPPE status is configured as Optional, 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. • Disable: When the MPPE status is configured as Disable, then the PPPoE client does not agree to the MPPE parameters suggested by the PPPoE server. <p>Configure the desired status and click OK.</p>
Stateless Encryption Mode	<p>: <i>This parameter is applicable only when Authentication Protocol is configured as "MSCHAP v2" and MPPE Status is configured as "Mandatory".</i></p> <p>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.</p> <p>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.</p> <p>To enable stateless encryption, select Enable. To enable stateful encryption, select Disable.</p> <p>: <i>Enabling Stateless Encryption impacts throughput. It is useful to enable Stateless encryption when packet drops are more in the wireless link.</i></p>

Parameter	Description
MPPE Key Length	 : This parameter is applicable only when Authentication Protocol is configured as "MSCHAP v2" and MPPE Status 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 MPPE Key Length drop-down box.
Link Status	Indicates the status of the PPPoE link between the PPPoE client and server. The link can be in any of the following three stages: <ul style="list-style-type: none"> • Disconnected: No connection is established between PPPoE client and server. • Connecting: A connection attempt is in progress between PPPoE client and server. • Connected: Connection is established between PPPoE client and server. The Link Status can be viewed in Home Page.

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

5.2.6 IP over IP Tunneling



: Applicable only in Routing Mode.

Proxim's point-to-multipoint and point-to-point devices support IP Tunneling, 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:

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

IP Packet	
Sender Source IP	Recipient IP

2. 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.

Tunneled IP Packet			
(Inner IP Header)		(Outer IP Header)	
Sender Source IP	Recipient IP	Tunnel Entry Point IP	Tunnel Exit Point IP

3. 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.

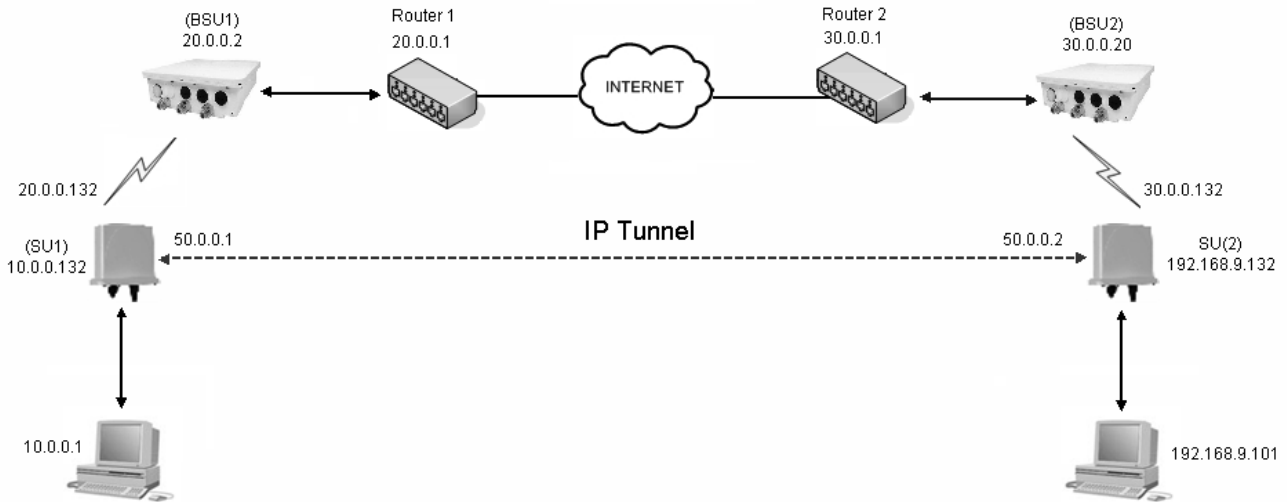


Figure 5-19 An Example: Tunnel Configuration

Lets say that the Computer with an IP address: 10.0.0.1 wants to communicate with the Computer with an IPA 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 5-19, 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

5.2.6.1 Create a Tunnel

To create a Tunnel interface,

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

Figure 5-20 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:

S.No.	Name	Encapsulation Method	Virtual IP Address	Local IP Address	Remote IP Address	TTL	Entry Status
1	Interface1	ipip	50.0.0.1	169.254.128.133	30.0.0.132	3	Enable

Figure 5-21 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	<input type="text" value="Interface2"/>
Encapsulation Method	<input style="border: none; background-color: #f0f0f0; width: 100%;" type="text" value="ipip"/>
Virtual IP Address	<input type="text" value="50.0.0.1"/>
Local IP Address	<input style="border: none; background-color: #f0f0f0; width: 100%;" type="text" value="169.254.128.133"/>
Remote IP Address	<input type="text" value="30.0.0.132"/>
TTL	<input type="text" value="3"/> (0-255)
Entry Status	<input style="border: none; background-color: #f0f0f0; width: 100%;" type="text" value="Enable"/>

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 5-22 Adding a new Tunnel Interface

6. Given 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	<p>The device supports two types of network tunnels:</p> <ul style="list-style-type: none"> • ipip: A tunneling protocol that allow only IP traffic over the tunnel. • gre (Generic Routing Encapsulation): 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. <p>Select the tunnel type as either ipip or gre.</p>
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 Time to Live . 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 Disable .

7. Next, click **Add**.



- You can create a maximum of 16 tunnels.
- 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.

5.2.6.2 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	Interface 1	ipip	50.0.0.1	169.254.128.13	30.0.0.132	3	Enable

Figure 5-23 IP Tunneling Interfaces

5.3 Ethernet

The **Ethernet** tab enables 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:


INDEX	MAC Address	Operational Speed	Operational TxMode	Speed And TxMode	Admin Status *
1	00:20:a6:12:89:34	100 Mbit	Full Duplex	Auto	Enable
2	00:20:a6:12:89:35	UnKnown	UnKnown	Auto	Enable

* Reboot is required

Figure 5-24 Basic Ethernet Configuration

Given 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>Given below is the maximum operational speed of the Ethernet interface product wise:</p> <table border="1"> <thead> <tr> <th>Product (s)</th> <th>Maximum Speed</th> </tr> </thead> <tbody> <tr> <td> <ul style="list-style-type: none"> • MP-8100-BSU • MP-8100-SUA • MP-8150-SUR • MP-8150-SUR-100 • MP-8160-BSU • MP-8160-BS9 • MP-8160-SUA • QB-8100-EPA/LNK • QB-8150-EPR/LNK • QB-8150-LNK-100 • QB-8151-EPR/LNK • MP-8200-BSU • MP-8250-BS9 • MP-8250-BS1 • MP-8200-SUA • MP-8250-SUR • QB-8200-EPA/LNK • QB-8250-EPR/LNK • MP-820-BSU-100 • MP-820-SUA-50⁺ • MP-825-SUR-50⁺ • QB-825-EPR/LNK-50⁺ </td> <td>1 Gbps</td> </tr> <tr> <td> <ul style="list-style-type: none"> • MP-825-CPE-50 • MP-8150-CPE • MP-8160-CPE-A100 • QB-8150-LNK-12/50 • QB-825-EPR/LNK-50 </td> <td>100 Mbps</td> </tr> </tbody> </table>	Product (s)	Maximum Speed	<ul style="list-style-type: none"> • MP-8100-BSU • MP-8100-SUA • MP-8150-SUR • MP-8150-SUR-100 • MP-8160-BSU • MP-8160-BS9 • MP-8160-SUA • QB-8100-EPA/LNK • QB-8150-EPR/LNK • QB-8150-LNK-100 • QB-8151-EPR/LNK • MP-8200-BSU • MP-8250-BS9 • MP-8250-BS1 • MP-8200-SUA • MP-8250-SUR • QB-8200-EPA/LNK • QB-8250-EPR/LNK • MP-820-BSU-100 • MP-820-SUA-50⁺ • MP-825-SUR-50⁺ • QB-825-EPR/LNK-50⁺ 	1 Gbps	<ul style="list-style-type: none"> • MP-825-CPE-50 • MP-8150-CPE • MP-8160-CPE-A100 • QB-8150-LNK-12/50 • QB-825-EPR/LNK-50 	100 Mbps
Product (s)	Maximum Speed						
<ul style="list-style-type: none"> • MP-8100-BSU • MP-8100-SUA • MP-8150-SUR • MP-8150-SUR-100 • MP-8160-BSU • MP-8160-BS9 • MP-8160-SUA • QB-8100-EPA/LNK • QB-8150-EPR/LNK • QB-8150-LNK-100 • QB-8151-EPR/LNK • MP-8200-BSU • MP-8250-BS9 • MP-8250-BS1 • MP-8200-SUA • MP-8250-SUR • QB-8200-EPA/LNK • QB-8250-EPR/LNK • MP-820-BSU-100 • MP-820-SUA-50⁺ • MP-825-SUR-50⁺ • QB-825-EPR/LNK-50⁺ 	1 Gbps						
<ul style="list-style-type: none"> • MP-825-CPE-50 • MP-8150-CPE • MP-8160-CPE-A100 • QB-8150-LNK-12/50 • QB-825-EPR/LNK-50 	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"> • Half Duplex: Allows one-way data transmission at a time. • Full Duplex: Allows two-way transmission simultaneously.
Speed And TxMode	Enables the user to select the speed and transmission mode of the Ethernet interface. By default, it is set to Auto . When set to Auto (recommended to set), both the transmitter and the receiver negotiate and derive at the best transmission mode. <div style="text-align: center;">  </div> <ul style="list-style-type: none"> • <i>Please ensure the same transmission modes are configured on the transmitter and the receiver device.</i> • <i>In case of 82x devices, the Auto option will support Gigabit if the other end is capable of supporting it.</i>
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 a wireless medium by using two or more parallel links and additional Link Aggregation Control Protocol (LACP) capable switches.



! : Applicable only to QB-8100-EPA/LNK, QB-8150-EPR/LNK, QB-8150-LNK-100, QB-8151-EPR/LNK, QB-8200-EPA/LNK, and QB-8250-EPR/LNK.

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

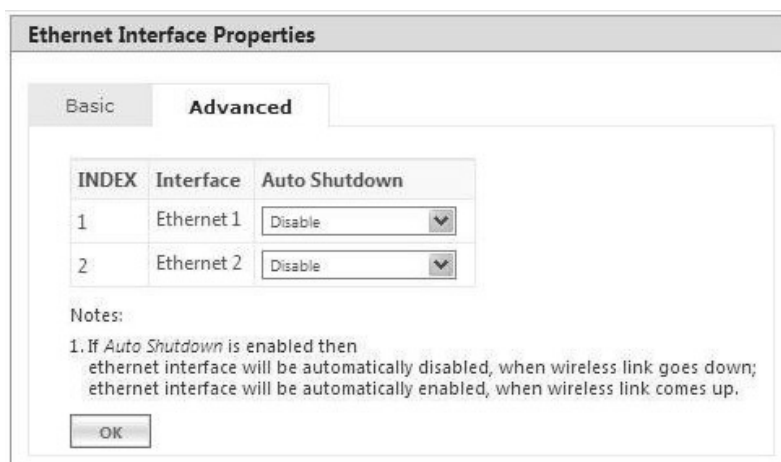




Figure 5-25 Advanced Ethernet Configuration

Given 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 or more QuickBridge links to achieve higher throughput and redundancy. By default, it is Disabled.</p> <p>If Auto Shutdown is enabled on the Ethernet Interface, then the Ethernet port will be automatically disabled, when the wireless link is DOWN. It will be automatically enabled once the wireless link is UP again.</p> <p> : This feature works only if STP/LACP Frames is set to <i>passthru</i> (See Filtering (Bridge Only))</p> <p>Tsunami® QuickBridge 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> <p> : When using second Ethernet port for management, ensure to disable <i>Auto Shutdown for Ethernet2</i>.</p> <p>For details on how to manage the QuickBridge devices through the second Ethernet port, refer LACP - Device Management.</p>

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

5.4 Wireless

The **Wireless** tab allows you to configure wireless properties (such as Network Name, Channel Bandwidth, DDRS and ATPC) on the device, which enables wireless communication between the Base Station and Subscriber, and Quick Bridges.

The features configurable under Wireless tab are as follows:

- Link Profiles

- Wireless Outdoor Router Protocol (WORP)
- Wireless Interface Properties
- Dynamic Frequency Selection (DFS) / Dynamic Channel Selection (DCS)
- Roaming
- BSU / SU Profiles

5.4.1 Link Profiles

The **Link Profiles** feature enables you to create wireless profiles on a per link basis.

These link profiles help to determine the wireless transmission properties (Tx data rate, TPC, Tx antenna ports) of a WORP link.

- On an SU, it determines the transmission properties of all the transmitted packets.
- On BSU, it determines the transmission properties of all the unicast packets.
- On BSU, it determines the transmission properties of all the broadcast/multicast and announcement packets by considering all the active link properties and active profiles. While sending broadcast messages, BSU considers the most viable wireless parameters (Tx Rate, Data Streams and TPC) so that all the connected SUs receive the message.

In point-to-multipoint (BSU and SU) devices, you can create a maximum of eight link profiles including the default pre-configured profile. Profiles that are created on the BSU are mapped to the SUs, and vice versa. If BSU/SU is not mapped to any configured profile, it will be mapped to the default profile.

The point-to-point (Quick Bridges) devices support only one link profile.



: When working with multiple link profiles with varying data rates, the overall wireless network performance gets affected. To optimize the overall network performance, use QoS.



: On upgrade from prior software versions, the WORP link configurations are copied to the Default link profile.

To create a link profile, navigate to **ADVANCED CONFIGURATION > Wireless > Link Profiles**. The **Link Profiles** screen appears:

Link Profiles			
S.No.	Profile Name	Delete	Edit
1	Default	-	
2	Subscriber1	<input type="button" value="Delete"/>	

Notes:

1. Maximum 8 entries are allowed.
2. Profile 1 is default profile, cannot be deleted.
3. Profile in use cannot be deleted.

Figure 5-26 Link Profiles

In the **Link Profiles** screen, you can add, edit and delete the link profiles.

The default profile can be modified to suit the network requirements. However, it is possible that one profile may not be able to satisfy the requirements of all the WORP links (due to different operating conditions, link distance etc). In such a case, additional link profiles can be defined and associated with respective links appropriately (refer BSU / SU Profiles on how to associate profile to a link).

It is intended that all the WORP links that are expected to exhibit similar behavior be grouped under one link profile.



- You can edit but not delete the **Default** profile.
- The link profiles in use cannot be deleted; This includes the **Roaming Link Profile** irrespective of the roaming status.
- A single profile can be mapped to multiple SUs/BSUs.
- Link profiles are local to the device and should be configured independently on all devices.

5.4.1.1 Add a Link Profile

To add a link profile, click **Add** in the **Link Profiles** screen. The **Link Profile Add Entry** screen appears:

Figure 5-27 Add a Link Profile


Type a name for the link profile in the **Profile Name** field. Next, click **ADD** and then **COMMIT**.



- By default, the link profiles are created with default values.
- After adding a link profile it must be associated with a peer (refer BSU / SU Profiles for it to be effective).

5.4.1.2 Edit a Link Profile

The link profiles are created with pre-configured wireless parameters.

In order to edit these pre-configured values for a desired profile, click **Edit** symbol  in the **Link Profiles** screen. The **Link Profile Edit Entry** screen appears, which is classified under two categories: **Basic** and **Advanced**.

Link Profile Edit Entry - 1

Basic
Advanced

Profile Name	Default
DDRS Status	Enable ▼
Data Streams	Auto ▼
DDRS Max Data Rate	MCS15 (130 Mbps) ▼
ATPC Status	Enable ▼

Antenna Status

Auto Tx Antenna Status	Disable ▼		
Tx Antenna Status	A1 <input checked="" type="checkbox"/>	A2 <input checked="" type="checkbox"/>	A3 <input type="checkbox"/>

Notes:
1.Auto Tx Antenna Status is applicable only in Single Stream Mode.



OK
Back




Figure 5-28 Edit a Link Profile (Basic)

5.4.1.2.1 Basic

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

Parameter	Description
Profile Name	Represents the link profile name whose wireless parameters are edited. Enter a new name, if you wish to edit the existing profile name.
DDRS Status	<p>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.</p> <p>The factors for adjusting the transmission data rate are,</p> <ol style="list-style-type: none"> 1. Remote average Signal-to-noise (SNR) ratio 2. Number of retransmissions <p>The DDRS Status parameter allows to either enable or disable DDRS per link profile. By default, DDRS is enabled.</p>

Parameter	Description
Data Streams	<p>Select the data stream as either Auto, Single or Dual.</p> <ul style="list-style-type: none"> • Dual Stream: Select Dual, for higher throughput. • Single Stream: Select Single, for reliability and longer range. • Auto Stream: When configured to Auto, DDRS decides the stream modes based on the environment conditions. <p>When DDRS is enabled, based on the selected data stream, DDRS dynamically chooses the data rate.</p>  <ul style="list-style-type: none"> • <i>Data Stream mode is not applicable in legacy mode.</i> • <i>When DDRS is disabled, Auto stream is not applicable.</i>
DDRS Max Data Rate	<p>Represents the maximum data rate that DDRS can dynamically choose to operate. A change in data streams resets the maximum data rate to its default value.</p>
Tx Rate	<p>This parameter enables you to manually set the transmission data rate, when DDRS is disabled. A change in data streams resets Tx rate to its default value.</p>
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"> • Equivalent Isotropically Radiated Power (EIRP) • Maximum Optimal SNR <p>In case of a BSU, when ATPC is enabled, TPC is adjusted on a per link basis.</p>  : In 820/8200 US SKUs, ATPC cannot be disabled for DFS frequencies.

Parameter	Description
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> : In case of 82x devices, you can manually set TPC ranging from 0 to 15 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 neighbouring 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 0 dBm.</p> <p> :</p> <ul style="list-style-type: none"> • Adjust TPC such that the wireless link SNR does not cross the maximum optimal SNR value (For minimum and maximum SNR values, see An Example - Local SNR Information). • 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. • TPC can be configured in the steps of 0.5 dB
Antenna Status	
Auto Tx Antenna Status	<p>Applicable only in single data stream mode.</p> <p>When Auto Tx Antenna Status is enabled for single stream, the device automatically selects the antenna port with highest received RSSI for data transmission.</p>
Tx Antenna Status	<p>Applicable only when Auto Tx Antenna Status is disabled.</p> <p>Allows the user to select the antenna port(s) for data transmission. Select the checkbox against each antenna(s) for data transmission and click OK.</p> <p> :</p> <ul style="list-style-type: none"> • On a BSU, selection of antenna ports is on a per link basis. The Tx Antenna port being used for each link can be seen on the Link Statistics page. • Atleast two Tx antenna ports should be enabled when Data Stream is dual or auto.

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

5.4.1.2.2 Advanced

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

Link Profile Edit Entry - 1

Basic **Advanced**




DDRS Min Data Rate	MCS0 (6.5 Mbps)
DDRS Max Data Rate	MCS15 (130 Mbps)
DDRS Lower SNR Correction	0 dB
DDRS Upper SNR Correction	3 dB
DDRS Rate Incr RTX Threshold	25 %
DDRS Rate Decr RTX Threshold	30 %
DDRS Chain Balance Threshold	15 dB
DDRS Rate Back Off Interval	300 secs
DDRS Rate Blacklist Interval	600 secs
DDRS Rate Stable Interval	10 secs

ATPC Upper Margin	<input type="text" value="10"/>	(0-20) dB
ATPC Lower Margin	<input type="text" value="10"/>	(0-20) dB

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

Figure 5-29 Edit a Link Profile (Advanced)

Parameter	Description
DDRS Min Data Rate and DDRS Max Data Rate	Represents the minimum and maximum data rate for DDRS to dynamically select the transmission data rate. These will vary depending on the configured data stream.
DDRS 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 0 dB .
DDRS Upper SNR Correction	Represents the margin value to be added to the maximum 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 3 dB .

Parameter	Description
DDRS Rate Incr RTX Threshold	<p>Represents a threshold for the percentage of retransmissions, below which the rate can be increased. By default, it is set to 25%.</p> <p> : If the percentage of retransmissions is between "Rate Increment RTX Threshold" and "Rate Decrement RTX Threshold" then the current operation rate is maintained.</p>
DDRS Rate Decr RTX Threshold	<p>Represents a threshold for percentage of retransmissions, above which the rate can be decreased. By default, it is set to 30%. 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.</p>
DDRS 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 15 dB.</p> <p> :</p> <ul style="list-style-type: none"> • This parameter is applicable only in Auto stream mode. • When Auto stream mode is configured and if chains are not balanced, then Single Stream rates are considered.
DDRS Rate Back Off Interval	<p>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 Rate Back Off Interval and remains at this value. By default, it is set to 300 seconds.</p>
DDRS Rate Blacklist Interval	<p>Applicable when data stream mode is set to Auto.</p> <p>DDRS algorithm dynamically determines the performance of the single and dual stream data rates independently and blacklists unviable data rates to avoid unnecessary fluctuations, for a period of DDRS Rate Blacklist Interval. By default, it is set to 600 seconds.</p> <p> : DDRS Rate Back Off Interval must be less than the DDRS Rate Blacklist Interval.</p>
DDRS Rate Stable Interval	<p>DDRS algorithm attempts higher data rates only when the current data rate is stable for a period of DDRS Rate Stable Interval. By default, it is set to 10 seconds.</p>

Parameter	Description
ATPC Upper Margin and Lower 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 SNR Initial and adjusts power only when the current SNR goes beyond the SNR Upper Limit and SNR Lower Limit.</p> <p>By default, the ATPC Lower Margin and ATPC Upper Margin is 10 dB. To configure, type a value ranging from 0 to 20 dB.</p>

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

Local SNR Information

Wireless 1

INDEX	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	13.5	9	9	50	50
2	MCS1	QPSK(1/2)	Single	27.0	10	10	50	50
3	MCS2	QPSK(3/4)	Single	40.5	14	14	50	50
4	MCS3	16QAM(1/2)	Single	54.0	16	16	50	50
5	MCS4	16QAM(3/4)	Single	81.0	20	20	50	50
6	MCS5	64QAM(2/3)	Single	108.0	24	24	50	50
7	MCS6	64QAM(3/4)	Single	121.5	27	27	50	50
8	MCS7	64QAM(5/6)	Single	135.0	29	29	50	50
9	MCS8	BPSK(1/2)	Dual	27.0	10	10	50	50
10	MCS9	QPSK(1/2)	Dual	54.0	13	13	50	50
11	MCS10	QPSK(3/4)	Dual	81.0	16	16	50	50
12	MCS11	16QAM(1/2)	Dual	108.0	20	20	50	50
13	MCS12	16QAM(3/4)	Dual	162.0	24	24	50	50
14	MCS13	64QAM(2/3)	Dual	216.0	27	27	50	50
15	MCS14	64QAM(3/4)	Dual	243.0	30	30	50	50
16	MCS15	64QAM(5/6)	Dual	270.0	33	33	50	50

Notes:

1. Minimum Required SNR values are used by remote device when *DDRS* is enabled.
2. Maximum Optimal SNR values are used by remote device when *ATPC* is enabled.

Close

Figure 5-30 An Example - SNR Information

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

5.4.2 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	MY_NETWORK (1-32) Characters
Maximum SUs	250 (1-250)
WORP MTU	3808 (350-3808) Bytes
Super Framing	Enable
Sleep Mode	Disable
Multi Frame Bursting	Enable
Auto Multi Frame Bursting	Disable
Registration Timeout	10 (1-10) Seconds
Retry Count	3 (0-10)
Input Bandwidth Limit	56320 55Mbps (64 - 102400) Kbps
Output Bandwidth Limit	56320 55Mbps (64 - 102400) Kbps
Bandwidth Limit Type	Shaping
Security Profile Name	WORP Security
RADIUS Profile Name	Default Radius
MAC ACL Status	Disable
RADIUS MAC ACL Status	Disable
Poll Backoff on Timeout	Disable
Error Count Threshold	0 (0-100) %


OK


Figure 5-31 WORP Configuration (BSU)



WORP Configuration	
Mode	SU
Active Mode	BSU
Primary BSU Name	<input type="text"/>
Secondary BSU Name	<input type="text"/>
Network Name	MY_NETWORK (1-32) Characters
WORP MTU	3808 (350-3808) Bytes
Super Framing	Enable
Registration Timeout	10 (1-10) Seconds
Retry Count	3 (0-10)
Input Bandwidth Limit	56320 55Mbps (64 - 102400) Kbps
Output Bandwidth Limit	56320 55Mbps (64 - 102400) Kbps
Bandwidth Limit Type	Shaping
Security Profile Name	WORP Security
Error Count Threshold	0 (0-100) %
RSSI Drop Threshold	0 (0-50) dB
<p>Notes:</p> <ol style="list-style-type: none"> 1. Primary BSU Name and Secondary BSU Name should be unique. 2. Primary BSU Name cannot be empty when Secondary BSU Name is configured. 3. Configuring Secondary BSU Name will enable Auto Channel Selection and disable Roaming. 	
<input type="button" value="OK"/>	




Figure 5-32 WORP Configuration (SU)




Given 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).
Primary BSU Name	<p>Applicable only to an SU.</p> <p>Represents the Primary BSU name. If the primary BSU name is configured then SU establishes link with it. If a name is not configured then SU establishes link with any BSU on the same network, which meets the registration criteria.</p> <p> : This is the system name as configured on a BSU.</p>

Parameter	Description
Secondary BSU Name	<p>This parameter serves as a Secondary / Redundant BSU for the SU and helps in reducing the network outage in the case of Primary BSU failure. This feature can help in reducing the network outage in case of the Primary BSU failure. This feature enables the SU to keep track of the Primary and the Secondary BSU availability through a proprietary protocol. This allows the SU to switch between the Primary and the Secondary BSU depending on the link status. If both the Primary and the Secondary BSU are not available, the SU attempts to find any other BSU within its network.</p> <p>This feature is activated only on a SU. By default, it is disabled. Use a non-empty string to enable this feature and an empty string to disable this feature. When this feature is enabled, it is mandatory to configure both the Primary and the Secondary BSU name on the SU. It is expected that the Primary and the Secondary BSUs are connected to the same L2 Broadcast domain and are configured with the same "Network Name" as the SU.</p>  <ul style="list-style-type: none"> • <i>The Primary and the Secondary BSU names should be unique.</i> • <i>The Secondary BSU name is the 'System Name' of the BSU used as a secondary BSU.</i> • <i>Frequency Domain, Channel Bandwidth and Channel Offset should be same for all BSUs which participate in redundancy.</i> • <i>If the BSU that participates in redundancy, operates in a channel that is blacklisted, SU will not switch.</i> • <i>An SU will switch to a BSU only when the BSU has not reached its maximum SU limit.</i> • <i>When Secondary BSU name is configured, Roaming is not applicable.</i> • <i>When Secondary BSU name is configured, Automatic Channel Selection is automatically enabled on the SU.</i>
End Point A Name	<p>Applicable only to an End Point B.</p> <p>If a name is configured for End Point A then End Point B establishes a wireless link with it. If a name is not configured then End Point B establishes link with any End Point A on the same network that meets the registration criteria.</p>
Network Name	<p>It is a unique name of given to a logical network. Devices only within this logical network can establish wireless connection.</p> <p>The Network Name can be of 1 to 32 characters in length. By default it is MY_NETWORK.</p>

Parameter	Description																
Max SUs	<p>Represents the maximum number of SUs that can register with a BSU.</p> <p>Given below are the base stations and the maximum number of subscribers supported by each of them:</p> <table border="1" data-bbox="512 539 1358 987"> <thead> <tr> <th data-bbox="512 539 901 591">Base Station</th> <th data-bbox="901 539 1358 591">Maximum Number of Subscribers</th> </tr> </thead> <tbody> <tr> <td data-bbox="512 591 901 642">MP-8100-BSU (rev 1 to rev 6)</td> <td data-bbox="901 591 1358 642">100</td> </tr> <tr> <td data-bbox="512 642 901 694">MP-8100-BSU (rev 7 and above)</td> <td data-bbox="901 642 1358 694">250</td> </tr> <tr> <td data-bbox="512 694 901 781">MP-8160-BSU MP-8160-BS9</td> <td data-bbox="901 694 1358 781">250</td> </tr> <tr> <td data-bbox="512 781 901 833">MP-8200-BSU</td> <td data-bbox="901 781 1358 833">250</td> </tr> <tr> <td data-bbox="512 833 901 884">MP-8250-BS9</td> <td data-bbox="901 833 1358 884">250</td> </tr> <tr> <td data-bbox="512 884 901 936">MP-8250-BS1</td> <td data-bbox="901 884 1358 936">250</td> </tr> <tr> <td data-bbox="512 936 901 987">MP-820-BSU-100</td> <td data-bbox="901 936 1358 987">10</td> </tr> </tbody> </table> <p> : <i>Applicable only to the BSU.</i></p>	Base Station	Maximum Number of Subscribers	MP-8100-BSU (rev 1 to rev 6)	100	MP-8100-BSU (rev 7 and above)	250	MP-8160-BSU MP-8160-BS9	250	MP-8200-BSU	250	MP-8250-BS9	250	MP-8250-BS1	250	MP-820-BSU-100	10
Base Station	Maximum Number of Subscribers																
MP-8100-BSU (rev 1 to rev 6)	100																
MP-8100-BSU (rev 7 and above)	250																
MP-8160-BSU MP-8160-BS9	250																
MP-8200-BSU	250																
MP-8250-BS9	250																
MP-8250-BS1	250																
MP-820-BSU-100	10																
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 350 to 3808 bytes for High throughput modes and 350 to 2304 bytes for legacy mode. The default and maximum value of the WORP MTU is 3808 bytes for higher throughput and 2304 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 enabled.</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 disabled.</p> <p> : <i>Applicable only to the BSU.</i></p>																

Parameter	Description
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 acknowledgment.</p> <p>By default, the Multi Frame Bursting feature is enabled 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 Quality of Service (QoS).</p> <p> : Though Multi Frame Bursting configuration is not applicable to SU/End Point B, the SU/End Point B does Multi Frame Bursting under the control of BSU/End Point A respectively.</p>
Auto Multi Frame Bursting	<p>Auto Multi Frame Bursting feature takes effect only when Multi Frame Bursting feature is enabled.</p> <p>When enabled, the device monitors all active QoS Service Flow Classes and determines the highest priority QoS Service Flow Class for all wireless connections. 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 disabled on the device.</p> <p> : Though Auto Multi Frame Bursting configuration is not applicable to SU/End Point B, the SU/End Point B does Auto Multi Frame Bursting under the control of BSU/End Point A respectively.</p>
Registration Timeout	<p>Represents the maximum time for an SU to register with the BSU or vice versa, or an End Point B to register with the 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 10 seconds.</p>
Retry Count	<p>Represents the maximum number of times the data is retransmitted by the transmitter over the wireless medium, if acknowledgment from the peer is not received. The Retry Count parameter can be configured in the range 0 to 10. By default, it is set to 3.</p>
Input Bandwidth Limit and 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> <p> : Input/Output Bandwidth throttling does not throttle broadcast/multicast traffic. These traffic can be throttled by the Maximum Information Rate (MIR) / Committed Information Rate (CIR) configured for the Downlink L2 Broadcast QoS Class in QoS Service Flow. See QoS Service Flow Configuration (SFC)</p>
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 Shaping.</p> <ul style="list-style-type: none"> • Policing: When the traffic utilization reaches the configured limit, the excess traffic will be discarded. • Shaping: When the traffic utilization reaches the configured limit, the excess traffic will be buffered and sent at the rate specified in the Output Bandwidth Limit.

Parameter	Description
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 WORP Security . See Security.
Radius Profile Name	The Radius Profile Name, containing the IP address of the RADIUS server, is used to authenticate an SU or an End Point B. See RADIUS.  : Not applicable in SU mode and End Point B mode.
MAC ACL Status	When enabled, based on the configured Access Control list (ACL), the BSU/End Point A decides if SU/End Point B can register with them respectively.  : Not applicable in SU mode and End Point B mode.
Radius MAC ACL Status	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.  : Not applicable in SU mode and End Point B mode.
Poll BackOff on Timeout	When enabled, the BSU will back-off polling the SUs that timeout (due to interference or low SNR etc). 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 a scenario to make sure that the good SUs do not suffer due to under performing SUs, it is recommended to enable this parameter. 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.
Error Count Threshold	If the error percentage of the transmitted frames is greater than or equal to the configured threshold, an SNMP trap is generated by the device. For traps, see Reference Guide available at http://my.proxim.com .
RSSI Drop Threshold	Applicable only to an SU/End Point B. If SNR, on any of the antenna ports, drops by more than or equal to the configured threshold, an SNMP trap is generated by the SU. For traps, see Reference Guide available at http://my.proxim.com .

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



- Modifying any of the WORP parameters result in temporary loss of connectivity between the transmitter and receiver.
- MAC ACL Status and RADIUS MAC ACL Status parameters cannot be enabled simultaneously.

5.4.3 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:

Wireless Interface Properties

Properties MIMO

Channel Bandwidth	20	▼	MHz *
Channel Offset	0	▼	*
Auto Channel Selection	Enable	▼	*
Active Channel	100 (5.5 GHz)		
Satellite Density	Large	▼	
Max EIRP	30		(0-100) dBm
Antenna Gain	0		(0-40) dBi
Wireless Inactivity Timer	5		(0.5-600) Seconds
Legacy Mode	Disable	▼	*

* Reboot is required

Notes:

1. Change in *Channel Bandwidth* will reset the *Max EIRP* to default.
2. *Auto Channel Selection* cannot be disabled when *Secondary BSU Name* is configured.

OK

Figure 5-33 Wireless Interface Properties (BSU)

Wireless Interface Properties

Properties MIMO

Channel Bandwidth	20	▼	MHz *
Channel Offset	0	▼	*
Auto Channel Selection	Enable	▼	
Active Channel	100 (5.5 GHz)		
Satellite Density	Large	▼	
Max EIRP	30		(0-100) dBm
Antenna Gain	0		(0-40) dBi
Wireless Inactivity Timer	5		(0.5-600) Seconds
Legacy Mode	Disable	▼	*

* Reboot is required

Notes:

1. Change in *Channel Bandwidth* will reset the *Max EIRP* to default.
2. *Auto Channel Selection* cannot be disabled when *Secondary BSU Name* is configured.

OK





Figure 5-34 Wireless Interface Properties (SU)


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

5.4.3.0.1 Properties


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

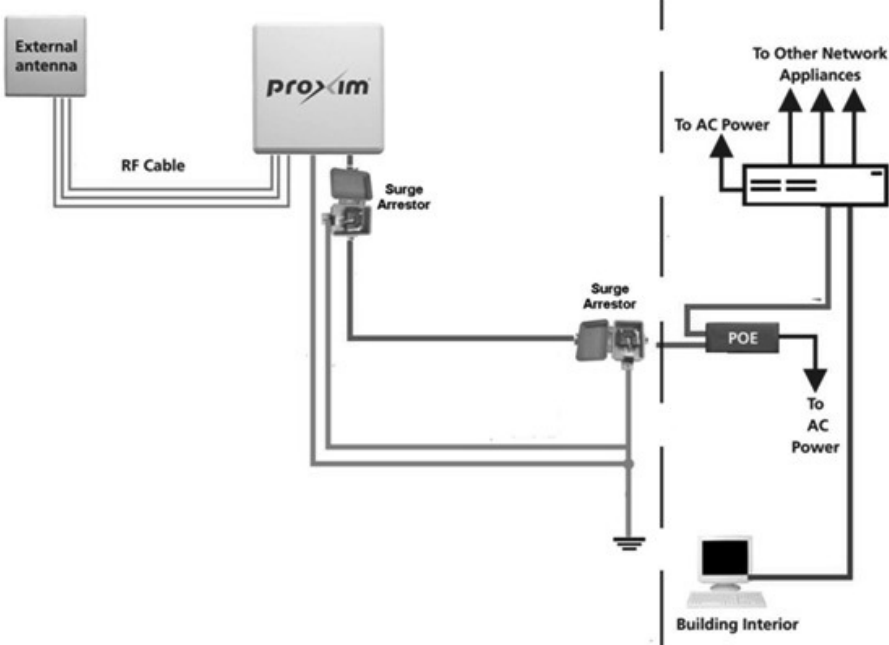
Parameter	Descriptions
Channel Bandwidth	<p>By default, the channel bandwidth is set to 20 MHz. 40 MHz can be selected for higher throughputs depending on the distance and signal quality. 5 and 10 MHz can be selected for greater flexibility in spectrum selection.</p> <div style="display: flex; align-items: flex-start;"> <ul style="list-style-type: none"> 40 MHz channel bandwidth is not applicable in Legacy mode. A change in Channel Bandwidth will reset the Tx Rate and Maximum EIRP to default value. </div> <p>For more details, see Frequency Domains and Channels.</p>

Parameter	Descriptions
Channel Offset	 : Applicable only to MP-8160-BSU; MP-8160-BS9; MP-8160-SUA; MP-8150-CPE; MP-8160-CPE-A100; MP-825-CPE-50; MP-820-BSU-100; MP-820-SUA-50 ⁺ ; MP-825-SUR-50 ⁺ ; QB-825-EPR/LNK-50 ⁺ ; QB-825-EPR/LNK-50; QB-8150-LNK-12/50 devices. 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 requirement 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. 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.  : Even though the center channel frequency is changed, the channel number still remains same, in this case 100.
Auto Channel Selection (ACS)	Auto Channel Selection (ACS) enables the device to determine the best channel for wireless data transmission with less interference. 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 the suitable BSU/End Point A and connects to it. By default, ACS is disabled on BSU/End Point A and enabled on SU/End Point B.  : On BSU/End Point A, ACS is performed only during startup.
Preferred Channel	Allows the user to select and operate in the preferred channel. 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.
Active Channel	A read-only parameter that displays the current operating channel.  : Active Channel can be different from Preferred Channel if radar interface is detected.


Parameter	Descriptions																								
Satellite Density	<p>Satellite Density setting helps to 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 Large. 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.</p> <p>Defer Threshold (CCA Threshold) parameter enables the device (BSU or SU) to establish a reliable link in high interference environments by increasing its value. This allows the device to defer the transmission as long as other interference signals in the wireless medium are greater than the configured Defer Threshold value.</p> <table border="1" data-bbox="456 1173 1426 1330"> <thead> <tr> <th>Interference Signal</th> <th>Radio Behavior</th> </tr> </thead> <tbody> <tr> <td>Greater than or equal to Defer Threshold</td> <td>Defer the transmission</td> </tr> <tr> <td>Less than Defer Threshold</td> <td>Continue the transmission</td> </tr> </tbody> </table> <p>Given below are the Sensitivity Threshold Values corresponding to various Satellite Density values:</p> <table border="1" data-bbox="528 1447 1355 1789"> <thead> <tr> <th>Satellite Density</th> <th>Receive Sensitivity Threshold</th> <th>Defer Threshold</th> </tr> </thead> <tbody> <tr> <td>Large</td> <td>-96 dB</td> <td>-62 dB</td> </tr> <tr> <td>Medium</td> <td>-86 dB</td> <td>-62 dB</td> </tr> <tr> <td>Small</td> <td>-78 dB</td> <td>-52 dB</td> </tr> <tr> <td>Mini</td> <td>-70 dB</td> <td>-42 dB</td> </tr> <tr> <td>Micro</td> <td>-62 dB</td> <td>-36 dB</td> </tr> </tbody> </table> <p> : 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.</p>	Interference Signal	Radio Behavior	Greater than or equal to Defer Threshold	Defer the transmission	Less than Defer Threshold	Continue the transmission	Satellite Density	Receive Sensitivity Threshold	Defer Threshold	Large	-96 dB	-62 dB	Medium	-86 dB	-62 dB	Small	-78 dB	-52 dB	Mini	-70 dB	-42 dB	Micro	-62 dB	-36 dB
Interference Signal	Radio Behavior																								
Greater than or equal to Defer Threshold	Defer the transmission																								
Less than Defer Threshold	Continue the transmission																								
Satellite Density	Receive Sensitivity Threshold	Defer Threshold																							
Large	-96 dB	-62 dB																							
Medium	-86 dB	-62 dB																							
Small	-78 dB	-52 dB																							
Mini	-70 dB	-42 dB																							
Micro	-62 dB	-36 dB																							

Parameter	Descriptions																																																																											
Max EIRP	<p>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.</p> <p>Given below are the default maximum EIRP values that are set according to regulatory domain:</p> <table border="1" data-bbox="488 622 1390 1895"> <thead> <tr> <th data-bbox="488 622 679 719" rowspan="2">Regulatory Domain</th> <th data-bbox="679 622 874 719" rowspan="2">Frequency (MHz)</th> <th colspan="2" data-bbox="874 622 1390 667">Max EIRP (dBm)</th> </tr> <tr> <th data-bbox="874 667 1129 719">PTP Mode (QB)</th> <th data-bbox="1129 667 1390 719">PTMP Mode (MP)</th> </tr> </thead> <tbody> <tr> <td data-bbox="488 719 679 763">World</td> <td data-bbox="679 719 874 763">All</td> <td data-bbox="874 719 1129 763">Unlimited (100)</td> <td data-bbox="1129 719 1390 763">Unlimited (100)</td> </tr> <tr> <td data-bbox="488 763 679 1173" rowspan="7">United States</td> <td data-bbox="679 763 874 875">2402-2472</td> <td data-bbox="874 763 1129 875">32 + 2/3(antenna gain)</td> <td data-bbox="1129 763 1390 875">BSU: 36 SU/CPE: 32 + 2/3 (antenna gain)</td> </tr> <tr> <td data-bbox="679 875 874 987">4940 – 4990</td> <td data-bbox="874 875 1129 987">33 (20 MHz) 30 (10 MHz) 27 (5 MHz)</td> <td data-bbox="1129 875 1390 987">33 (20 MHz) 30 (10 MHz) 27 (5 MHz)</td> </tr> <tr> <td data-bbox="679 987 874 1032">5250 – 5330</td> <td data-bbox="874 987 1129 1032">30</td> <td data-bbox="1129 987 1390 1032">30</td> </tr> <tr> <td data-bbox="679 1032 874 1077">5490 – 5590</td> <td data-bbox="874 1032 1129 1077">30</td> <td data-bbox="1129 1032 1390 1077">30</td> </tr> <tr> <td data-bbox="679 1077 874 1122">5650 – 5710</td> <td data-bbox="874 1077 1129 1122">30</td> <td data-bbox="1129 1077 1390 1122">30</td> </tr> <tr> <td data-bbox="679 1122 874 1167">5730 - 5860</td> <td data-bbox="874 1122 1129 1167">53</td> <td data-bbox="1129 1122 1390 1167">36</td> </tr> <tr> <td data-bbox="488 1173 679 1473" rowspan="5">Canada</td> <td data-bbox="679 1173 874 1285">4940 – 4990</td> <td data-bbox="874 1173 1129 1285">33 (20 MHz) 30 (10 MHz) 27 (5 MHz)</td> <td data-bbox="1129 1173 1390 1285">33 (20 MHz) 30 (10 MHz) 27 (5 MHz)</td> </tr> <tr> <td data-bbox="679 1285 874 1330">5250 – 5330</td> <td data-bbox="874 1285 1129 1330">30</td> <td data-bbox="1129 1285 1390 1330">30</td> </tr> <tr> <td data-bbox="679 1330 874 1375">5490 – 5590</td> <td data-bbox="874 1330 1129 1375">30</td> <td data-bbox="1129 1330 1390 1375">30</td> </tr> <tr> <td data-bbox="679 1375 874 1420">5650 – 5710</td> <td data-bbox="874 1375 1129 1420">30</td> <td data-bbox="1129 1375 1390 1420">30</td> </tr> <tr> <td data-bbox="679 1420 874 1473">5730 - 5860</td> <td data-bbox="874 1420 1129 1473">53</td> <td data-bbox="1129 1420 1390 1473">36</td> </tr> <tr> <td data-bbox="488 1473 679 1659" rowspan="4">Europe (including UK)</td> <td data-bbox="679 1473 874 1518">2402 – 2472</td> <td data-bbox="874 1473 1129 1518">20</td> <td data-bbox="1129 1473 1390 1518">20</td> </tr> <tr> <td data-bbox="679 1518 874 1563">5490 – 5590</td> <td data-bbox="874 1518 1129 1563">30</td> <td data-bbox="1129 1518 1390 1563">30</td> </tr> <tr> <td data-bbox="679 1563 874 1608">5650 – 5710</td> <td data-bbox="874 1563 1129 1608">30</td> <td data-bbox="1129 1563 1390 1608">30</td> </tr> <tr> <td data-bbox="679 1608 874 1659">5735 – 5875</td> <td data-bbox="874 1608 1129 1659">36</td> <td data-bbox="1129 1608 1390 1659">36</td> </tr> <tr> <td data-bbox="488 1659 679 1800" rowspan="3">Russia</td> <td data-bbox="679 1659 874 1704">5150 – 5350</td> <td data-bbox="874 1659 1129 1704">33</td> <td data-bbox="1129 1659 1390 1704">33</td> </tr> <tr> <td data-bbox="679 1704 874 1749">5350 – 5650</td> <td data-bbox="874 1704 1129 1749">Unlimited (100)</td> <td data-bbox="1129 1704 1390 1749">Unlimited (100)</td> </tr> <tr> <td data-bbox="679 1749 874 1800">5650 – 6425</td> <td data-bbox="874 1749 1129 1800">53</td> <td data-bbox="1129 1749 1390 1800">53</td> </tr> <tr> <td data-bbox="488 1800 679 1895" rowspan="2">Taiwan</td> <td data-bbox="679 1800 874 1845">5490 – 5710</td> <td data-bbox="874 1800 1129 1845">30</td> <td data-bbox="1129 1800 1390 1845">30</td> </tr> <tr> <td data-bbox="679 1845 874 1895">5735 – 5835</td> <td data-bbox="874 1845 1129 1895">36</td> <td data-bbox="1129 1845 1390 1895">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	5490 – 5590	30	30	5650 – 5710	30	30	5730 - 5860	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																																																																									
	5490 – 5590	30	30																																																																									
	5650 – 5710	30	30																																																																									
	5730 - 5860	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				
	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
		<ul style="list-style-type: none"> • If the maximum EIRP is not defined in the above table then it is set to 100 (unlimited EIRP). • Maximum EIRP criterion is enforced only when ATPC is enabled. • For DFS bands (5.25-5.725 GHz), the EIRP limit is 23 dBm for the Subscriber units if DFS is not activated. • Operation is not allowed in 5.600 - 5.650 GHz in USA, Canada, Australia and European Countries. 			

Parameter	Descriptions
<p>Antenna Gain</p>	<p>When using external antenna, the professional installer should ensure to configure proper antenna gain so that the radio does not exceed the EIRP allowed per regulatory domain.</p>  <p>Calculate the antenna gain as follows:</p> <p>Antenna Gain to be configured = Antenna Gain of the antenna used - Cable Loss</p> <p>Example: Consider an example where the device is operating in United States 5.3 GHz with the EIRP 30 dBm. The antenna gain of the antenna used is 23 dBi and the cable loss is 1dB.</p> <p>Given this case, Configurable Antenna Gain = [23 dBi – 1 dB] = 22 dBi</p> <p>Maximum Radio Power = EIRP – Configured Antenna Gain = 30 dBm – 22 dBi = 8 dBm</p> <p>With this configuration, the ATPC feature will limit the radio power to a maximum of 8 dBm to avoid exceeding EIRP limit of 30 dBm.</p>

Parameter	Descriptions																		
	<p>Improper configuration of Antenna Gain will affect the sensitivity of the radio card. As the radar detection threshold is fixed by ETSI, the FCC and IC, any change in sensitivity of the radio card will result in false radar detections or actual radar signal not being detected. If the configured antenna gain is higher than the actual antenna gain, Radar signals may go undetected. If the configured antenna gain is lower than the actual antenna gain, False Radar may be detected.</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>Given below are the default Antenna Gain, for devices with integrated antenna:</p> <table border="1" data-bbox="592 790 1299 1561"> <thead> <tr> <th data-bbox="592 790 1023 842">Product (s)</th> <th data-bbox="1023 790 1299 842">Antenna Gain</th> </tr> </thead> <tbody> <tr> <td data-bbox="592 842 1023 965">MP-8150-SUR MP-8250-SUR MP-8250-BS1</td> <td data-bbox="1023 842 1299 965">23 dBi</td> </tr> <tr> <td data-bbox="592 965 1023 1016">MP-8150-SUR-100</td> <td data-bbox="1023 965 1299 1016">21 dBi</td> </tr> <tr> <td data-bbox="592 1016 1023 1140">MP-8150-CPE MP-8160-BS9 MP-8250-BS9</td> <td data-bbox="1023 1016 1299 1140">16 dBi</td> </tr> <tr> <td data-bbox="592 1140 1023 1263">MP-825-SUR-50+ MP-825-CPE-50 MP-8160-CPE-A100</td> <td data-bbox="1023 1140 1299 1263">15 dBi</td> </tr> <tr> <td data-bbox="592 1263 1023 1346">QB-8150-EPR/LNK QB-8250-EPR/LNK</td> <td data-bbox="1023 1263 1299 1346">23 dBi</td> </tr> <tr> <td data-bbox="592 1346 1023 1429">QB-8150-LNK-100 QB-8151-EPR/LNK</td> <td data-bbox="1023 1346 1299 1429">21 dBi</td> </tr> <tr> <td data-bbox="592 1429 1023 1480">QB-8150-LNK-12/50</td> <td data-bbox="1023 1429 1299 1480">16 dBi</td> </tr> <tr> <td data-bbox="592 1480 1023 1561">QB-825-EPR/LNK-50 QB-825-EPR/LNK-50+</td> <td data-bbox="1023 1480 1299 1561">15 dBi</td> </tr> </tbody> </table>	Product (s)	Antenna Gain	MP-8150-SUR MP-8250-SUR MP-8250-BS1	23 dBi	MP-8150-SUR-100	21 dBi	MP-8150-CPE MP-8160-BS9 MP-8250-BS9	16 dBi	MP-825-SUR-50+ MP-825-CPE-50 MP-8160-CPE-A100	15 dBi	QB-8150-EPR/LNK QB-8250-EPR/LNK	23 dBi	QB-8150-LNK-100 QB-8151-EPR/LNK	21 dBi	QB-8150-LNK-12/50	16 dBi	QB-825-EPR/LNK-50 QB-825-EPR/LNK-50+	15 dBi
Product (s)	Antenna Gain																		
MP-8150-SUR MP-8250-SUR MP-8250-BS1	23 dBi																		
MP-8150-SUR-100	21 dBi																		
MP-8150-CPE MP-8160-BS9 MP-8250-BS9	16 dBi																		
MP-825-SUR-50+ MP-825-CPE-50 MP-8160-CPE-A100	15 dBi																		
QB-8150-EPR/LNK QB-8250-EPR/LNK	23 dBi																		
QB-8150-LNK-100 QB-8151-EPR/LNK	21 dBi																		
QB-8150-LNK-12/50	16 dBi																		
QB-825-EPR/LNK-50 QB-825-EPR/LNK-50+	15 dBi																		
Wireless Inactivity Timer	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 5 seconds (disabled if set to 0 seconds) and can be configured between 5 to 600 seconds.																		

Parameter	Descriptions
Legacy Mode	<p>By default, Legacy Mode is disabled. When enabled, the MP 800 & 8000 BSU and SU devices can interoperate with the legacy products of the Tsunami® MP.11 family.</p> <p>The MP 800 & 8000 devices that provide legacy support are,</p> <ul style="list-style-type: none"> • MP-8100-BSU • MP-8100-SUA • MP-8150-SUR • MP-8150-CPE • MP-8150-SUR-100 • MP-8200-BSU • MP-8250-BS9 • MP-8250-BS1 • MP-8200-SUA • MP-8250-SUR • MP-825-CPE-50 • MP-825-SUR-50⁺ • MP-820-BSU-100 • MP-820-SUA-50⁺ <p> : MP 800/8000 BSU device in legacy mode can connect to a MP 800/8000 SU device only when configured in legacy mode.</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 an asterisk (*) symbol.

5.4.3.0.2 MIMO

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

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

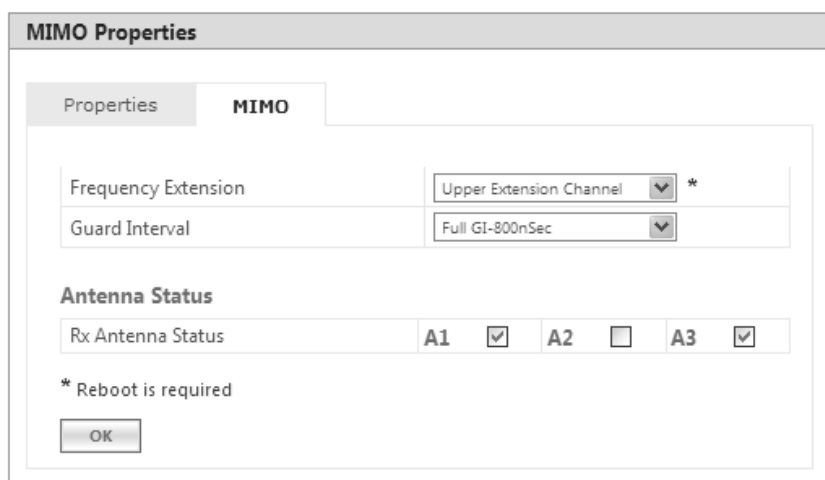




Figure 5-35 MIMO

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 throughput.</p> <p>By default, Full GI is enabled for 5 MHz, 10 MHz and 20 MHz channels.</p> <p>:</p> <ul style="list-style-type: none"> • Short GI-400 nSec is valid only for 40 MHz channel bandwidth • Short GI-400 nSec is not valid for 82x devices.
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>: At least two Rx antenna ports should be enabled when data stream is dual or auto.</p>

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

Reboot the device, if you have changed any of the MIMO parameters with an asterisk (*) symbol.

5.4.4 Dynamic Frequency Selection (DFS) / Dynamic Channel Selection (DCS)

5.4.4.1 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 to MP-8160-BSU, MP-8160-BS9, MP-8160-SUA, MP-8160-CPE devices.

5.4.4.1.1 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 Automatic Channel Selection (ACS) is disabled on the device, the device chooses the Preferred Channel to be the operational channel.



By default, ACS is disabled on the BSU or End Point A device.

- 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 list 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 is blacklisted earlier.
- Even if the preferred channel is configured with a DFS channel manually, the SU will scan for the BSU/End Point A's channel and associates automatically.

5.4.4.1.2 DFS in SU or End Point B Mode

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

1. When SU/End Point B has no WORP 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 WORP 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 WORP 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 will 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.

5.4.4.2 Dynamic Channel Selection (DCS)



DCS is applicable to a BSU or End Point A only.

Dynamic Channel Selection feature enables you to monitor the link quality (retransmissions due to interference) on the operating channel. If the link quality is found to be below the threshold, then the device stops transmitting on that channel and switches to another channel, among the available channels.

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

- Enable DCS. By default, it is in disabled state.
- When DCS is enabled, the device computes the percentage of retransmissions (due to interference) for each link:

- If the link quality is bad, the channel is blacklisted for 30 minutes. ACS will scan all the non-blacklisted channels and selects the channel with good link quality (least interference).
- If the link quality is above the threshold, the device continues to operate in the same channel.
- Periodically, the device monitors the current operating channel for link quality. If the link quality is found to be below the threshold, the device stops transmitting in that channel and the channel is blacklisted.
- A channel in the blacklisted list is purged once the Non Occupancy Period (NOP) has elapsed for that channel.
- The BSU switches to the preferred channel once it is de-blacklisted.



- *If DCS is enabled in BSU, ensure that ACS is enabled in SU.*
- *When DCS is enabled, Spectrum Analyzer scan cannot be performed.*

To configure **DCS** parameters, navigate to **ADVANCED CONFIGURATION > Wireless > Interface 1 > DFS/DCS**. The **DFS / DCS/ Manual Blacklist Configuration** screen appears.

DFS / DCS / Manual Blacklist Configuration

DFS / DCS
Manual Blacklist

Dynamic Frequency Selection

Channel Wait Time	60	(60-3600) Seconds
SUs Reporting RADAR	0	(0-250)

Dynamic Channel Selection

Dynamic Channel Selection	Enable	▼
Retransmission Threshold	1	(1-100) %
Bad Link Threshold	1	(1-250)

Notes:

1.If *Dynamic Channel Selection (DCS)* is enabled in BSU, ensure that *Auto Channel Selection (ACS)* is enabled in SU.

Blacklist Information

Channel Number	Reason	Time Elapsed (Minutes)
100 (5.5 GHz)	Interference	3
101 (5.505 GHz)	Interference	3
102 (5.51 GHz)	Unusable	3
103 (5.515 GHz)	Unusable	3
107 (5.535 GHz)	Unusable	0
108 (5.54 GHz)	Unusable	0
109 (5.545 GHz)	Manual	0
110 (5.55 GHz)	Unusable	0
111 (5.555 GHz)	Unusable	0

Figure 5-36 DFS Configuration (BSU Mode)

DFS / Manual Blacklist Configuration

DFS Manual Blacklist

Dynamic Frequency Selection

Channel Wait Time: (60-3600) Seconds

DFS Status:

Blacklist Information

Channel Number	Reason	Time Elapsed (Minutes)
132 (5.66 GHz)	Local Radar	12
133 (5.665 GHz)	Local Radar	12
134 (5.67 GHz)	Unusable	12
135 (5.675 GHz)	Unusable	12

Figure 5-37 DFS Configuration (SU/End Point B Mode)

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

Parameter	Description
Dynamic Frequency Selection	
Channel Wait Time	Once 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 60 to 3600 seconds. By default, the wait time is set to 60 seconds .
SUs Reporting RADAR	Applicable only to BSU. When an SU detects a RADAR, it reports to BSU. The BSU will take a decision on whether to blacklist this channel based on SUs Reporting RADAR 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 0 .
DFS Status	Applicable only to SU or End Point B devices. An SU or End Point B device can either enable or disable DFS. By default, DFS is disabled.
Dynamic Channel Selection	
Dynamic Channel Selection	This parameter is used to enable DCS on the device. By default, DCS is disabled. To enable, select Enable and Click OK .

Parameter	Description
Retransmission Threshold	<p>This parameter enables to configure the retransmission threshold percentage on the device. The device computes percentage of retransmission for each link and compares with the configured threshold. If the retransmission percentage is greater than the user configured retransmission threshold, the link is considered as bad link.</p> <p>By default, the retransmission percentage is set to 50.</p>
Bad Link Threshold	<p>Applicable only to BSU.</p> <p>The BSU decides to blacklist the operating channel based on Bad Link Threshold parameter. If the number of Bad Links (Between BSU and SU) equals or exceeds the configured Bad Link Threshold parameter then the channel is blacklisted. Else, it continues to operate in the same channel.</p> <p>By default, Bad Link Threshold value is set to 1.</p>

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"> 1. Remote Radar: An SU/End Point B detects radar and informs BSU/End Point A respectively. 2. Local Radar: The device detects the radar on its own. 3. Interference: BSU detects interference based on the retransmission threshold. 4. Unusable: 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. 5. Manual: A channel is manually blacklisted by the administrator.
Time Elapsed	<p>The time elapsed since the channel was blacklisted due to radar and interference. When the channel is blacklisted due to the presence of radar and interference, it will be blacklisted again after 30 minutes.</p> <p>This parameter is applicable for radar and interference blacklisted channels only.</p>

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

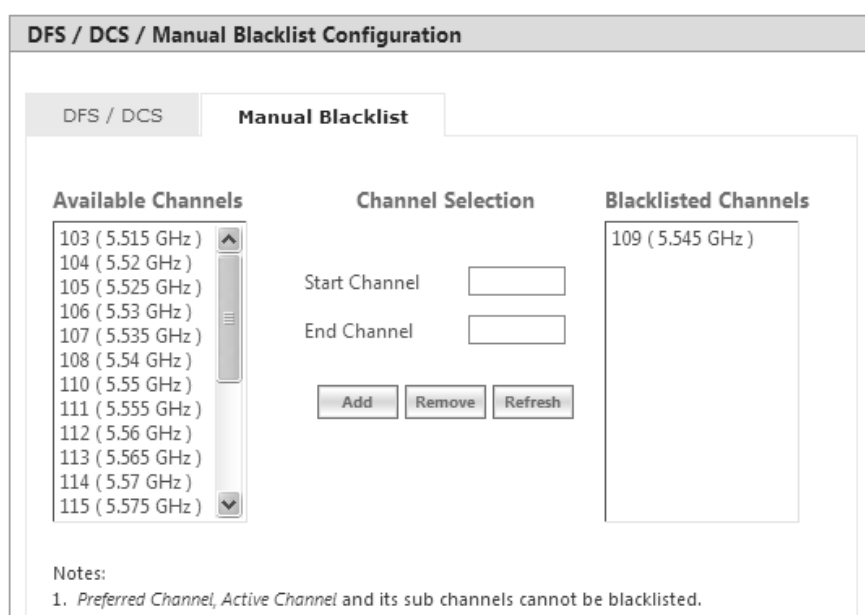
5.4.4.4 Manual Blacklist

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 manually blacklisted.
- When WORP link is UP, the active channel and its sub-channels that are part of the current channel bandwidth cannot be manually 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 manually blacklist channels, click **Manual Blacklist** in the **Dynamic Frequency Selection (DFS)** screen. The following screen appears:



DFS / DCS / Manual Blacklist Configuration

DFS / DCS **Manual Blacklist**

Available Channels	Channel Selection	Blacklisted Channels
103 (5.515 GHz)	Start Channel <input type="text"/>	109 (5.545 GHz)
104 (5.52 GHz)	End Channel <input type="text"/>	
105 (5.525 GHz)	<input type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="Refresh"/>	
106 (5.53 GHz)		
107 (5.535 GHz)		
108 (5.54 GHz)		
110 (5.55 GHz)		
111 (5.555 GHz)		
112 (5.56 GHz)		
113 (5.565 GHz)		
114 (5.57 GHz)		
115 (5.575 GHz)		

Notes:
1. Preferred Channel, Active Channel and its sub channels cannot be blacklisted.

Figure 5-38 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 Roaming

The Roaming feature enables a mobile SU to provide seamless network services by constantly monitoring the quality of the wireless link with the current associated BSU. The SU uses the link quality parameters such as local SNR values and Rx modulation rates to calculate the Rx SNR for each BSU. If the calculated Rx SNR is lower than or equal to the configured SNR threshold, then the SU roams.



: Roaming feature is applicable only to the point-to-multipoint devices but not applicable in legacy mode.

5.4.5.1 Definition(s)

- **Roaming Preferred Channels:** A list of channels maintained by a BSU where its neighbour BSUs are operating.
- **Roaming Channel List (RCL):** A list of channels that are learnt from the associated BSU (known as Roaming Preferred Channels), and are not blacklisted locally on the SU. An SU uses this channel list to scan BSUs while roaming.
- **Usable Channel List (UCL):** A list of channels that are available to an SU for the configured frequency domain and are not blacklisted.



: Manual Blacklisting can be used to reduce the number of channels in the UCL and there by reducing the scanning and roaming time.

5.4.5.2 Roaming Types

5.4.5.2.1 Slow Roaming

When the calculated Rx SNR, for the current link, goes lower than or equal to the configured Slow Roam Rx SNR Threshold, then SU starts Slow Roaming.

During Slow Roaming, the SU scans channels from the RCL, one at a time. After scanning a channel, it returns back to the channel where the current BSU operates, resumes data transfer and then jumps to another channel in the RCL, and so forth until it scans all the channels. Once the scanning completes, the SU calculates the Rx SNR for each BSU and finds the BSU with the highest Rx SNR value. If the BSU is better than the current BSU, then the SU roams to that BSU.

5.4.5.2.2 Fast Roaming

When the calculated Rx SNR, for the current link, goes lower than or equal to the configured Fast Roam Rx SNR Threshold, then SU starts Fast Roaming.

During Fast Roaming, the SU starts scanning all the channels in the RCL until it finds a BSU with better Rx SNR than the current BSU. Once it finds such BSU, the SU roams to that BSU and does not scan any more channels.

If the SU does not find a BSU with better Rx SNR, in any of the channels in the RCL, it resumes operation with the current BSU.

If the quality of the link with the current BSU is still such that Fast Roaming procedure has to be started again, SU starts scanning channels from the UCL, instead of the RCL, until it find a BSU with better Rx SNR. Once the whole list is scanned, and no better BSU is found, SU resumes operation with the current BSU. SU repeats this procedure until either link quality improves, or a BSU with better Rx SNR is found.

5.4.5.2.3 Emergency Roaming

An SU starts Emergency Roaming when the wireless link with the current associated BSU is lost for at least 1000 milliseconds.

During Emergency Roaming, the SU scans all the channels in the RCL until it finds any BSU. If the whole RCL is scanned and no BSU is found, then SU starts scanning the channels from the beginning of the UCL, instead of the RCL. The SU keeps scanning the channels from the UCL until any BSU is found. When a BSU is found, SU roams to that BSU.



: There is a possibility that the new BSU may not be better than the previous BSU.

5.4.5.3 Configurable Parameters on a BSU


To configure the roaming parameters on a BSU, navigate to **ADVANCED CONFIGURATION > Wireless > Interface 1 > Roaming**. The **Roaming Configuration** screen appears:



The screenshot shows two instances of the 'Roaming Configuration' screen. The top instance shows 'Roaming Status' set to 'Disable' with an 'OK' button. The bottom instance shows 'Roaming Status' set to 'Enable', 'Roaming Link Profile' set to 'Default', 'Announce Period' set to '25 (25-100) ms', and 'Max. Packets Per Burst' set to '4 (1-16)'. Below this is a table for 'Roaming Preferred Channels' with one entry: INDEX 1, Channel 100 (5.5 GHz), and Entry Status Enable. There are 'OK' and 'Add' buttons at the bottom.

INDEX	Channel	Entry Status
1	100 (5.5 GHz)	Enable

Figure 5-39 BSU Roaming Configuration

Below is the table which explains roaming parameters for a BSU, and the method to configure the configurable parameter(s):

Parameter	Description
Roaming Status	<p>The Roaming feature can either be enabled or disabled on a BSU. By default, it is disabled.</p> <p>When the roaming status is enabled on a BSU, the other roaming parameters such as Roaming Link Profile, Announce Period, Maximum Packets Per Burst and Roaming Preferred Channels are configurable. These parameters are used by the registered SU when any of the roaming procedure starts.</p> <p> : Roaming can be enabled on the BSU, independent of the roaming status of the SU.</p>

Parameter	Description
Roaming Link Profile	<p>This parameter enables you to configure a roaming link profile for the roaming enabled SUs.</p> <p>When roaming is enabled on the BSU, select a profile from the configured link profiles, which serves as the roaming profile. The Default profile serves as the roaming profile when no profile is selected. The configured roaming profile is mapped to all the roaming enabled SUs. For the SUs with roaming disabled, the profile configured in the SU profiles list will be used.</p> <p>When roaming is disabled on the BSU, the SUs are mapped to the corresponding profile from the SU Profiles list.</p>
Announce Period	<p>When roaming is enabled on a BSU, the BSU sends ANNOUNCE messages for every configured Announce period. The Announce period can be configured in the range 25 to 100 milliseconds. By default, it is configured to 25 milliseconds.</p> <p>When roaming is disabled on a BSU, the Announce period is set to 150 milliseconds.</p> <p> : Reducing the Announce Period improves the roaming time and may result in lower throughput.</p>
Max. Packets Per Burst	<p>When roaming is enabled on a BSU, the maximum number of messages that can be sent in a burst can be configured in the range 1 to 16.</p> <p>When roaming is disabled on a BSU, the maximum packets per burst is set to 4.</p> <p> :</p> <ul style="list-style-type: none"> • Reducing the number of messages per burst improves the roaming time and may result in lower throughput. • If the maximum packets per burst configured in QoS (See Adding a New Service Flow (SFC)) is greater than this value, then this parameter supersedes.

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

Parameter	Description
<p>Roaming Preferred Channels</p>	<p>Each BSU on the network, maintains a list of channels where its neighbour BSUs are operating. When roaming is enabled, SU learns this list from the current BSU and uses it as Roaming Channel List (RCL), to reduce scanning time while searching for a BSU with better Rx SNR.</p> <p>To add channels, click Add under Roaming Preferred Channels. The Roaming Channel Add Entry screen appears:</p> <div data-bbox="635 584 1254 786" data-label="Form"> </div> <p style="text-align: center;">Figure 5-40 Add Channels to the Roaming Table</p> <p>Do the following:</p> <ul style="list-style-type: none"> • Channel: Select the channel of the neighbouring BSU, where the SU is likely to roam. • Entry Status: If the entry status is enabled, then this channel is allowed to be scanned by a roaming SU. • Next, click Add. <div data-bbox="651 1088 1241 1603" data-label="Form"> </div> <p style="text-align: center;">Figure 5-41 Channels Added to the Roaming Table</p> <p>At any point of time, the channels and their corresponding entry status can be edited. You can change the entry status to either,</p> <ul style="list-style-type: none"> • Enable: Allows a roaming SU to scan a channel. • Disable: Does not allow a roaming SU to scan a channel. • Delete: Allows to delete a channel from the table. <p>Click OK and then COMMIT, if the table entries are re-configured.</p> <div data-bbox="456 1912 523 1989" data-label="Image"> </div> <p>: A maximum of five channels can be added to the Roaming Preferred Channels Table.</p>

5.4.5.4 Configurable Parameters on an SU

To configure the roaming parameters on an SU, navigate to **ADVANCED CONFIGURATION > Wireless > Interface 1 > Roaming**. The **Roaming Configuration** screen appears:

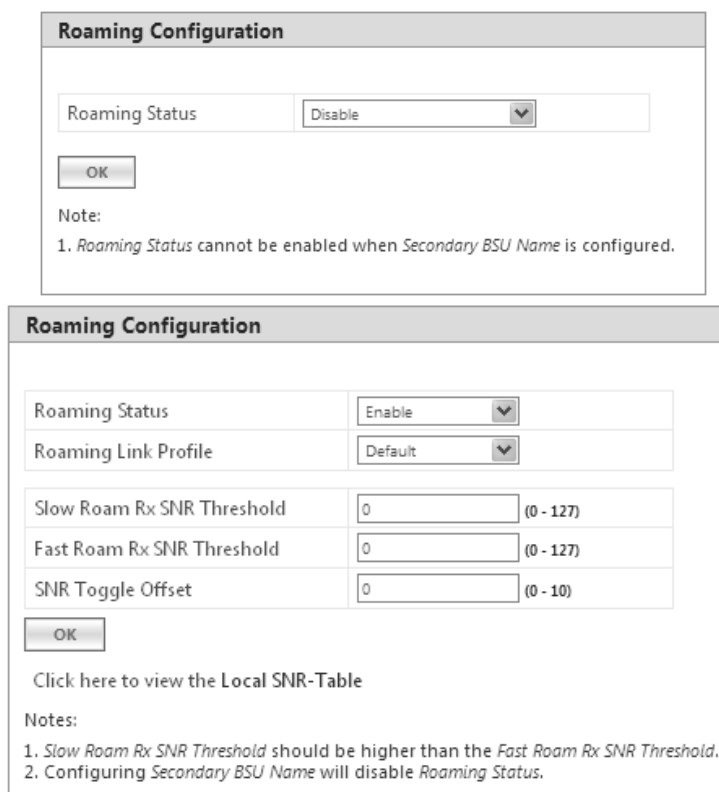



Figure 5-42 SU Roaming Configuration

Below is the table which explains roaming parameters for an SU, and the method to configure the configurable parameter(s):

Parameter	Description
Roaming Status	<p>By default, roaming status is disabled. Only when enabled, an SU can roam to a better BSU.</p> <p> : Roaming on the SU can be enabled independent of the roaming status on the BSU.</p> <p>The roaming parameters such as Rx SNR Thresholds for Slow and Fast Roaming are configurable only when the roaming status is enabled.</p>

Parameter	Description
Roaming Link Profile	<p>This parameter enables you to configure a roaming link profile for the roaming enabled BSU.</p> <p>When roaming is enabled on the SU, select a profile from the configured link profiles, which serves as the roaming profile. The Default profile serves as the roaming profile when no profile is selected. The configured roaming profile is mapped to the roaming enabled BSU. For the BSU with roaming disabled, the profile configured in the BSU Profiles list will be used.</p> <p>When roaming is disabled on the SU, the BSU is mapped to the corresponding profile from the BSU Profiles list.</p>
Slow Rx SNR Threshold	<p>When the calculated Rx SNR, for the current link, goes lower than or equal to the configured Rx Slow Roaming SNR Threshold, then SU starts Slow Roaming.</p> <p>The default threshold value is set to 0. To configure, enter a desired threshold value ranging from 0 - 127.</p>
Fast Rx SNR Threshold	<p>When the calculated Rx SNR, for the current link, goes lower than or equal to the configured Rx Fast Roaming SNR Threshold, then SU starts Fast Roaming.</p> <p>The default threshold value is set to 0. To configure, enter a desired threshold value ranging from 0 - 127.</p>
SNR Toggle Offset	<p>SNR Toggle Offset parameter is used to avoid frequent roaming (ping pong effect), in situations where the current BSU's Rx SNR and new BSU's Rx SNR are very close.</p> <p>If (Current BSU Rx SNR value + SNR Toggle offset) < (New BSU Rx SNR) then SU shifts to the new BSU. else, Continues with the same BSU.</p> <p>To configure, enter a desired offset value ranging from 0 - 10.</p>

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

To view the data rates and their corresponding minimum required SNR values to sustain an optimum link quality, click **Click here to view the Local SNR-Table**. See An Example - Local SNR Information.



- The Slow Roaming thresholds should be higher than the Fast Roaming thresholds, otherwise the Slow Roaming procedure will never be started. Switching from Slow to Fast, and from Fast to Emergency Roaming is possible but vice versa is not.
- In the roaming deployments, it is recommended to configure the same Announce Period in all the BSUs.
- While working on DFS channels, the roaming time increases and affects the performance as the device scans the channel for the presence of the RADAR for the duration of the configured Channel Wait Time.
- In VLAN aware scenarios, it is recommended not to use Roaming.

- The roaming time for an SU increases when the RADIUS based authentication is enabled on the BSU.
- When an SU registers with a new BSU, it will transfer all the data, buffered during transition, to the new BSU.

5.4.6 BSU / SU Profiles

In the BSU / SU Profiles tab, you can explicitly map a link profile to the peer device (See Link Profiles). When a link is established, using the peer MAC address, it is associated with a link profile based on the mapping created here. When no explicit mapping is created then the link is associated with the default profile.

5.4.6.1 Add a Profile



In this section, we have explained the method to map a link profile to an SU. The same method should be followed to map a link profile to a BSU.

To map a link profile to an SU device, navigate to **ADVANCED CONFIGURATION > Wireless > Interface 1 > SU Profiles**. The **SU Profiles** screen appears:

S.No.	SU Wireless MAC Address	Device Name	Configured Link Profile	Active Link Profile	Save
Notes:					
1. Maximum 250 entries are allowed.					
2. Default profile applied for SUs that donot have entry in table.					
<input type="button" value="Add"/>		<input type="button" value="Edit"/>			

Figure 5-43 SU Profiles

Click **Add** in the **SU Profiles** screen. The **SU Profile Add Entry** screen appears:

SU Wireless MAC Address	<input type="text" value="00:02:3a:4b:33:77"/>
Device Name	<input type="text" value="Subscriber1"/>
Link Profile Name	<input type="text" value="Profile1"/>
<input type="button" value="Add"/> <input type="button" value="Back"/>	

Figure 5-44 Add an SU Profile Entry

Configure the following parameters:

- **SU Wireless MAC Address:** Type the MAC Address of the peer.
- **Device Name:** Type the name of the peer.
- **Link Profile Name:** Map a link profile to the peer from the list of Link Profiles.

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

The profile is mapped to the peer device and is listed in the **SU Profiles** screen.

SU Profiles					
S.No.	SU Wireless MAC Address	Device Name	Configured Link Profile	Active Link Profile	Save
1	00:02:3a:4b:33:77	Subscriber1	Profile1	-	-

Notes:

- Maximum 250 entries are allowed.
- Default profile applied for SUs that donot have entry in table.

Figure 5-45 SU Profiles Entry Added

Consider a case where a device is currently connected to its peer and no link profile is explicitly mapped. Then in such a scenario, the default link profile is assigned and displayed in the **SU Profiles** screen along with a **Save** option, as shown below:

SU Profiles					
S.No.	SU Wireless MAC Address	Device Name	Configured Link Profile	Active Link Profile	Save
1	00:02:3a:4b:33:77	Subscriber1	Profile1	-	-
2	00:02:6f:5b:6b:30	System Name	Default	Default	<input type="button" value="Save"/>

Notes:

- Maximum 250 entries are allowed.
- Default profile applied for SUs that donot have entry in table.

Figure 5-46 Save an SU Profile

For such entries, user has the option to click **Save** button and configure this mapping in the profiles table. When you click **Save**, the following screen appears:

SU Profile Add Entry	
SU Wireless MAC Address	<input type="text" value="00:02:6f:5b:6b:30"/>
Device Name	<input type="text" value="System Name"/>
Link Profile Name	<input type="text" value="Default"/> ▼
<input type="button" value="Add"/> <input type="button" value="Back"/>	

Figure 5-47 Add an SU Profile

If you wish to map the peer with a profile other than default, then select a link profile (say Profile1) from **Link Profile Name** and click **Add**.

SU Profiles					
S.No.	SU Wireless MAC Address	Device Name	Configured Link Profile	Active Link Profile	Save
1	00:02:3a:4b:33:77	Subscriber1	Profile1	-	-
2	00:02:6f:5b:6b:30	System Name	Profile1	Default	-

Notes:

- Maximum 250 entries are allowed.
- Default profile applied for SUs that do not have entry in table.

Figure 5-48 SU Profile Added

The newly configured link profile will not be the Active Link Profile until you commit the changes. That is the reason, in the above screen, you are still able to see **Default** as the Active Link Profile for index 2, even though **Profile1** is configured. When you commit the changes, the Active Link Profile will change to **Profile1**, as shown in the following figure.

SU Profiles					
S.No.	SU Wireless MAC Address	Device Name	Configured Link Profile	Active Link Profile	Save
1	00:02:3a:4b:33:77	Subscriber1	Profile1	-	-
2	00:02:6f:5b:6b:30	System Name	Profile1	Profile1	-

Notes:

- Maximum 250 entries are allowed.
- Default profile applied for SUs that do not have entry in table.

Figure 5-49 Active SU Link Profile



- You can add a maximum of 250 entries in the profiles table.
- Under Link Statistics page, you can view the active profile the link is associated with.

5.4.6.2 Edit a Mapped Profile



In this section, we have explained the method to edit a mapped link profile of an SU. The same method should be followed to edit a mapped link profile of a BSU.

To edit a mapped profile, click **Edit** in the **SU Profiles** screen. The **SU Profile Edit Entry** screen appears:

SU Profile Edit Entry				
INDEX	SU Wireless MAC Address	Device Name	Link Profile Name	Delete
1	00:20:a6:11:33:55	Subscriber1	Profile1	Delete

OK Back

Figure 5-50 Edit a Mapped Profile

Make the necessary edits, and click **OK** followed by **COMMIT**.



: When the radio mode is changed (say BSU to SU, or SU to BSU), the link profiles and the peer profile mapping list is retained.

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 an SU, and a link between End Point A and End Point B. By default, the default security is **WORP Security**. A maximum of eight security profiles can be created as required; however, 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:

Wireless Security Configuration			
INDEX	Profile Name	Entry Status	Edit
1	WORP Security	Enable	

Notes:
1. Maximum 8 entries are allowed.

OK Add

Figure 5-51 Wireless Security Configuration

Given below is the table which explains Wireless Security parameters:

Parameter	Description
Profile Name	Specifies the security profile name. By default, it is WORP Security .
Entry status	Enables a user to either Enable or Disable the security profile on the device. By default, it is enabled.
Edit	Enables you to edit the existing security profiles. Click Edit 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:

Wireless Security Add Entry

Profile Name: WORP Security

Encryption Type: AES-CCM

Key:

Entry Status: Enable

Network Secret: (6-32) Characters

Notes:


1. For WEP the key length should be (Ascii 5/13/16) or (Hex 10/26/32).
2. For TKIP/AES-CCM the key length should be (Ascii 16) or (Hex 32).
3. WEP and TKIP are applicable when legacy mode is enabled.
4. For setting the *Network Secret* characters - = " ' ? \ / space are not allowed.

Add Back

Figure 5-52 Creating a New Security Profile

Given 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.

Parameter	Description
Encryption Type	<p>Select encryption type as either None, WEP, TKIP or AES-CCM.</p> <ol style="list-style-type: none"> None - If the encryption type is selected as None, then there exist no security to the data frames transmitted over the wireless medium. WEP (Wired Equivalent Privacy) - Represents the WEP Encryption type, which uses RC4 stream cipher for confidentiality and CRC-32 for integrity. The supported key lengths for WEP are 5/13/16 ASCII characters or 10/26/32 Hexadecimal digits. <ul style="list-style-type: none"> Key1 / Key 2 / Key 3 / key 4: You can configure a maximum of four WEP keys. Enter 5/13/16 ASCII Characters or 10/26/32 Hexadecimal digits for WEP keys. Transmit Key: Select one out of the four keys described above as the default transmit key, which is used for encrypting and transmitting the data. TKIP - Represents the TKIP Encryption type, which uses RC4 stream cipher for confidentiality. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism. It uses 128-bit keys for encryption. The key length for TKIP is 16 ASCII characters or 32 Hexadecimal digits. <ul style="list-style-type: none"> Key1 / Key 2 / Key 3 / key 4: You can configure a maximum of four TKIP keys. Enter 16 ASCII characters or 32 Hexadecimal digits. Transmit Key: Select one out of the four keys described above as the default transmit key, which is used for encrypting and transmitting the data. AES-CCM - Represents CCM Protocol with AES Cipher restricted to 128 bits. <ul style="list-style-type: none"> Key: Enter 16 ASCII characters or 32 Hex Digits for AES-CCM encryption keys.
Entry status	Enables you to either Enable or Disable 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 an SU with a BSU, and an End Point B with End Point A. The network secret should be same for both 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"> You can create a maximum of eight security profiles. A QuickBridge supports AES-CCM encryption type only. Special characters like - = \ " ' ? / space are not allowed while configuring the keys. 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. Transmit Key can be any one of the four keys, provided all the four keys are same in an SU and BSU, or End Point devices. WEP and TKIP Encryption types are supported only in legacy modes. The encryption mode should not be selected as AES-CCM while the device is interoperating with legacy Tsunami[®] MP.11 family devices.

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

5.5.1.1.1 Sample Security Profile Configuration

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

Profile Name	<input type="text" value="WORP Security"/>
Encryption Type	<input type="text" value="AES-CCM"/>
Key	<input type="text" value="....."/>
Entry Status	<input type="text" value="Enable"/>
Network Secret	<input type="text" value="....."/> (6-32) Characters

Notes:

1. For WEP the key length should be (Ascii 5/13/16) or (Hex 10/26/32).
2. For TKIP/AES-CCM the key length should be (Ascii 16) or (Hex 32).
3. WEP and TKIP are applicable when legacy mode is enabled.
4. For setting the *Network Secret* characters - = " ' ? \ / space are not allowed.

Figure 5-53 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 an 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 an 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 (See Wireless Outdoor Router Protocol (WORP)).

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

RADIUS Server Profile

INDEX	Profile Name	Max Retransmissions (0-3)	Message Response Time (3-9) Seconds	Re Authentication Period (0, 900-65535) Seconds
1	Default Radius	3	3	0

Notes:

1. Message Response Time < WORP Registration Timeout value.
2. Max Retransmissions * Message Response Time] < WORP Registration Timeout value.


INDEX	Server Type	IP Address	Server Port	Shared Secret	Entry Status
1	Primary Auth Server	169.254.128.133	1812	*****	Enable
2	Secondary Auth Server	169.254.128.134	1812	*****	Disable

OK

Figure 5-54 Configuring RADIUS Server Profile

Given 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 Default Radius .
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 an 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 enabled. 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"> 1. Primary RADIUS Server 2. Secondary RADIUS Server <p>The secondary RADIUS server serves as backup when the primary RADIUS server is down or not reachable.</p>

Parameter	Description
IP Address	Represents the IPv4 / IPv6 address of the primary and secondary RADIUS servers.  : IPv6 address should be the global IP address and not the link local IP address.
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 1812 .
Shared Secret	Specifies the password shared by the BSU/End Point A and the RADIUS server to communicate. The default password is public . 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 do not occur.
3. The value of **Max Retransmissions** multiplied by **Message Response Time** should be less than **WORP Registration Timeout** value.

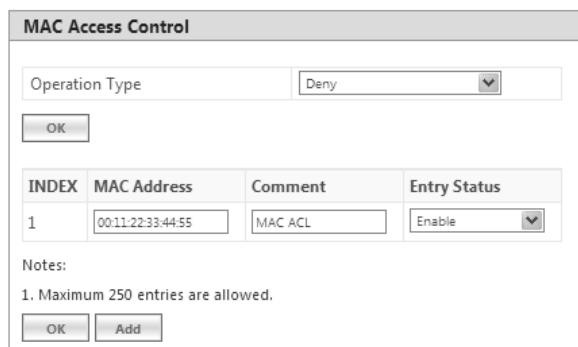
5.5.3 MAC ACL



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

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 (See Wireless Outdoor Router Protocol (WORP)).

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



MAC Access Control

Operation Type: Deny

OK

INDEX	MAC Address	Comment	Entry Status
1	00:11:22:33:44:55	MAC ACL	Enable

Notes:

1. Maximum 250 entries are allowed.

OK Add

Figure 5-55 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:

MAC ACL Add Entry	
MAC Address	00:11:22:33:44:55
Comment	TEST
Entry Status	Enable
<input type="button" value="Add"/> <input type="button" value="Back"/>	

Figure 5-56 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. QoS guarantees 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 classes by adding or using existing PIRs and SFCs; 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 frames and to Ethernet frames as well as to PPPoE encapsulated frames.

5.6.1 QoS Concepts and Definitions

QoS feature is applicable on both BSU/End Point A and SU/End Point B, but is configurable only on BSU/End Point A. When configured on BSU/End Point A, the QoS parameters is populated to all the registered SUs/End Point Bs and allows them to use the QoS configuration, as soon as they are connected to the BSU/ 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 out of maximum 64 PIRs may be associated per SFC
- **Class List** - Priority for each rule within each QoS class – 0 to 255, with 0 being lowest priority
- **QoS class** – up to 8 QoS classes, including 5 predefined classes; up to 8 out of maximum 32 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 where, each SFC contains the following parameters and values:

- Service flow name
- Scheduling type – Best Effort (BE); Real-Time Polling Service (RTPS)
 - **Best Effort Services:** Best Effort Services are typically provided by the Internet today for Web surfing. In the Tsunami[®] 800 and 8000 devices, Best Effort parameters include Maximum Information Rate, Committed Information Rate, Latency, Jitter and traffic priority.
 - **Real-Time Polling Services (RTPS):** RTPS is designed to support real-time services that generate fixed or variable size data packets on a periodic basis. Variable traffic can include MPEG video or VoIP with silence suppression. In the Tsunami[®] 800 and 8000 devices, RTPS QoS parameters include Maximum Information Rate, Committed Information Rate, Latency, Jitter and traffic priority.
- Time sensitive and real-time traffic should use RTPS (Including VoIP, Multicast Video and Serial Data). All other traffic (Variable Data, Unicast traffic, Internet) should be scheduled and prioritized using the Best Effort Service Flows. For QoS to function properly, ensure Interference is mitigated, keeping PHY and CRC errors at a minimum (<10/sec/avg). Retransmission at the PHY layer can cause latency, jitter overhead, packet loss and lower than expected throughput.
- Service Flow Direction – Downlink (DL: traffic from BSU/End Point A to SU/End Point B); 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 currently specified Maximum Information Rate (MIR)
- 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

The Traffic Priority with Scheduling Type and Committed Information Rate (CIR), defines the absolute Traffic Priority for a specific Service Flow as given below:

Committed Information Rate (CIR)	Scheduling Type	Traffic Priority	Absolute Priority
0	BE	0	0
0	BE	1	1
0	BE	2	2
0	BE	3	3

Committed Information Rate (CIR)	Scheduling Type	Traffic Priority	Absolute Priority
0	BE	4	4
0	BE	5	5
0	BE	6	6
0	BE	7	7
0	RtPS	0	8
0	RtPS	1	9
0	RtPS	2	10
0	RtPS	3	11
0	RtPS	4	12
0	RtPS	5	13
0	RtPS	6	14
0	RtPS	7	15
> 0 (<= MIR)	BE	0	16
> 0 (<= MIR)	BE	1	17
> 0 (<= MIR)	BE	2	18
> 0 (<= MIR)	BE	3	19
> 0 (<= MIR)	BE	4	20
> 0 (<= MIR)	BE	5	21
> 0 (<= MIR)	BE	6	22
> 0 (<= MIR)	BE	7	23
> 0 (<= MIR)	RtPS	0	24
> 0 (<= MIR)	RtPS	1	25
> 0 (<= MIR)	RtPS	2	26
> 0 (<= MIR)	RtPS	3	27
> 0 (<= MIR)	RtPS	4	28
> 0 (<= MIR)	RtPS	5	29
> 0 (<= MIR)	RtPS	6	30
> 0 (<= MIR)	RtPS	7	31

Obviously, there are 32 different absolute traffic priorities, priority 0 being the lowest and priority 31 being the highest.

It is important to note that for each SFC with CIR > 0, there are effectively two absolute traffic priorities allotted (total 16 priorities for the 8 SFC entries). The higher priority is used as long as the throughput of the traffic being sent through SFC is below or equal to the CIR, and the lower priority is used for the rest of the traffic, taking MIR configuration as the second priority. This switching of the priorities is done automatically by the scheduler, which makes sure that lower priority traffic gets transported only after all the higher priorities are transported successfully.

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 all types of traffic, the device will try to keep the jitter within the range 0 to configured Jitter value in milliseconds(ms). In order to allow the device maintain the traffic within the configured jitter range, each packet is buffered until a time interval equal to the difference between Latency and jitter (Latency – Jitter) has elapsed. When this interval elapses, the receiving device will deliver the packet. The delay of the packets is kept in the range (Latency – Jitter) to configured Latency value in millisecond(ms), that in turn maintains the jitter within the range 0 to configured Jitter value in milliseconds(ms).

However, possible retransmissions can increase maximum delay of the packet beyond Latency milliseconds, which can result in increased jitter as well. If the SFC's scheduling type is real-time polling (RtPS) and the packet is not delivered out from the transmitting unit within the time period equal to the Latency milliseconds, then the packet will be discarded on transmitting device. 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. Therefore RtPS type of polling must be used only if it is absolutely necessary.

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. To add new QoS classes, SFC and PIR, build the hierarchy of a QoS class as follows:

1. If new MAC Address, IP Address, and/or TCP/UDP Port are necessary, define the PIR MAC Address, IP Address and/or 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.

5.6.2.0.1 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.

QoS PIR MAC Address Entries				
INDEX	MAC Address	Mask	Comment	Entry Status
1	00:00:00:00:00:00	00:00:00:00:00:00	All	Enable <input type="button" value="v"/>
2	01:00:00:00:00:00	01:00:00:00:00:00	L2 Multicast	Enable <input type="button" value="v"/>
3	ff:ff:ff:ff:ff:ff	ff:ff:ff:ff:ff:ff	L2 Broadcast	Enable <input type="button" value="v"/>

Notes:

1. Maximum 256 entries are allowed.
2. MAC Address & Mask combination should be unique.
3. MAC Address entry in use cannot be deleted.

Figure 5-57 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.

QoS PIR MAC Address Add Entry	
MAC Address	10:20:30:10:50:80
Mask	10:20:11:25:33:66
Comment	TEST_CASE
Entry Status	Enable
<input type="button" value="Add"/> <input type="button" value="Back"/>	

Figure 5-58 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

5.6.2.0.2 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**.

QoS PIR IP Address Entries				
INDEX	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 in use cannot be deleted.

OK Add

Figure 5-59 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 5-60 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.

5.6.2.0.3 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**.

QoS PIR TCP/UDP Port Entries				
INDEX	Start Port	End Port	Comment	Entry Status
1	16000	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 in use cannot be deleted.

OK Add

Figure 5-61 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	60000
End Port	60000
Comment	TEST_CASE
Entry Status	Enable

Add Back

Figure 5-62 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 Service Flow Details. PIR rule referred by any QoS Class cannot be deleted.
- Click **OK**.

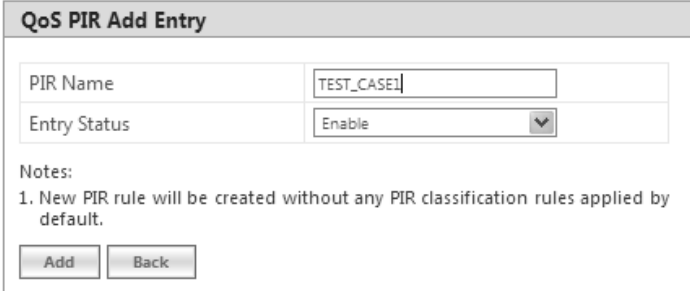
QoS PIR List			
S.No.	PIR Name	Entry Status	Details
1	All	Enable <input type="button" value="v"/>	<input type="button" value="Details"/>
2	L2 Multicast	Enable <input type="button" value="v"/>	<input type="button" value="Details"/>
3	L2 Broadcast	Enable <input type="button" value="v"/>	<input type="button"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

Notes:
 1. Maximum 64 entries are allowed.
 2. PIR Rule in use cannot be deleted.

Figure 5-63 QoS PIR Entries

To Add a New PIR Rule,

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



The screenshot shows a web-based configuration form titled "QoS PIR Add Entry". It contains two input fields: "PIR Name" with the value "TEST_CASE1" and "Entry Status" with a dropdown menu set to "Enable". Below the fields is a "Notes" section with a single bullet point: "1. New PIR rule will be created without any PIR classification rules applied by default." At the bottom of the form are two buttons: "Add" and "Back".

Figure 5-64 QoS PIR Add Entry

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

5.6.2.1.1 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

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

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 5-65 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	<p>This parameter is used to enable or disable a TOS rule. When ToS rule is enabled, configure the values for the following to specify the ToS-related configuration:</p> <ul style="list-style-type: none"> • ToS Low • ToS High • ToS Mask <p>In ToS Configuration, enter the decimal value of entire ToS 1 byte in "ToS Low" and "ToS High" parameters of the PIR rule.</p> <div data-bbox="539 741 1353 1115" style="text-align: center;"> <p>The diagram illustrates the bit-level structure of the ToS field in an IP header. It shows a sequence of bits from 7 down to 0. Bits 7, 6, 5, and 4 are grouped under 'IP Precedence'. Bits 3, 2, 1, and 0 are grouped under 'DSCP'. Bits 1 and 0 are specifically labeled as 'ECN (Unused Bits)'. Below this, a 1-byte header structure is shown with fields: Version Length, ToS, Length, ID, Offset, TTL, Protocol, FCS, SIP, DIP, and DATA. A bracket under 'Version Length' and 'ToS' indicates they together form the 1-byte ToS field.</p> </div> <p style="text-align: center;">Figure 5-66 IP Header Format</p> <p>ToS Low and ToS High values can be derived from DSCP (6 bits) and ECN (2 bits) values. ToS Value (8 bits) = DSCP Value (most significant 6 bits) + ECN Value (least significant 2 bits)</p> <p>Consider the following while configuring PIR TOS parameters:</p> <ol style="list-style-type: none"> To prioritize traffic based on specific DSCP value, configure the ToS Low and ToS High to the value derived from that DSCP (as mentioned in the example below) <p>For Example: To configure ToS Low and ToS High values, when the DSCP packet value is 10:</p> <ul style="list-style-type: none"> - DSCP (6 bit) = 10 (Binary value = 001010) - ECN (2 bit) = 0 (Binary value = 00) - ToS (Low and High) (8 bit) = DSCP(001010) + ECN(00) = 40 <p>Configure:</p> <ul style="list-style-type: none"> - ToS Low = 40 - ToS High = 40 To prioritize the traffic based on range of DSCP value, configure "ToS low" and "ToS High" to a range. <p>For Example: To configure ToS Low and ToS High values, when the DSCP packet is in range of 10 to 20, configure:</p> <ul style="list-style-type: none"> - ToS Low = 40 (DSCP = 10 (Binary 001010) + ECN = 0 (Binary 00)) - ToS High = 80 (DSCP = 20 (Binary 010100) + ECN = 0 (Binary 00))

Parameter	Description
	<p>3. To prioritize DSCP packets based on IP-Precedence/DSCP value/ToS value, configure "ToS Mask".</p> <ol style="list-style-type: none"> IP Precedence: To prioritize based on only IP precedence, set all the 3 IP Precedence bits in the ToS Mask parameter to "1" and set rest of the bits in the ToS Mask parameter to '0" (i.e decimal value = 224). DSCP Value: To prioritize based on DSCP value, set all the DSCP bits in the ToS Mask parameter to "1" and set rest of the bits in the ToS Mask parameter to '0" (i.e decimal value = 252). ToS Value: To prioritize based on entire ToS value then set all the bits in the ToS Mask parameter to "1" (i.e decimal value = 255).
Ether Priority Rule	<p>This parameters is used to enable or disable 802.1p priority rule. Enter the values for the following to specify 802.1p priority configuration:</p> <ul style="list-style-type: none"> • Priority Low • Priority High
VLAN Rule	<p>This parameters allows to enable or disable VLAN rule. Enter the VLAN ID when the VLAN rule is enabled.</p>
PPPoE Encapsulation	<p>This parameter is used to classify PPPoE traffic.</p>  <ul style="list-style-type: none"> • <i>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.</i> • <i>When PPPoE Encapsulation is enabled, incoming packet will be checked against Ether value "0x8864" and look for PPPoE Protocol Id value "0x0021"(IP Protocol) by default. User can modify the PPPoE Protocol Id but all the other classification rules which are specified in the PIR rule will work only if the PPPoE Protocol Id is "0021".</i> • <i>Ether Value is not valid when PPPoE Encapsulation is enabled.</i>
Ether Type Rule	<p>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:</p> <ul style="list-style-type: none"> • Ether Type • PPPoE Protocol Id • Ether Value  <ul style="list-style-type: none"> • <i>PPPoE Protocol Id is not valid if PPPoE Encapsulation is disabled.</i> • <i>Ether Value is not valid if PPPoE Encapsulation is enabled.</i>

5.6.2.1.2 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.

QoS PIR Protocol Id Add Entry

Notes:
 1. Maximum 4 entries are allowed.
 2. Valid range for Protocol Id is 1-65535.

New Protocol Entry

Protocol Id

Existing Protocol Entries

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

Figure 5-67 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.

5.6.2.1.3 Adding TCP/UDP Source Port Add Entry

- 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.

QoS PIR TCP/UDP Source Port Add Entry

Notes:
 1. 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 checked="" type="radio"/>
3	10000	20000	Vonage VOIP-2	<input checked="" type="radio"/>

Existing TCP/UDP Port Entries

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

Figure 5-68 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.

5.6.2.1.4 Adding TCP/UDP Destination Port Add Entry

- 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 Source Port Add Entry

Notes:
1. Maximum 4 entries are allowed.

New TCP/UDP Port Entry ADD Back

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

Existing TCP/UDP Port Entries

S.No.	Start Port	End Port	Comment	Delete
1	16000	33000	Cisco VOIP	Delete

Figure 5-69 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.

5.6.2.1.5 Adding IP Addresses

5.6.2.1.5.1 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

Notes:
1. Maximum 4 entries are allowed.

New IP Address Entry ADD Back

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

Existing IP Address Entries

S.No.	IP Address	Subnet Mask	Comment	Delete

Figure 5-70 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.

5.6.2.1.5.2 Adding Destination IP Address

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

QoS PIR Destination IP Address Add Entry

Notes:
1. Maximum 4 entries are allowed.

New IP Address Entry ADD Back

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

Figure 5-71 QoS PIR Destination IP Address Add Entry

- 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.

The following is explained with the help of an example:

1. Creating Matching profile for single IP address

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

IP Address: 169.254.28.133

IP Mask: 255.255.255.255

In this example, all bits in the IP Mask are enabled, so incoming traffic's IP address should exactly match with specified configured IP Address (i.e, 169.254.28.133). Other traffic is considered as non-matching traffic.

2. Creating Matching profile for all IP Address

IP Address: 0.0.0.0

IP Mask: 0.0.0.0

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

3. Creating Matching Profile for range of IP Address (169.254.128.0 to 169.254.128.255)

IP Address: 169.254.128.0

IP Mask: 255.255.255.0

4. Creating Matching Profile for Broadcast IP Address

IP Address: 255.255.255.255

IP Mask: 255.255.255.255

5. Creating Matching Profile for Single Multicast IP Address

IP Address: 224.0.0.9

IP Mask: 255.255.255.255

In this example, all bits in the IP Mask are enabled, so incoming traffic's multicast IP address should exactly match with specified configured multicast IP Address (i.e, 224.0.0.9). Other traffic is considered as non-matching traffic.

6. Creating Matching Profile for range of Multicast IP Address (224.0.0.0 to 224.0.0.255)

IP Address: 224.0.0.9

IP Mask: 255.255.255.255

5.6.2.1.6 Adding Source MAC Address

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

QoS PIR Source MAC Address Add Entry

Notes:
1. A maximum of 4 entries can be added.

New MAC Address Entry Add Back

Index	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	ff:ff:ff:ff:ff:ff	ff:ff:ff:ff:ff:ff	L2 Broadcast	<input type="radio"/>

Existing MAC Address Entries

Index	MAC Address	Mask	Comment	Delete
-------	-------------	------	---------	--------

Figure 5-72 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.

5.6.2.1.7 Adding Destination MAC Address

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

QoS PIR Destination MAC Address Add Entry

Notes:
1. 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	ff:ff:ff:ff:ff:ff	ff:ff:ff:ff:ff:ff	L2 Broadcast	<input type="radio"/>

Existing MAC Address Entries

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

Figure 5-73 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 List										
INDEX	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	Enabl
2	DL-Unlimited BE	BE	Down	307200	0	5	5	0	16	Enabl
3	DL-L2 Broadcast BE	BE	Down	307200	0	5	5	0	16	Enabl
4	UL-G711 20ms VoIP r	RTPS	Uplink	88	88	20	20	1	16	Enabl
5	DL-G711 20ms VoIP r	RTPS	Down	88	88	20	20	1	16	Enabl
6	UL-G729 20ms VoIP r	RTPS	Uplink	66	66	20	20	1	16	Enabl
7	DL-G729 20ms VoIP r	RTPS	Down	66	66	20	20	1	16	Enabl
8	DL 2 Mbps Video	RTPS	Down	2048	2048	20	20	1	16	Enabl

Notes:

1. Maximum 32 entries are allowed.
2. Service Flow entry in use cannot be deleted.
3. Recommended characters for *Service Flow Name* are **A-Z a-z 0-9 - _ = : . @ \$ & space**.

OK Add

Figure 5-74 QoS Service Flow Entries


- Adding a **New Service Flow (SFC)**
 - Click **Add** to add new entry. The following screen appears for configuring the new SU SFC Entry.

QoS Service Flow Add Entry	
Service Flow Name	TEST1
Scheduler Type	BE
Traffic Direction	Downlink
MIR	307200 (8- 307200) Kbps
CIR	0 (0- 307200) Kbps
Max Latency	10 (5-100) ms
Tolerable Jitter	10 (0-100) ms
Traffic Priority	0 (0-7)
Max Msgs In Burst	16 (1-16)
Entry Status	Enable
Notes:	
1. Recommended characters for <i>Service Flow Name</i> are A-Z a-z 0-9 - _ = : . @ \$ & space .	
<input type="button" value="Add"/> <input type="button" value="Back"/>	

Figure 5-75 QoS Service Flow Add Entry

- 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.
- Click **Add**.

Parameter	Description
Service Flow Name	Specifies the Name of the Service Flow. It can be of length 1-32 characters.
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**.

QoS Class List

Default QoS Class: ▼

L2 Broadcast QoS Class: ▼

Index	Class Name	Entry Status	Details
1	<input type="text" value="Unlimited Best Effort"/>	Enable ▼	<input type="button" value="Details"/>
2	<input type="text" value="L2 Broadcast Best Effort"/>	Enable ▼	<input type="button" value="Details"/>
3	<input type="text" value="G711 VoIP"/>	Enable ▼	<input type="button" value="Details"/>
4	<input type="text" value="G729 VoIP"/>	Enable ▼	<input type="button" value="Details"/>
5	<input type="text" value="2 Mbps Video"/>	Enable ▼	<input type="button" value="Details"/>

Notes:

1. A maximum of 8 entries can be added.
2. When an entry is not added to an SU, the *Default QoS Class* is applied.
3. *L2 Broadcast QoS Class* should have atleast one downlink *Service Flow*.
4. The QoS Class in use cannot be deleted.
5. Recommended characters for *Class Name* are **A-Z a-z 0-9 - _ = : . @ \$ & space**

Figure 5-76 QoS Class List

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.

QoS Class Add Entry

Class Name	<input type="text" value="Test1"/>
Service Flow Name	<input type="text" value="UL-G711 20ms VoIP rtPS"/> ▼
PIR Rule Name	<input type="text" value="ARP"/> ▼
Priority	<input type="text" value="5"/> (0-255)
Entry Status	<input type="text" value="Enable"/> ▼

Notes:
1. Recommended characters for *Class Name* are **A-Z a-z 0-9 - _ = : . @ \$ & space .**

Figure 5-77 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.
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.

5.6.2.3.1 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**.

QoS Class Service Flow Details			
Class Name		Unlimited Best Effort	
S.No.	SFC Name	Entry Status	Details
1	UL-Unlimited BE	Enable <input type="button" value="v"/>	<input type="button" value="Details"/>
2	DL-Unlimited BE	Enable <input type="button" value="v"/>	<input type="button" value="Details"/>
Notes:			
1. Maximum 8 entries are allowed.			
2. QoS class should have atleast one Service Flow entry.			
<input type="button" value="OK"/>		<input type="button" value="Add"/> <input type="button" value="Back"/>	

Figure 5-78 QoS Class Service Flow Details

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

QoS Service Flow Add Entry	
Service Flow Name	UL-Unlimited BE <input type="button" value="v"/>
PIR Rule Name	All <input type="button" value="v"/>
Priority	0 (0-255)
Entry Status	Enable <input type="button" value="v"/>
Notes:	
1. Same Service Flow cannot exists more than once in a QoS Class.	
<input type="button" value="Add"/> <input type="button" value="Back"/>	

Figure 5-79 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.

5.6.2.3.2 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**.

QoS Class PIR Details			
Class Name		Unlimited Best Effort	
Service Flow Name		UL-Unlimited BE	
S.No.	PIR Name	Priority (0-255)	Entry Status
1	All	0	Enable
Notes:			
1. Maximum 8 entries are allowed.			
2. The same PIR rule can not exists more than once in either direction of the QoS Class.			
OK		ADD Back	

Figure 5-80 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.

QoS Class PIR Add Entry	
PIR Rule Name	PPPoE Control
Priority	0 (0-255)
Entry Status	Enable
Notes:	
1. Each PIR cannot exist more than once in either direction(Uplink/Downlink) per QoS Class.	
Add Back	

Figure 5-81 QoS Class PIR Add Entry

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



: When you change the entry status of an existing QoS Class, the status changes immediately. For example, when you change the entry status to **delete**, the corresponding QoS Class get deleted even before you click **OK**.

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.

QoS SU List				
S.No.	MAC Address	Class Name	Comment	Entry Status
1	10:20:30:40:50:60	Unlimited Best Effort	Test_case	Enable

Notes:

- Maximum 250 entries are allowed.

Figure 5-82 QoS SU or End Point B List

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

5.6.2.4.1 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 Entry	
Wireless MAC Address	<input type="text" value="10:20:30:40:50:60"/>
Class Name	<input type="text" value="Unlimited Best Effort"/> ▼
Comment	<input type="text" value="Test_case"/>
Entry Status	<input type="text" value="Enable"/> ▼
<input type="button" value="Add"/> <input type="button" value="Back"/>	

Figure 5-83 QoS SU or End Point B Table Add Entry

- 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 BSU/End Point A or SU/End Point B 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.

5.6.3.0.1 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.

5.6.3.0.2 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)

5.6.3.0.3 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.

5.6.3.0.4 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.



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).

5.6.3.0.5 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 (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 b - h 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 an 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 an SU from a RADIUS Server.

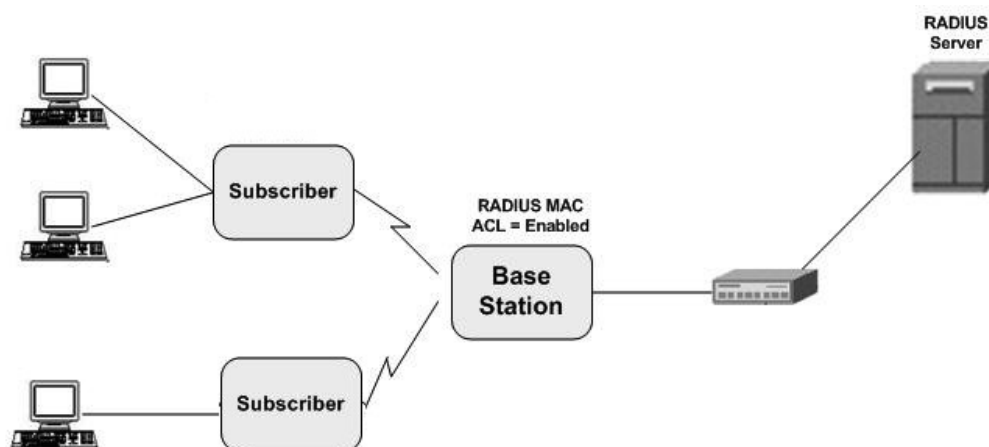


Figure 5-84 RADIUS Based QoS Configuration

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.

Given 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
- Limits the broadcast and multicast traffic to a specific VLAN group
 - 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.*
- *The MP.11 SU should locally configure VLAN parameters when it is connected to a MP 82x/8000 BSU in legacy mode.*
- *The MP 82x/8000 SU in legacy mode should locally configure VLAN parameters when it is connected to a MP.11 BSU.*

5.8.1 System-Level VLAN Configuration

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

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

Figure 5-85 System-Level VLAN Configuration (BSU)

VLAN	
VLAN Status	<input type="checkbox"/>
Management VLAN Id	-1 (-1, 1-4094)
Management VLAN Priority	0 (0 - 7)
Double VLAN (Q in Q) Status	Disable
OK	

Figure 5-86 System-Level VLAN Configuration (SU/End Point A/End Point B)

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**.



- Only SU, End Point A and End Point B support Double VLAN (Q in Q) feature.
- 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 based on the management VLAN ID configured.

For more details on QinQ, refer to Appendix QinQ.

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 WORP 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 5-87 Transparent Mode

Given 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 VLAN mode as Transparent .  : 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 an 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 WORP 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 WORP 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:

Figure 5-88 Access Mode

Given 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 VLAN mode as Access and click OK .
Access VLAN Id	Enter the Access VLAN Id in the Access VLAN Id 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.

Parameter	Description
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.
Allow Untagged Mgmt Access	When enabled, the Management Access is allowed using untagged packets. By default, it is disabled.

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 an 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: Disable

INDEX	Trunk Id	Entry Status
1.1	6	Enable

Notes:
1. Maximum 256 entries are allowed.

OK Add

Figure 5-89 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)

INDEX	Trunk Id	Entry Status
Notes: 1. If <i>Double VLAN Status</i> is enabled, <i>VLAN mode</i> should not be Transparent. 2. Maximum 16 entries are allowed. 3. If <i>Double VLAN Status</i> is enabled, <i>Port VLAN id</i> should not be -1. 4. <i>Port VLAN id</i> should not exist in Trunk Table.		

Figure 5-90 Trunk Mode (SU/End Point A/End Point B)

Given 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 VLAN Mode as Trunk .
Allow Untagged Frames	Select Enable or Disable . By default, it is disabled. <ul style="list-style-type: none"> • Disable: If this option is selected, the Ethernet interface forwards only tagged frames whose VLAN Id matches with a VLAN ID present in trunk table. • Enable: <ul style="list-style-type: none"> – In case of a BSU, when Allow Untagged Frames is enabled, the Ethernet interface of the device forwards the data packets as-is. – In case of an SU/End Point A/End Point B, when Allow Untagged Frames is enabled, the device behaves as in Access mode. Click OK.

Parameter	Description
Port VLAN ID	<p>Enter the Port VLAN ID in the Port VLAN ID 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"> • <i>Applicable only on an SU, End Point A and End Point B.</i> • <i>When Double VLAN is enabled on the device, the Port VLAN ID should not be set to -1.</i> • <i>The configured Port VLAN Id should not exist in the Trunk table.</i>
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>  : <i>Applicable only to SU and End Point devices.</i>

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

5.8.2.3.1 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 5-91 Add VLAN IDs to Trunk Table

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

Parameter	Description
Trunk Id	Enter VLAN ID in the Trunk Id box.
Entry Status	This parameter indicates the status of each VLAN Trunk Id entry. By default, the Trunk Id is enabled. To disable, select Disable from the Entry Status 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 trunk VLAN Ids in an SU and End Point B device.

5.9 RADIUS Based SU VLAN Configuration

RADIUS based VLAN configuration enables you to configure VLAN parameters on an 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 an SU from a RADIUS Server.

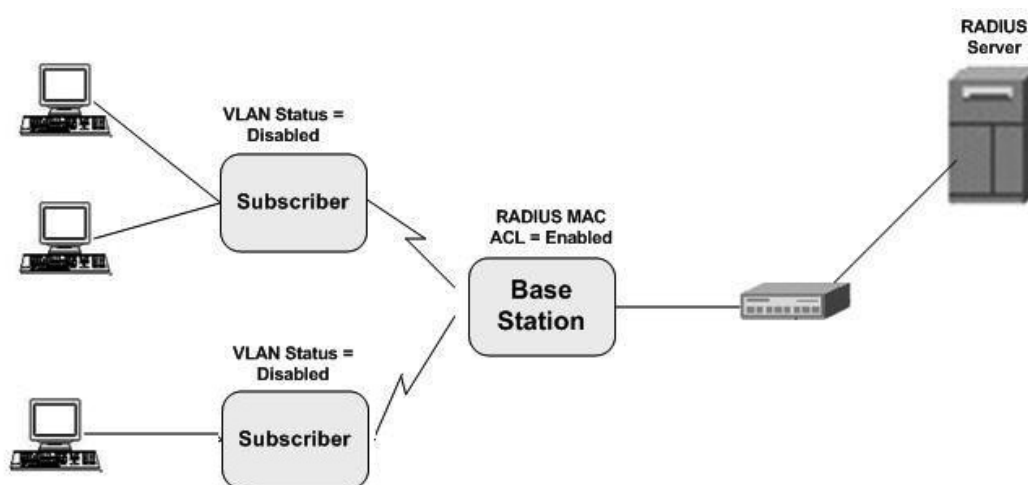


Figure 5-92 RADIUS Based VLAN Configuration

To connect to a 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.

Given 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
Ethernet 1 VLAN Mode	4	Decimal	1 –Transparent Mode 2 – Access Mode / 3 – Trunk Mode
SU VLAN Name	5	String	SU VLAN Name
Ethernet 1 Access VLAN ID	6	Decimal	1 – 4095
Ethernet 1 Access VLAN Priority	7	Decimal	0 – 7

Name of the attribute	Vendor Assigned Attribute Number	Attribute Format	Attribute Value
Management Attribute VLAN ID	8	Decimal	1 – 4095
Management VLAN Priority	9	Decimal	0 – 7
VLAN Ethernet 1 Trunk IDs 1 to 16	10 ... 25	Decimal	1 – 4095
SU VLAN Table Status (Applicable only to MP/QB.11 devices)	26	Decimal	1 – enable / 2 – disable / 3 – delete
Service VLAN ID (Q-in-Q)	32	Decimal	1 – 4095
Service VLAN Priority (Q-in-Q)	33	Decimal	0 – 7
QoS Class Index	34	Decimal	1 – 8
QoS Class SU Table Status	35	Decimal	1 – Enable / 2 – Disable
Ethernet 2 VLAN Mode	40	Decimal	1 – Transparent Mode 2 – Trunk Mode / 3 – Access Mode
Ethernet 2 Access VLAN ID	41	Decimal	1 – 4095
Ethernet 2 Access VLAN Priority	42	Decimal	0 – 7
VLAN Ethernet 2 Trunk IDs 1 to 16	43 ... 58	Decimal	1 – 4095
Double VLAN (Q-in-Q) Status	59	Decimal	1 – Enable / 2 – Disable
Serviceably TPID (Q-in-Q)	60	Decimal	1 - InnerTag / 2 - Outer Tag
Ethernet 1 Port VLAN ID	61	Decimal	1 – 4095
Ethernet 1 port VLAN Priority	62	Decimal	0 – 7
VLAN Ethernet 1 Allow Untag Frames	63	Decimal	1 – Enable / 2 – Disable
Ethernet 2 Port VLAN ID	64	Decimal	1 – 4095
Ethernet 2 Port VLAN Priority	65	Decimal	0 – 7
VLAN Ethernet 2 Allow Untag Frames	66	Decimal	1 – Enable / 2 – Disable
VLAN Ethernet 1 Allow Untag Management	68	Decimal	1-Enable 2-Disable
VLAN Ethernet 2 Allow Untag Management	69	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.

- An MP.11 SU should locally configure VLAN parameters when connected to a MP 82x/8000 BSU in legacy mode as the BSU will not assign any VLAN parameters based on RADIUS authentication.
- An MP 82x/8000 SU should locally configure VLAN in legacy mode when connected to a MP.11 BSU, should locally configure VLAN parameters as the BSU shall not assign VLAN parameters based on RADIUS authentication.

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
- WORM Intra Cell Blocking

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.

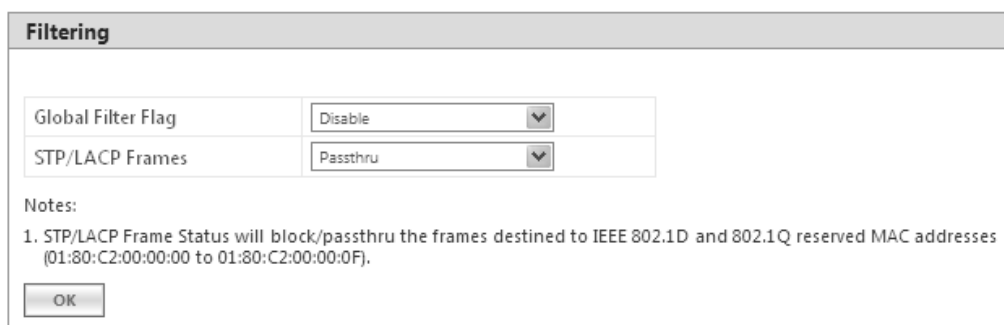



Figure 5-93 Filtering

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

Parameter	Description
Global Filter Flag	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. Please note that if Global Filter Flag is not enabled on the device, then none of the filters can be applied on the device.

Parameter	Description
STP/LACP Frames	<p>This parameter allows you to either Block or Passthru STP/LACP frames on the network.</p> <ul style="list-style-type: none"> • Passthru: 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. • Block: When blocked, the STP/LACP frames encountered on a network are terminated at bridge. <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:

INDEX	Protocol Name	Protocol Number	Filter Status	Entry Status
1	<input type="text" value="Apollo-Domain"/>	<input type="text" value="8019"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>
2	<input type="text" value="Apple-Talk-1-and-2"/>	<input type="text" value="809b"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>
3	<input type="text" value="Apple-Talk-ARP-1-and-2"/>	<input type="text" value="80f3"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>
4	<input type="text" value="Banyan-VINES"/>	<input type="text" value="0bad"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>
5	<input type="text" value="Banyan-VINES-Echo"/>	<input type="text" value="0baf"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>
6	<input type="text" value="Decnet-Phase-IV"/>	<input type="text" value="6003"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>
7	<input type="text" value="DEC-Diagnostic"/>	<input type="text" value="6005"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>
8	<input type="text" value="DEC-LAT"/>	<input type="text" value="6004"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>
9	<input type="text" value="DEC-MOP-Dump/Load"/>	<input type="text" value="6001"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>
10	<input type="text" value="DEC-MOP-Rem-Cons"/>	<input type="text" value="6002"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>
11	<input type="text" value="DEC-NetBIOS"/>	<input type="text" value="8040"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>
12	<input type="text" value="HP-Probe-Control"/>	<input type="text" value="8005"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>
13	<input type="text" value="IBM-SNA-Services"/>	<input type="text" value="80d5"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>
14	<input type="text" value="IP-ARP"/>	<input type="text" value="0806"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>
15	<input type="text" value="Novell(ECONFIG-E)"/>	<input type="text" value="8137"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>
16	<input type="text" value="RARP-Reverse-ARP"/>	<input type="text" value="8035"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>
17	<input type="text" value="SNMP-Over-Ethernet"/>	<input type="text" value="814c"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>
18	<input type="text" value="Xyplex"/>	<input type="text" value="0888"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>
19	<input type="text" value="EAPOL-ether-type"/>	<input type="text" value="888e"/>	<input type="text" value="Block"/>	<input type="text" value="Disable"/>

Notes:
1. Maximum 64 entries are allowed.

Figure 5-94 Protocol Filter