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

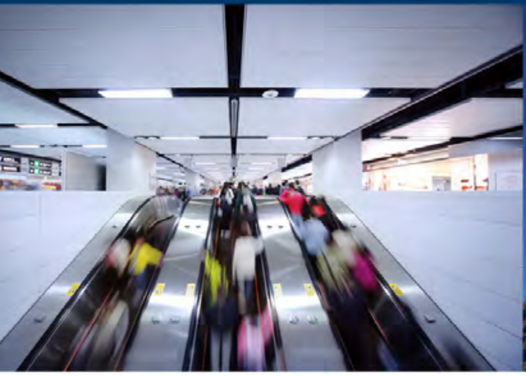
Products Covered

--> Tsunami® Multipoint

- MP-8200-BSU-G; MP-8250-BS9-G; MP-8250-BS1-G
- MP-8200-BSU; MP-8250-BS9; MP-8250-BS1
- MP-820-BSU-100
- MP-822-BSU-100
- MP-825-BS3-100
- MP-820-SUA-50$^+$
- MP-820-SUA-100
- MP-822-SUA-100
- MP-825-SUR-50$^+$
- MP-825-SUR-100
- MP-825-CPE-50
- MP-825-CPE-100
- MP-835-CPE-10
- MP-835-CPE-25
- MP-835-CPE-50
- MP-835-CPE-100
- MP-8100-SUA
- MP-8150-SUR
- MP-8150-SUR-100
- MP-8200-SUA
- MP-8250-SUR

--> Tsunami Quickbridge®

- QB-8200-EPA-G/LNK-G
- QB-8250-EPR-G/LNK-G
- QB-8200-EPA/LNK
- QB-8250-EPR/LNK
- QB-825-EPR/LNK-50$^+$
- QB-825-EPR/LNK-100
- QB-835-EPR/LNK-25
- QB-835-EPR/LNK-50
- QB-826-EPR/LNK-100



proxim wireless

Copyright

Trademarks

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

OpenSSL License Note

Tsunami® 800 and 8000 Series - Software Management Guide

Documentation Version: 6.5
P/N 765-00131, May 2016

Preface

This chapter contains the following information:

- 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

Product(s)	Supported Countries	Supported Software Version
MP-8200-BSU-G	US, WD, EU	3.2.1 (901050)
MP-8250-BS9-G	US, WD, EU	3.2.1 (901050)
MP-8250-BS1-G	US, WD	3.2.1 (901050)
MP-8200-BSU	US, WD, EU	3.2.1 (901050)
MP-8250-BS9	US, WD, EU	3.2.1 (901050)
MP-8250-BS1	US, WD	3.2.1 (901050)
MP-820-BSU-100	US, WD, EU	3.3.0 (905192)
MP-822-BSU-100	IC	3.3.0 (905192)
MP-825-BS3-100	US, WD, EU	3.3.0 (905192)
MP-8100-SUA	US, WD, EU	3.2.1 (901050)
MP-8150-SUR	US, WD, EU	3.2.1 (901050)
MP-8150-SUR-100	US, WD, EU	3.2.1 (901050)
MP-8200-SUA	US, WD, EU, JP	3.2.1 (901050)
MP-8250-SUR	US, WD, EU, JP	3.2.1 (901050)
MP-820-SUA-50$^+$	US, WD, EU	3.3.0 (905192)
MP-820-SUA-100	US, WD	3.3.0 (905192)
MP-822-SUA-100	IC	3.3.0 (905192)
MP-825-SUR-50$^+$	US, WD, EU	3.3.0 (905192)
MP-825-SUR-100	US, WD	3.3.0 (905192)
MP-825-CPE-50	US, WD, EU	3.3.0 (905192)

Product(s)	Supported Countries	Supported Software Version
MP-825-CPE-100	US, WD, EU	3.3.0 (905192)
MP-835-CPE-10	US, WD, EU	3.3.0 (905192)
MP-835-CPE-25	US, WD, EU	3.3.0 (905192)
MP-835-CPE-50	US, WD, EU	3.3.0 (905192)
MP-835-CPE-100	US, WD, EU	3.3.0 (905192)
QB-8200-EPA-G/LNK-G	US, WD, EU	3.2.1 (901050)
QB-8250-EPR-G/LNK-G	US, WD, EU	3.2.1 (901050)
QB-8200-EPA/LNK	US, WD, EU	3.2.1 (901050)
QB-8250-EPR/LNK	US, WD, EU	3.2.1 (901050)
QB-825-EPR/LNK-50^{+}	US, WD, EU	3.3.1 (905201)
QB-825-EPR/LNK-100	US, WD	3.3.1 (905201)
QB-835-EPR/LNK-25	US, WD	3.3.1 (905201)
QB-835-EPR/LNK-50	US, WD	3.3.1 (905201)
QB-826-EPR/LNK-100	WD	3.3.1 (905201)

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

For more information, please refer to the following additional documents that are available at Proxim's support site http://my.proxim.com.

- **Quick Installation Guide (QIG)**: A quick reference guide that provides essential information for installing and configuring the device.
- **Hardware Installation Guide**: A guide that provides a hardware overview and details about the installation procedures and hardware specifications.
- **Reference Guide**: A guide that provides essential information on how to configure, manage and monitor the device using the Command Line Interface.
- **Safety and Regulatory Compliance Guide**: A guide that provides essential information on the country specific safety and regulatory norms to be followed while installing the device.
- **Antenna Recommendation Guide** - A guide that gives insight on the recommended antennas for the device, along with the antenna specifications.
- **Antenna Installation Guide** - A guide that gives insight on how to set up and install the outdoor antenna(s).

Proxim recommends you to visit its support site http://my.proxim.com for regulatory information and latest product updates.

Documentation Conventions

Icon Representation

Name	Image	Meaning
Note	📝	A special instruction that draws attention of a 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.

Overview

1

This chapter contains information on the following:

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-8200-BSU-G	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 GPS Sync ready, a 3x3 MIMO high power radio and three N-Type connectors to connect external antennas.	
MP-8250-BS9-G	The MP-8250 Base Station unit comes with GPS Sync ready, 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-G	The MP-8250 Base Station unit comes with GPS Sync ready, 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-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-820-BSU-100	The MP-820 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 GPS Sync Ready, a 2x2 MIMO radio and two N-Type connectors to connect external antennas. It provides an aggregate throughput of 100 Mbps.	

Product	Description	Image
MP-822-BSU-100	The MP-822 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 2x2 MIMO radio and two N-Type connectors to connect external antennas. It provides an aggregate throughput of 100 Mbps.	
MP-825-BS3-100	The MP-825 Base Station unit comes with GPS Sync Ready, a 2x2 MIMO radio and 15 dBi integrated dual-polarized panel antenna that operates in 4.900 to 5.925 GHz frequency band. It provides an aggregate throughput of 100 Mbps.	
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-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-820-SUA-50+	The MP-820 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 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-820-SUA-100	The MP-820 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 2x2 MIMO radio and two N-Type connectors to connect external antennas. It provides an aggregate throughput of 100 Mbps.	
MP-822-SUA-100	The MP-822 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 2x2 MIMO radio and two N-Type connectors to connect external antennas. It provides an aggregate throughput of 100 Mbps.	

Product	Description	Image
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 4.900 to 5.925 GHz frequency band. It provides an aggregate throughput of 50 Mbps, license upgradable to 100 Mbps.	
MP-825-SUR-100	The MP-825 Subscriber unit comes with a 2x2 MIMO radio and 15 dBi integrated dual-polarized panel antenna that operates in 4.900 to 5.925 GHz frequency band. It provides an aggregate throughput of 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 4.900 to 5.925 GHz frequency band with aggregate throughput of 50 Mbps.	
MP-825-CPE-100	The MP-825 Customer Premises Equipment comes with a 2x2 MIMO radio and 15 dBi integrated dual-polarized panel antenna that operates in 4.900 to 5.925 GHz frequency band with an aggregate throughput of 100 Mbps.	
MP-835-CPE-10	The MP-835 Customer Premises Equipment comes with a 2x2 MIMO radio and 15 dBi integrated dual-polarized panel antenna that operates in 4.900 to 5.925 GHz frequency band with an aggregate throughput of 10 Mbps.	
MP-835-CPE-25	The MP-835 Customer Premises Equipment comes with a 2x2 MIMO radio and 15 dBi integrated dual-polarized panel antenna that operates in 4.900 to 5.925 GHz frequency band with an aggregate throughput of 25 Mbps.	
MP-835-CPE-50	The MP-835 Customer Premises Equipment comes with a 2x2 MIMO radio and 15 dBi integrated dual-polarized panel antenna that operates in 4.900 to 5.925 GHz frequency band with an aggregate throughput of 50 Mbps.	
MP-835-CPE-100	The MP-835 Customer Premises Equipment comes with a 2x2 MIMO radio and 15 dBi integrated dual-polarized panel antenna that operates in 4.900 to 5.925 GHz frequency band with an aggregate throughput of 100 Mbps.	
QB-8200-EPA-G	The QB-8200-EPA-G QuickBridge operates in 4.900 – 5.925 GHz frequency band. This connectorized device comes with GPS Sync ready, a 3x3 MIMO high power radio and three N-Type connectors to connect external antennas.	
QB-8200-LNK-G	A pair of QB-8200-EPA-G -G devices form a link.	

Product	Description	Image
QB-8250-EPR-G	The QB-8250-EPR QuickBridge comes with GPS Sync ready, a 2x2 MIMO high power radio and 23 dBi integrated dual-polarized panel antenna that operates in 4.900 – 5.925 GHz frequency band.	
QB-8250-LNK-G	A pair of QB-8250-EPR-G devices form a link.	
QB-8200-EPA	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.	
QB-8200-LNK	A pair of QB-8200-EPA devices form a link.	
QB-8250-EPR	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.	
QB-8250-LNK	A pair of QB-8250-EPR devices form a link.	
QB-825-EPR-50+	The QB-825-EPR-50+ device comes with GPS Sync Ready, a 2x2 MIMO high power radio and 15 dBi integrated dual-polarized panel antenna that operates in 4.900 to 5.925 GHz frequency band. It provides an aggregate throughput of 50 Mbps, license upgradable to 100 Mbps.	
QB-825-LNK-50+	A pair of QB-825-EPR-50+ devices form a link.	
QB-825-EPR-100	The QB-825-EPR-100 device comes with a 2x2 MIMO high power radio and 15 dBi integrated dual-polarized panel antenna that operates in 4.900 to 5.925 GHz frequency band. It provides an aggregate throughput of100 Mbps.	

Product	Description	Image
QB-825-LNK-100	A pair of QB-825-EPR-100 devices form a link.	
QB-835-EPR-25	The QB-835-EPR-25 device comes with a 2x2 MIMO radio and 15 dBi integrated dual-polarized panel antenna that operates in 4.900 to 5.925 GHz frequency band with aggregate throughput of 25 Mbps License upgradable to 50 Mbps.	
QB-835-LNK-25	A pair of QB-835-EPR-25 devices form a link.	
QB-835-EPR-50	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 4.900 to 5.925 GHz frequency band with aggregate throughput of 50 Mbps.	
QB-835-LNK-50	A pair of QB-835-EPR-50 devices form a link.	
QB-826-EPR-100	The QB-826-EPR-100 device comes with a 2x2 MIMO high power radio and 15 dBi integrated dual-polarized panel antenna that operates in 5.900 – 6.425 GHz frequency band. It provides an aggregate throughput of 100 Mbps.	
QB-826-LNK-100	A pair of QB-826-EPR-100 devices form a link.	

1.2 Wireless Network Topology

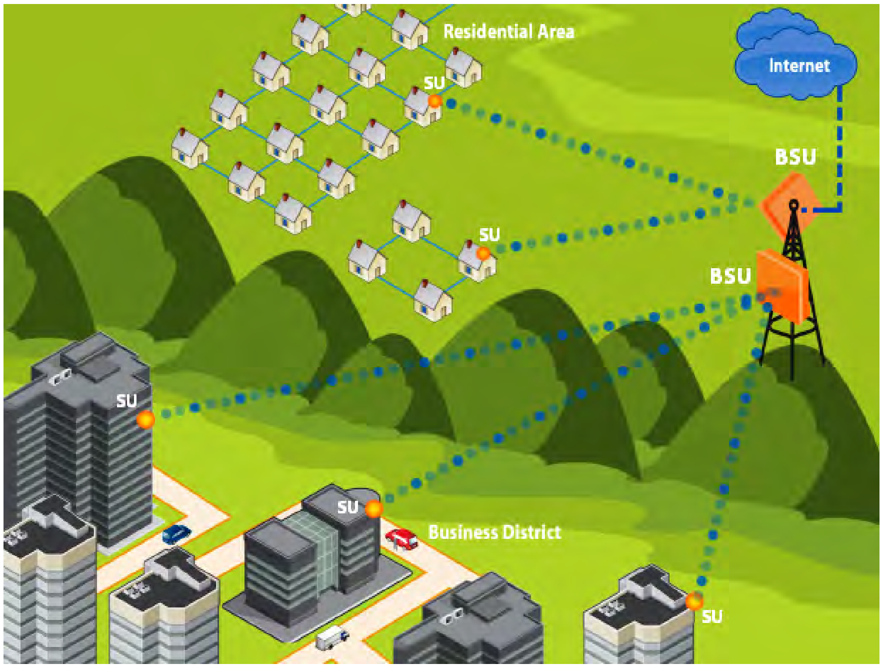
1.2.1 Point-to-Multipoint (PTMP)

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.

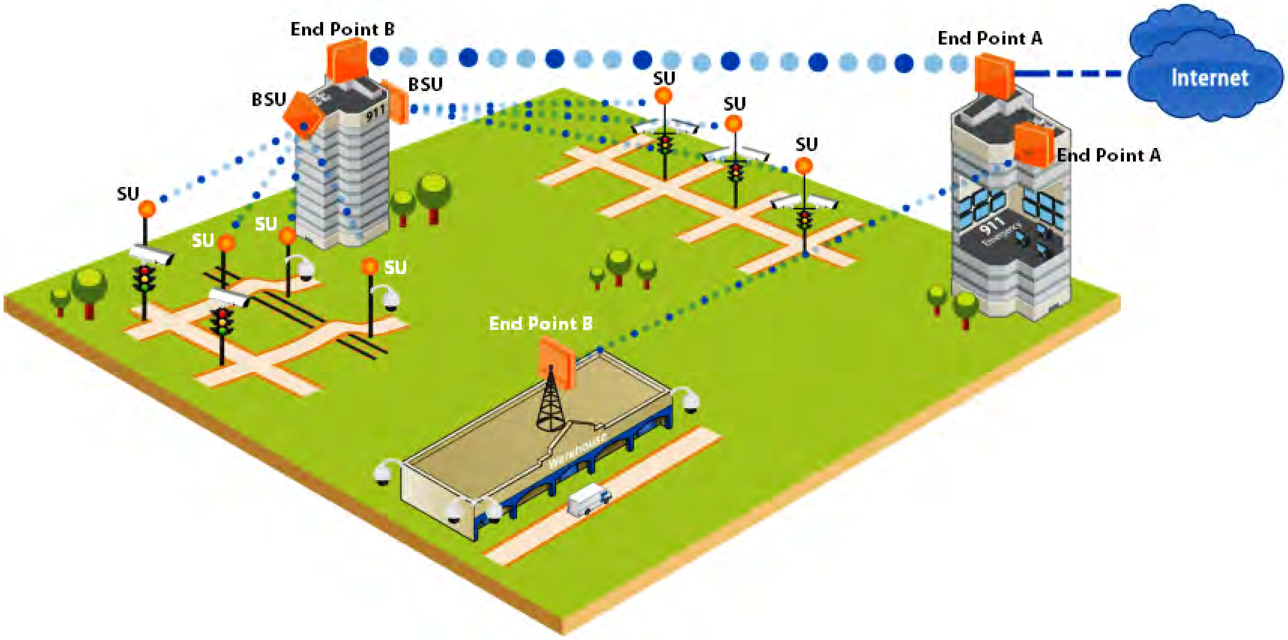
Given below are the deployment scenarios, where Proxim's point-to-multipoint devices are recommended. The Proxim devices used in the deployment images are commonly referred to as BSU (Base Station Unit) and SU (Subscriber Unit). The combinations that are used for BSU and SU multipoint devices are:

Base Station Unit (BSU)	Subscriber Unit (SU)
MP-822-BSU-100	MP-822-SUA-100
MP-8200-BSU-G MP-8250-BS9-G MP-8250-BS1-G MP-8200-BSU MP-8250-BS9 MP-8250-BS1 MP-820-BSU-100 MP-825-BS3-100	MP-8100-SUA
	MP-8150-SUR
	MP-8150-SUR-100
	MP-8200-SUA
	MP-8250-SUR
	MP-820-SUA-50^{+}
	MP-820-SUA-100
	MP-825-SUR-50^{+}
	MP-825-SUR-100
	MP-825-CPE-100
	MP-825-CPE-50
	MP-835-CPE-10
	MP-835-CPE-25
	MP-835-CPE-50
	MP-835-CPE-100

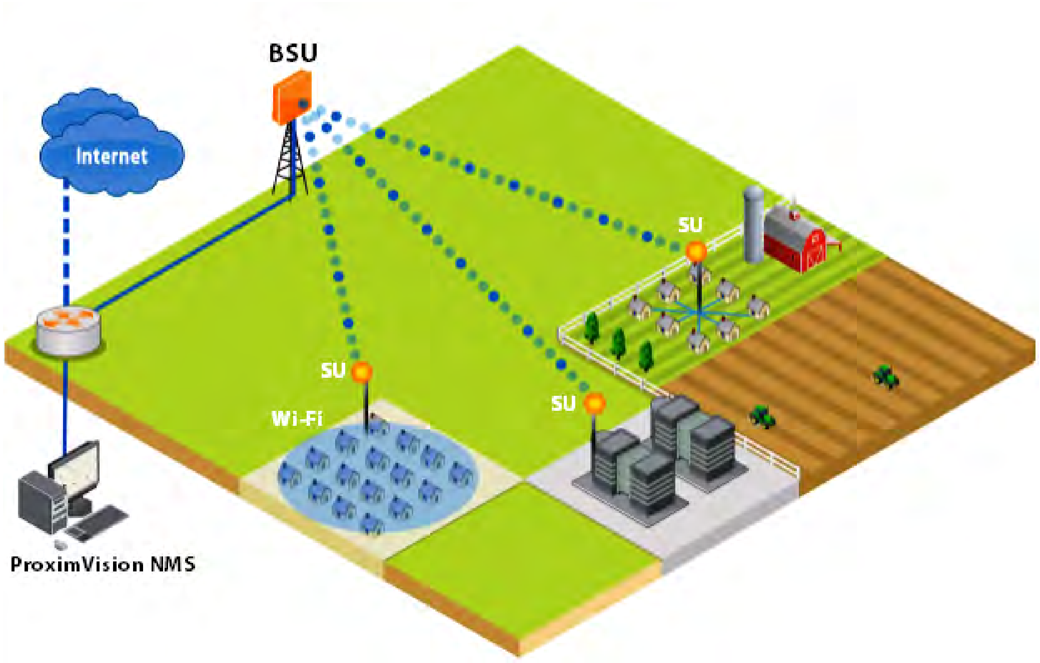
- **Last Mile Access**: Competitive broadband service access alternative to Digital Subscriber Line (DSL) or cable for residences and T1 or Ethernet for businesses.



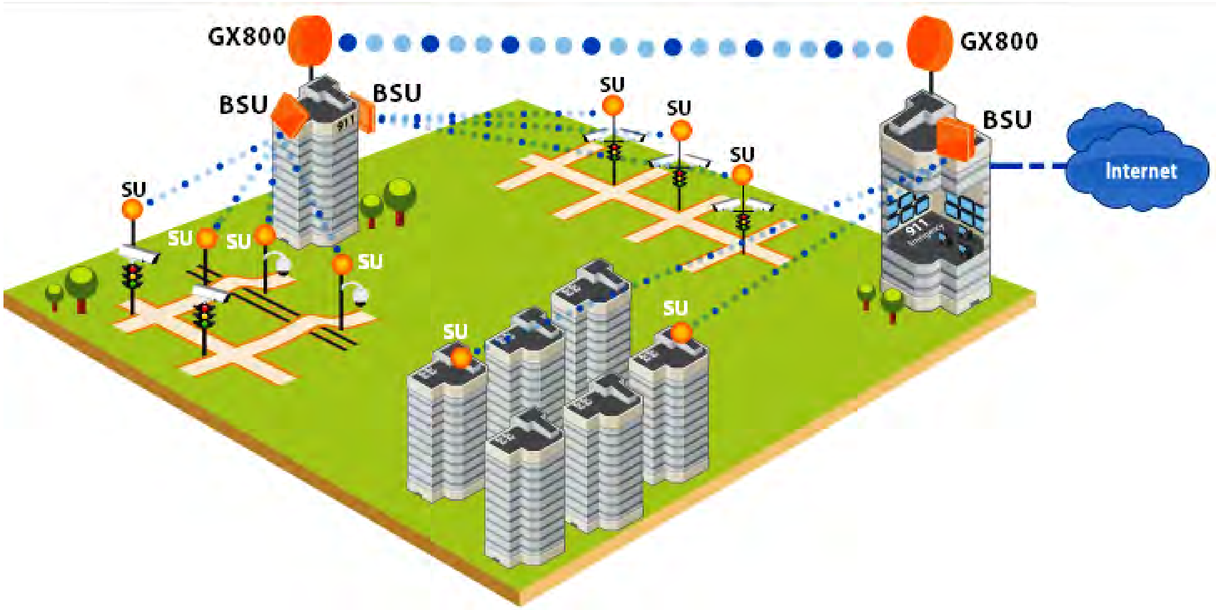
- **Security and Surveillance**: High definition IP-surveillance cameras for monitoring city streets, airports, bridges, seaports, transportation hubs, offices and warehouses.



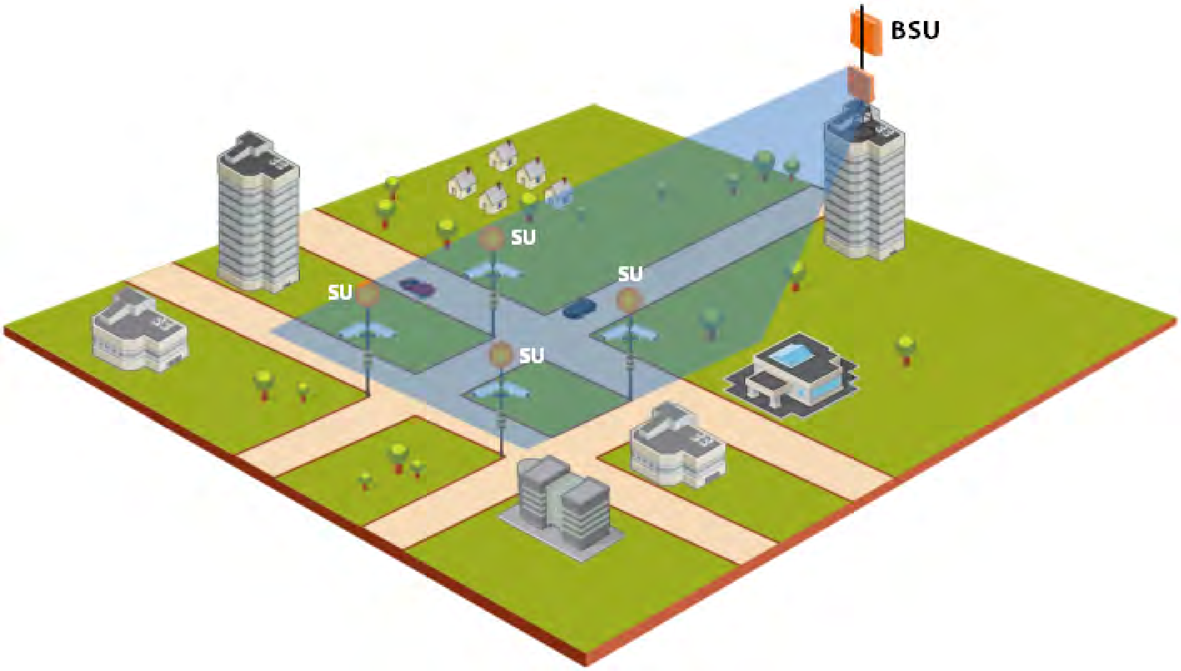
- **Metropolitan Area Network**: Secure and reliable connectivity between city buildings.



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

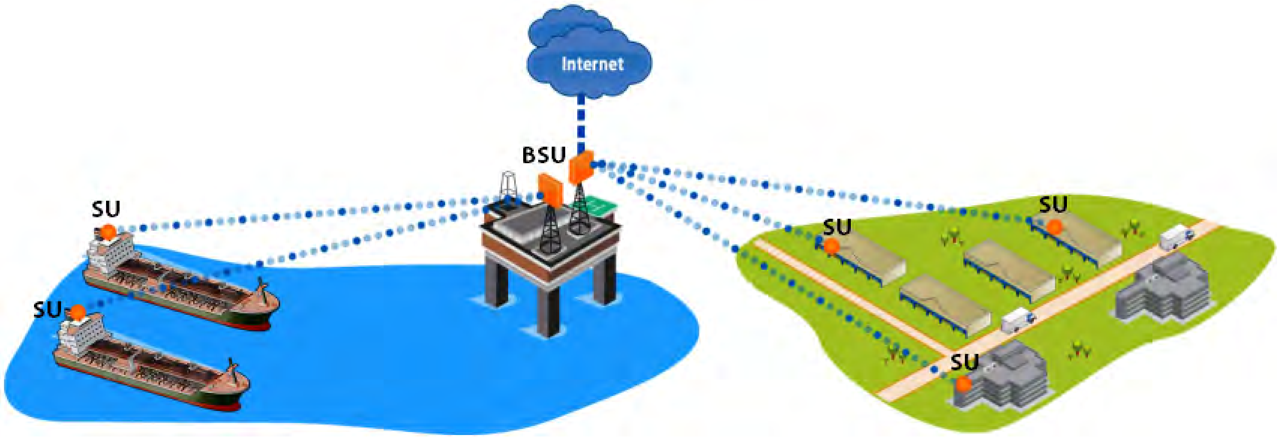


- **Wireless Intelligent Transport System (ITS)**: Increases the traffic efficiency and reduces the commuting time in cities and metropolitan areas.



- **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.

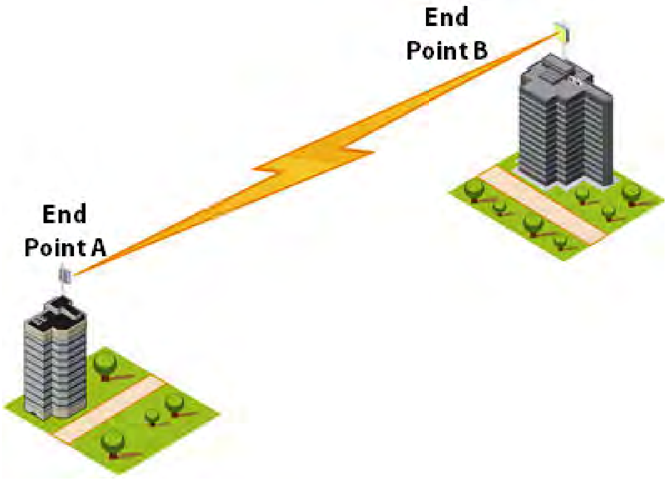


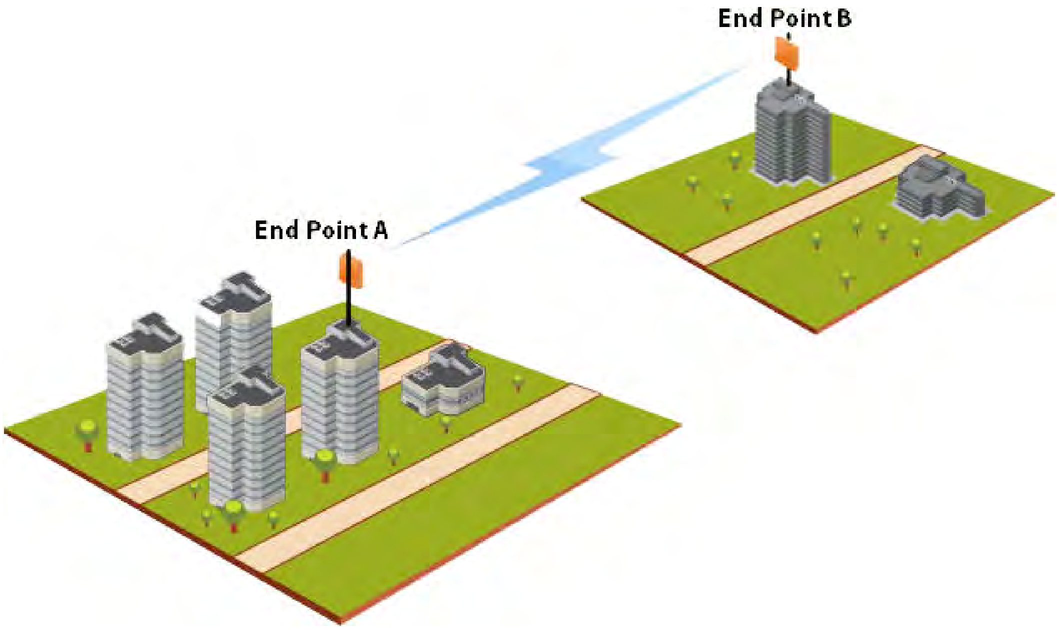
Figure 1-1 Point-to-Point-Link (An Example)

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:

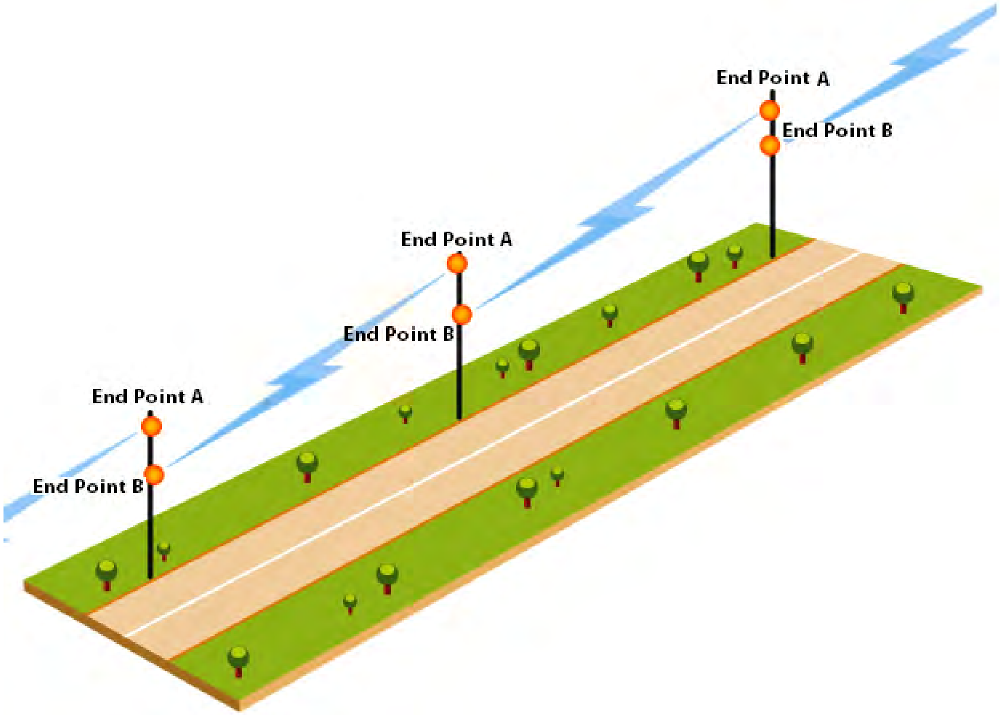
End Point A	End Point B
QB-8200-EPA-G/QB-8200-EPA	QB-8200-EPA-G/QB-8200-EPA
QB-8250-EPR-G/QB-8250-EPR	QB-8250-EPR-G/QB-8250-EPR
QB-825-EPR-50+	QB-825-EPR-50+
QB-825-EPR-100	QB-825-EPR-100
QB-835-EPR-25	QB-835-EPR-25
QB-835-EPR-50	QB-835-EPR-50
QB-826-EPR-100	QB-826-EPR-100

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

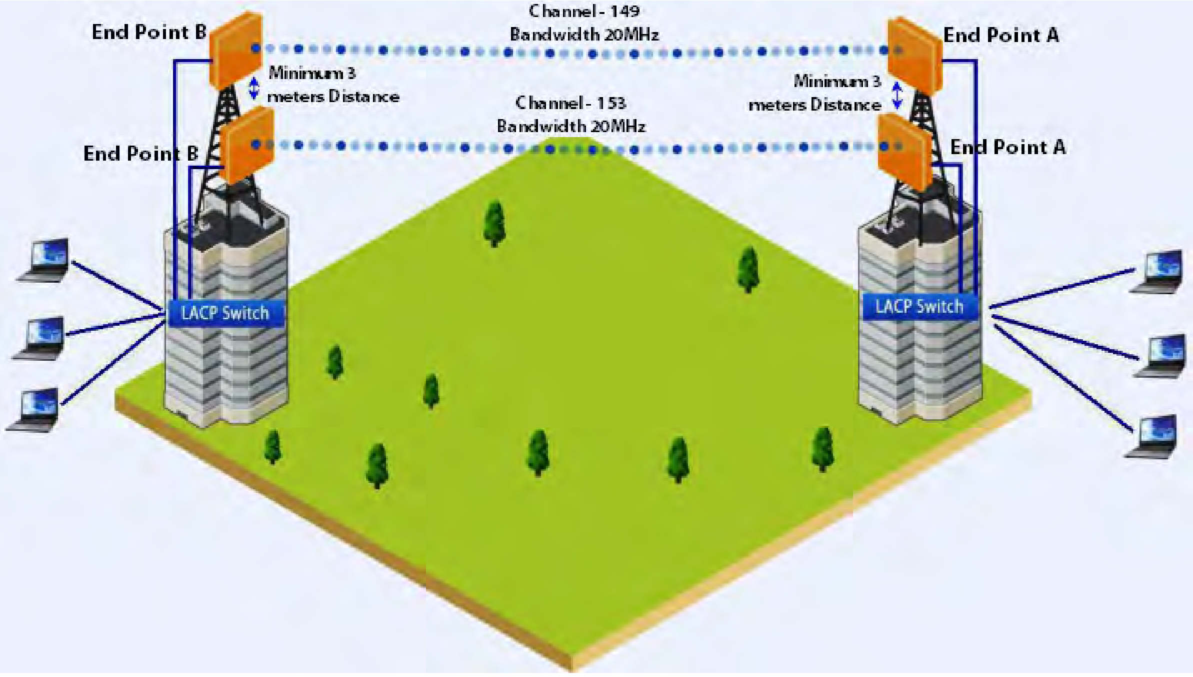
- **Backhaul to a Central POP**: Avoids expensive installation and recurring charge of a second wireline backhaul to a remote virtual POP.



- **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-8200-EPA-G/LNK-G, and QB-8250-EPR-G/LNK-G 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 Contro**l: 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 2

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
- PV Advanced

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 PV Advanced

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

PV Advanced 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 PV Advanced 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 3

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-8250-LNK-G/QB-8250-LNK, 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-825-CPE-50, MP-825-CPE-100, MP-835-CPE-10, MP-835-CPE-25, MP-835-CPE-50, MP-835-CPE-100 and QB-826-EPR/LNK-100 devices 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

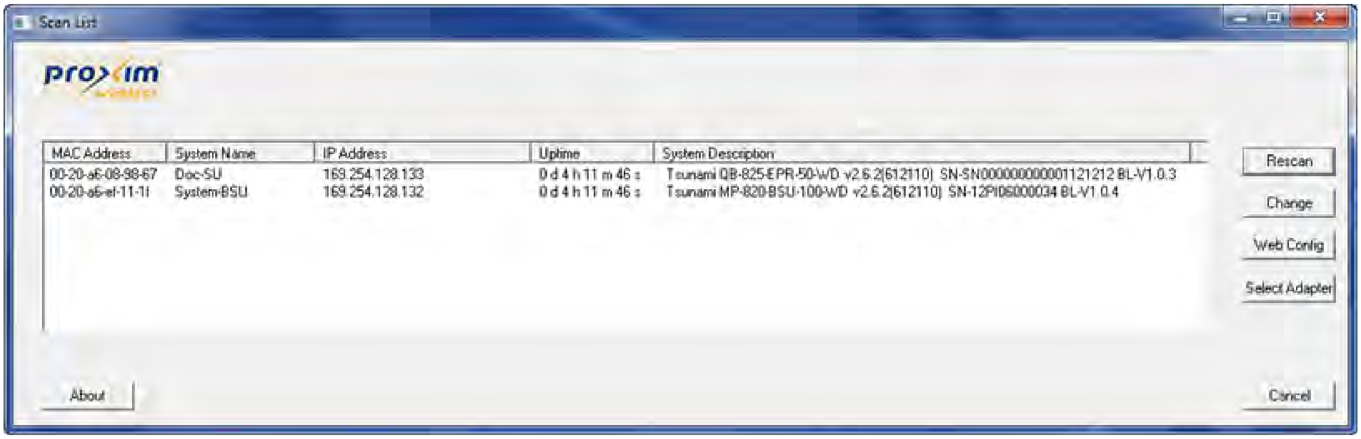
:

- *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

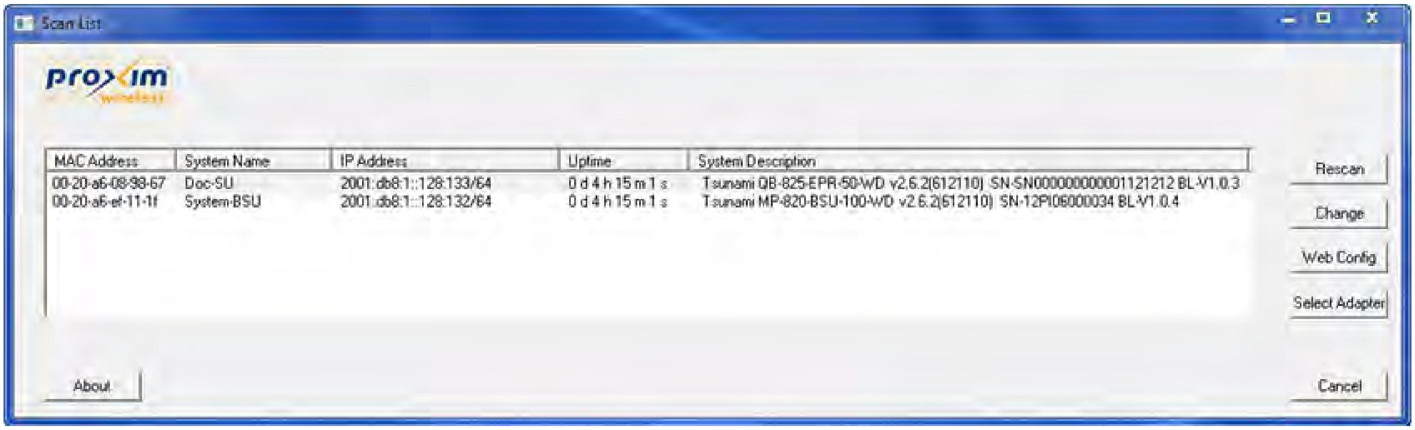
To scan and locate the devices on a network by using ScanTool, do the following:

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 an Ethernet adapter. Select an adapter and click **OK**. The following **Scan List** screen appears, which displays all devices that are connected to the selected adapter.



MAC Address	System Name	IP Address	Uptime	System Description
00-20-a6-08-98-67	Doc-SU	169.254.128.133	0 d 4 h 11 m 46 s	Tsunami QB-825-EPR-50-WD v2.6.2(612110) SN-SN0000000000001121212 BL-V1.0.3
00-20-a6-ef-11-1f	System-BSU	169.254.128.132	0 d 4 h 11 m 46 s	Tsunami MP-820-BSU-100-WD v2.6.2(612110) SN-12PI06000034 BL-V1.0.4

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



MAC Address	System Name	IP Address	Uptime	System Description
00-20-a6-08-98-67	Doc-SU	2001:db8:1::128:133/64	0 d 4 h 15 m 1 s	Tsunami QB-825-EPR-50-WD v2.6.2(612110) SN-SN0000000000001121212 BL-V1.0.3
00-20-a6-ef-11-1f	System-BSU	2001:db8:1::128:132/64	0 d 4 h 15 m 1 s	Tsunami MP-820-BSU-100-WD v2.6.2(612110) SN-12PI06000034 BL-V1.0.4

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

This screen contains the following device information:

- **MAC Address**

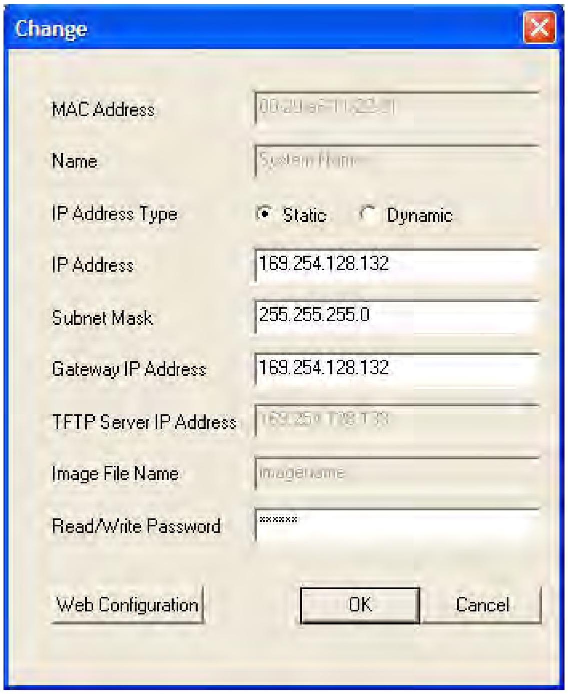
- **System Name**
- **IP Address**
- **Uptime**
- **System Description:** The system description comprises the following information:
  - — **Device Description:** For example, MP-820-BSU-100-WD
  - — **Firmware Version:** 2.X.Y; For example, version 2.6.2
  - — **Serial Number :** For example, SN-12PI06000034
  - — **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

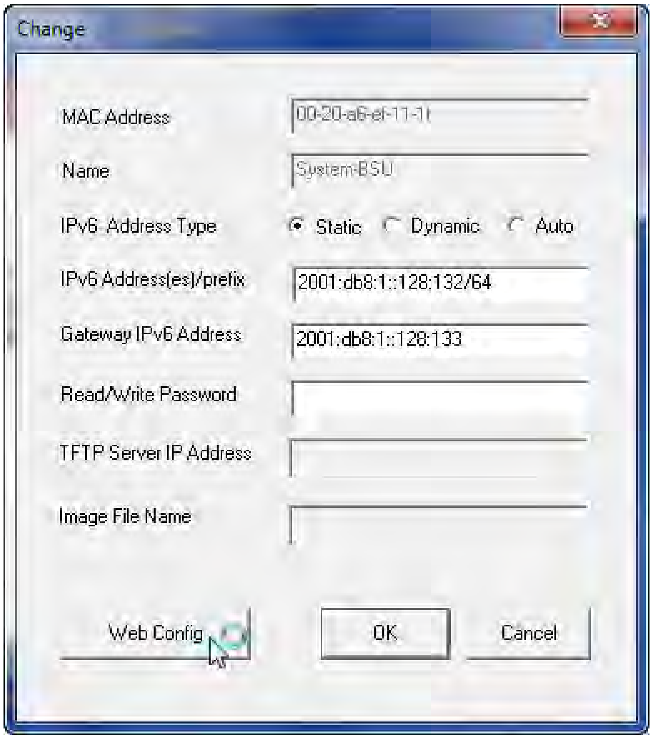
To modify the IP address of a device by using ScanTool, select the device from the scan list and click **Change**. A **Change** screen appears as shown in the following screen. The system automatically populates the **MAC Address**, **System Name**, **TFTP Server IP Address** and **Image File Name**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



Change

MAC Address	00-20-a6-11-22-31
Name	System Name
IP Address Type	● Static ○ Dynamic
IP Address	169.254.128.132
Subnet Mask	255.255.255.0
Gateway IP Address	169.254.128.132
TFTP Server IP Address	169.254.128.133
Image File Name	imagename
Read/Write Password	******

Figure 3-3 Modifying Device's IP Address (IPv4)



MAC Address: 00-20-a6-ef-11-1

Name: System-BSU

IPv6 Address Type: ● Static ○ Dynamic ○ Auto

IPv6 Address(es)/prefix: 2001:db8:1::128:132/64

Gateway IPv6 Address: 2001:db8:1::128:133

Read/Write Password:

TFTP Server IP Address:

Image File Name:

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.

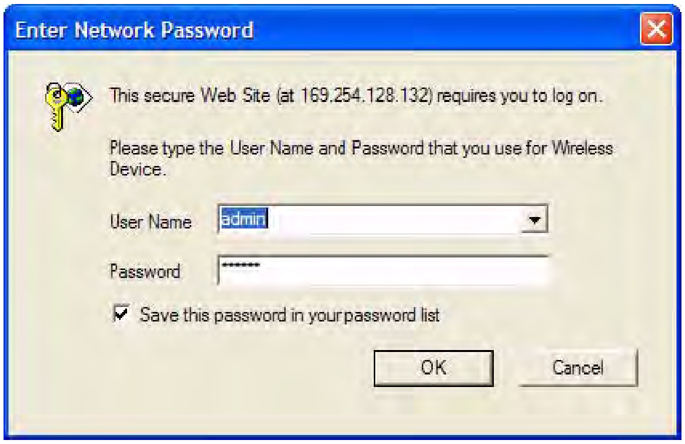
To log on to the Web Interface, click **Web Configuration**.

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.



Enter Network Password

This secure Web Site (at 169.254.128.132) requires you to log on.

Please type the User Name and Password that you use for Wireless Device.

User Name: admin

Password: *******

☑ Save this password in your password list

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.

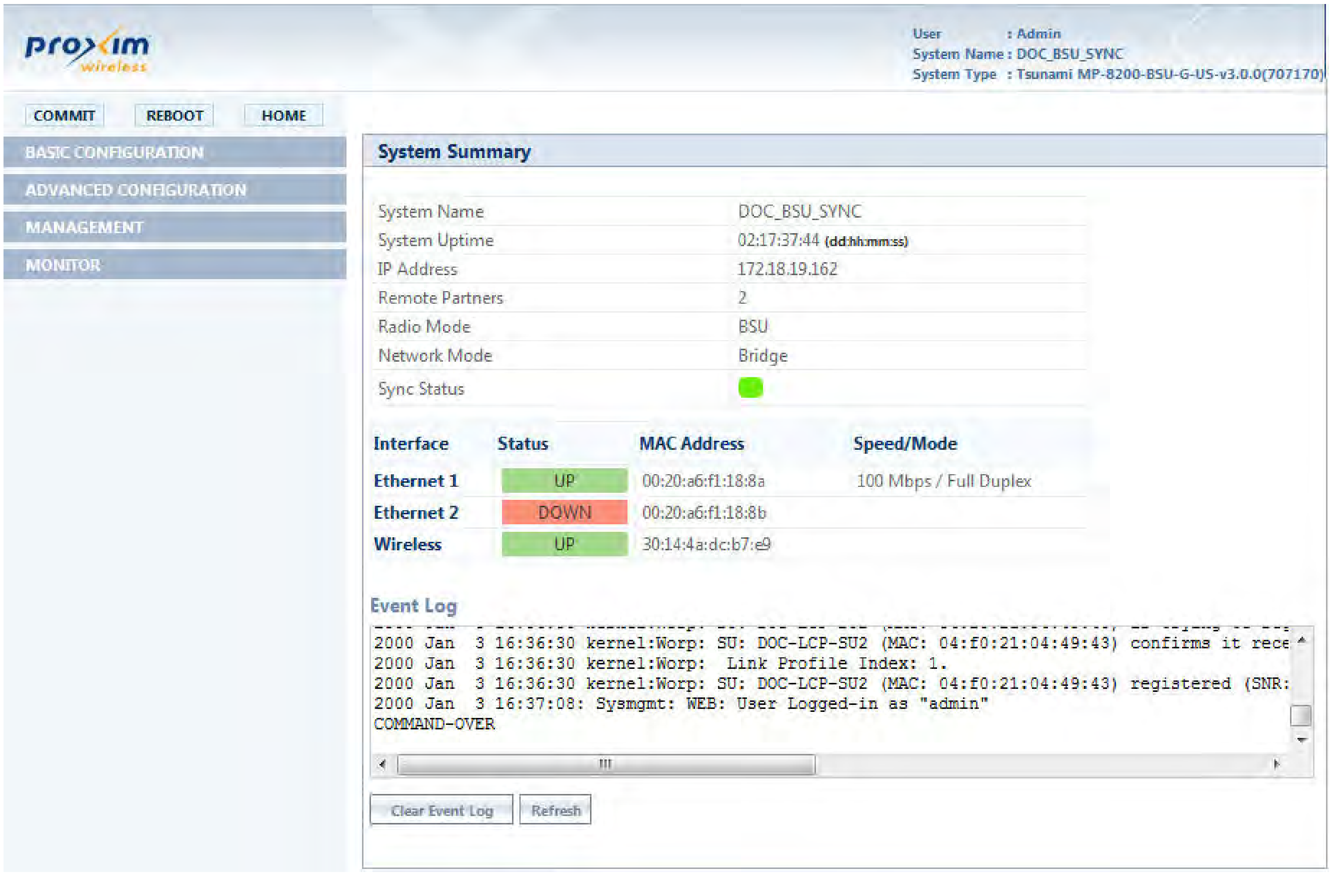
:

- *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**".*

- *For QB-8xx products, three types of user can access the device;* ***Administrator****,* ***Monitor*** *and* ***Advanced****. Refer 'Tsunami Quickbridge® 800 Series User Guide' available at http://my.proxim.com for more details.*

3.2.1 Home Page

Upon successful logon, the device home page appears.



User : Admin
System Name : DOC_BSU_SYNC
System Type : Tsunami MP-8200-BSU-G-US-v3.0.0(707170)

System Summary

System Name	DOC_BSU_SYNC
System Uptime	02:17:37:44 (dd:hh:mm:ss)
IP Address	172.18.19.162
Remote Partners	2
Radio Mode	BSU
Network Mode	Bridge
Sync Status	🟩

Interface	Status	MAC Address	Speed/Mode
Ethernet 1	UP	00:20:a6:f1:18:8a	100 Mbps / Full Duplex
Ethernet 2	DOWN	00:20:a6:f1:18:8b	
Wireless	UP	30:14:4a:dc:b7:e9	

Event Log

```
2000 Jan  3 16:36:30 kernel:Worp: SU: DOC-LCP-SU2 (MAC: 04:f0:21:04:49:43) confirms it rece
2000 Jan  3 16:36:30 kernel:Worp:  Link Profile Index: 1.
2000 Jan  3 16:36:30 kernel:Worp: SU: DOC-LCP-SU2 (MAC: 04:f0:21:04:49:43) registered (SNR:
2000 Jan  3 16:37:08: Sysmgmt: WEB: User Logged-in as "admin"
COMMAND-OVER
```

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, Sync Status, and so on.
  - **Sync Status**: The glowing LED in this field displays the Sync status. The LED behavior for Sync mode is tabulated below:

Sync LED Behavior	Sync Status
OFF (Grey)	Synchronous mode is disabled or the device is out of Sync
Blinking (Green-Fast)	Synchronous mode is enabled, but Sync signal is not received
ON (Solid-Green)	Synchronous mode is enabled and Sync signal is received

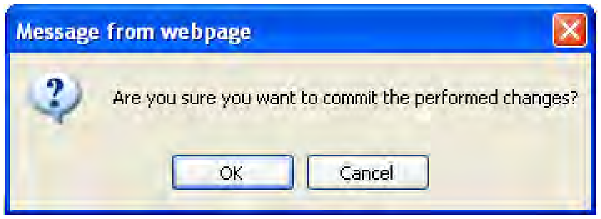
- **COMMIT Button**: See COMMIT

- **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:

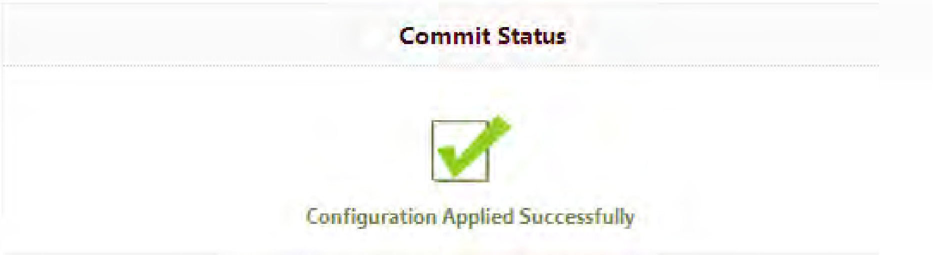


Are you sure you want to commit the performed changes?

Figure 3-7 Commit

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

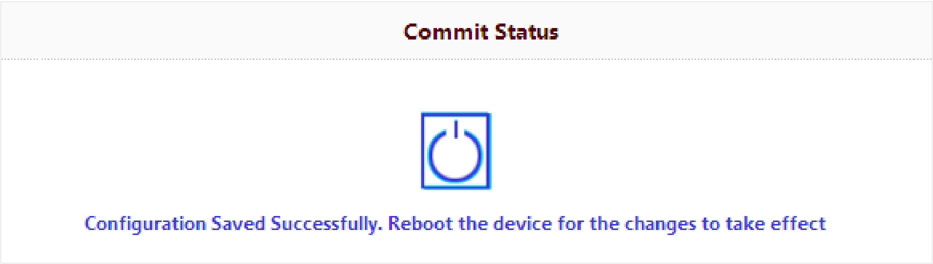
On successful **COMMIT** operation, the following screen appears:


Commit Status

Configuration Applied Successfully

Figure 3-8 Commit Status

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


Commit Status

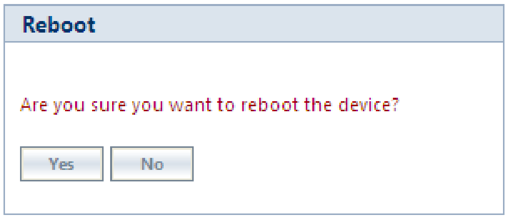
Configuration Saved Successfully. Reboot the device for the changes to take effect

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.



Reboot

Are you sure you want to reboot the device?

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	169.254.128.131
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-8200-BSU-G/ MP-8200-BSU --> 250 MP-8250-BS9-G/ MP-8250-BS9 --> 250 MP-8250-BS1-G/ MP-8250-BS1--> 250 MP-820-BSU-100 -->32 MP-822-BSU-100 -->32 MP-825-BS3-100 -->32	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
IGMP Snooping	Disabled	Disabled

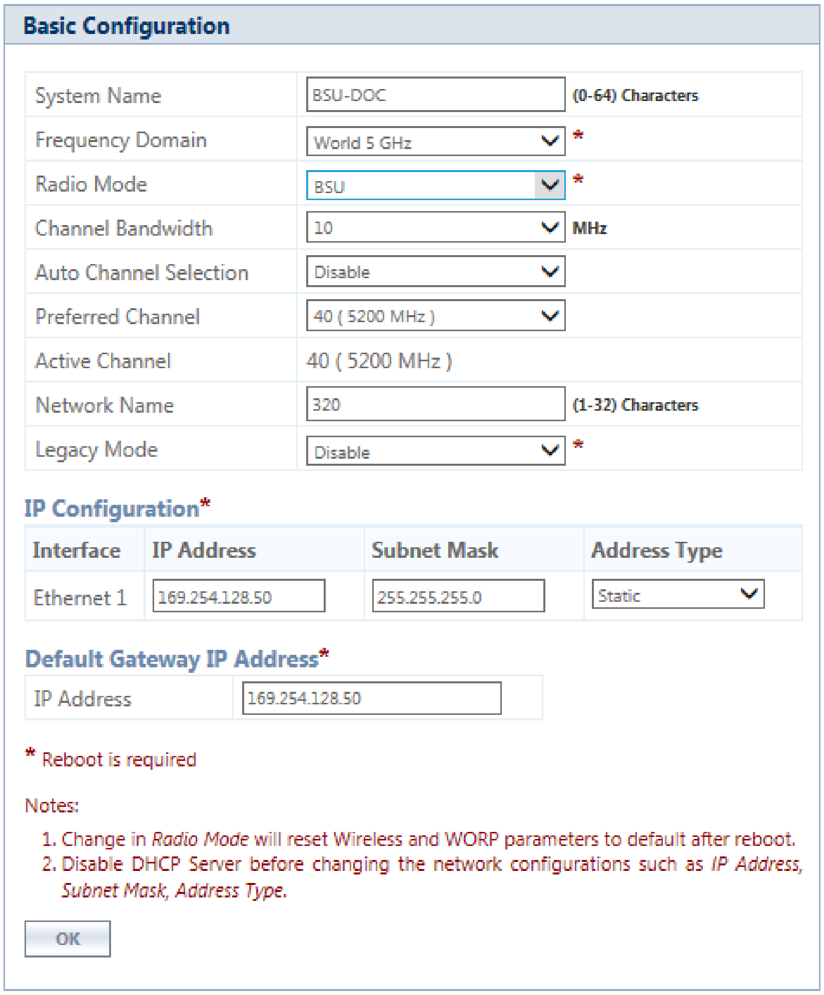
Parameter	BSU Mode/ End Point A	SU Mode/ End Point B
RIP	Disabled	Disabled
NAT	Disabled	Disabled
PPPoE Client	Not Applicable	Disabled in SU Mode Not Applicable in End Point B
HTTP Management Interface	Enabled	Enabled
Telnet Management Interface	Enabled	Enabled
SNMP Management Interface	Enabled with SNMPv1-v2c	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

4

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	BSU-DOC	(0-64) Characters
Frequency Domain	World 5 GHz	*
Radio Mode	BSU	*
Channel Bandwidth	10	MHz
Auto Channel Selection	Disable	
Preferred Channel	40 (5200 MHz)	
Active Channel	40 (5200 MHz)	
Network Name	320	(1-32) Characters
Legacy Mode	Disable	*

IP Configuration*

Interface	IP Address	Subnet Mask	Address Type
Ethernet 1	169.254.128.50	255.255.255.0	Static

Default Gateway IP Address*

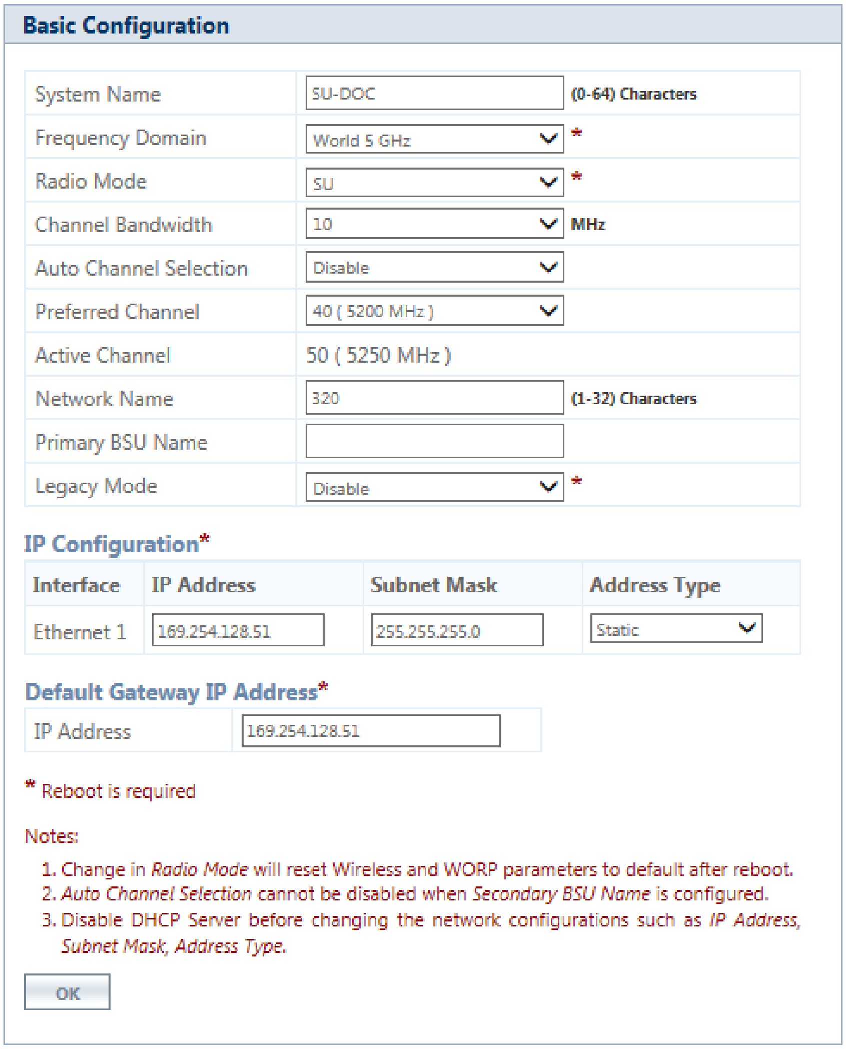
IP Address	169.254.128.50

* Reboot is required

Notes:

1. Change in *Radio Mode* will reset Wireless and WORP parameters to default after reboot.
2. Disable DHCP Server before changing the network configurations such as *IP Address, Subnet Mask, Address Type.*

Figure 4-1 Basic Configuration (BSU)



Basic Configuration

System Name	SU-DOC	(0-64) Characters
Frequency Domain	World 5 GHz	*
Radio Mode	SU	*
Channel Bandwidth	10	MHz
Auto Channel Selection	Disable	
Preferred Channel	40 (5200 MHz)	
Active Channel	50 (5250 MHz)	
Network Name	320	(1-32) Characters
Primary BSU Name		
Legacy Mode	Disable	*

IP Configuration*

Interface	IP Address	Subnet Mask	Address Type
Ethernet 1	169.254.128.51	255.255.255.0	Static

Default Gateway IP Address*

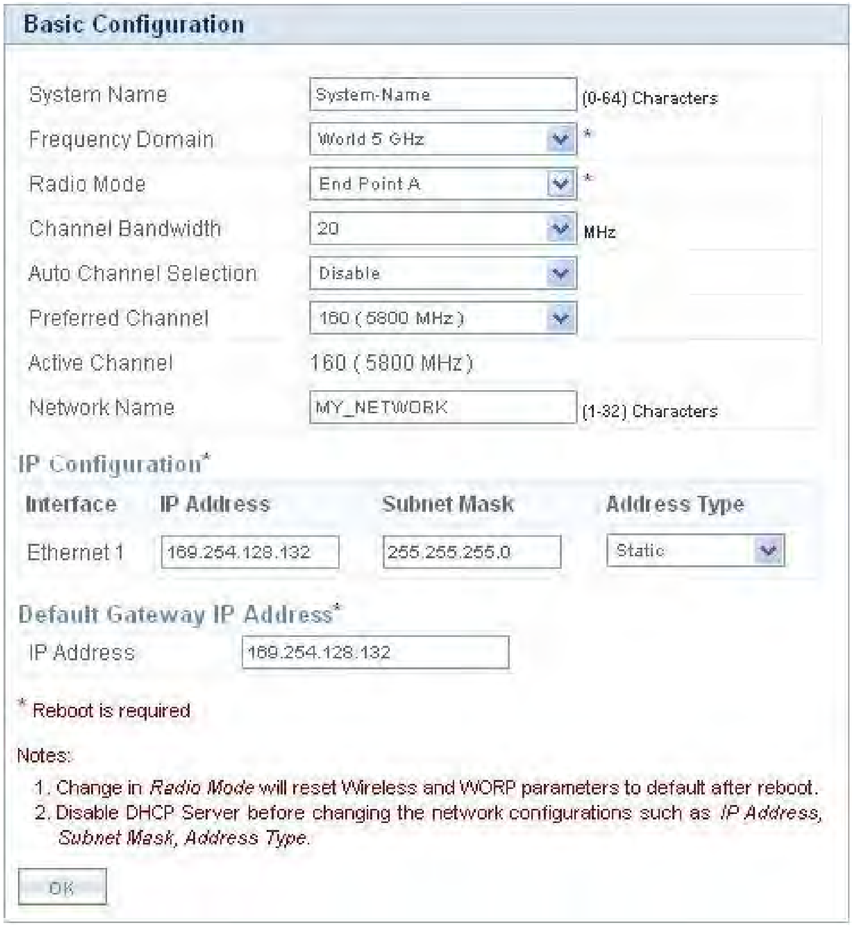
IP Address	169.254.128.51

* 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	System-Name	(0-64) Characters
Frequency Domain	World 5 GHz	*
Radio Mode	End Point A	*
Channel Bandwidth	20	MHz
Auto Channel Selection	Disable	
Preferred Channel	160 (5800 MHz)	
Active Channel	160 (5800 MHz)	
Network Name	MY_NETWORK	(1-32) Characters

IP Configuration*

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

Default Gateway IP Address*

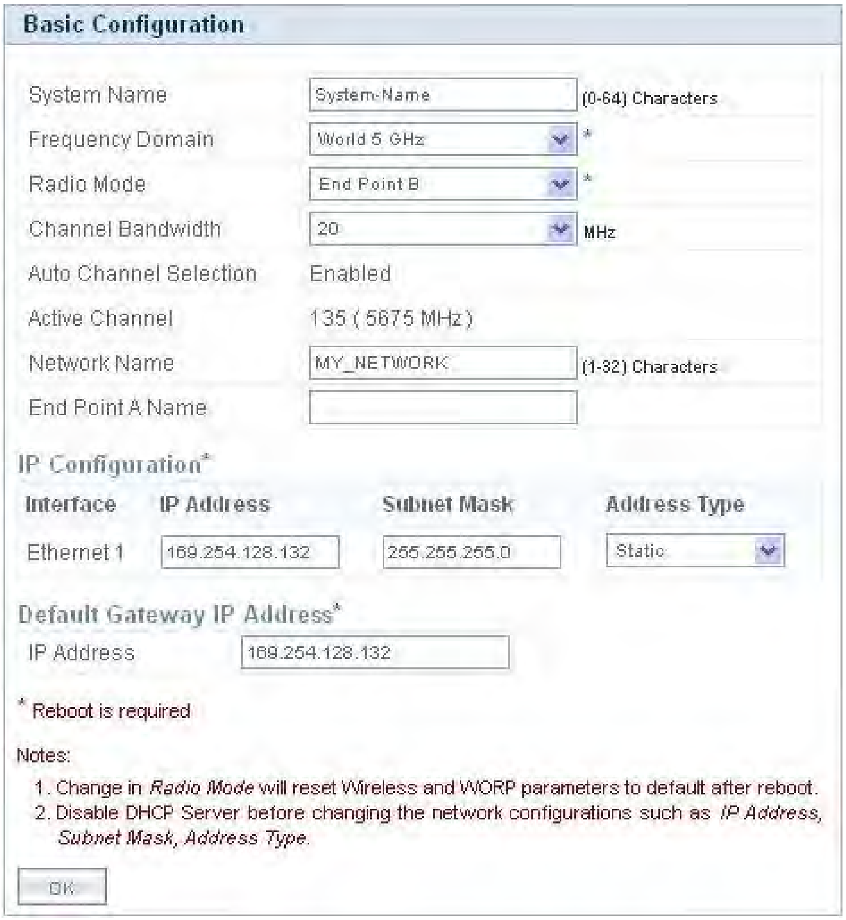
IP Address 169.254.128.132

* Reboot is required

Notes:

1. Change in *Radio Mode* will reset Wireless and WORP parameters to default after reboot.
2. Disable DHCP Server before changing the network configurations such as *IP Address, Subnet Mask, Address Type.*

Figure 4-3 Basic Configuration (End Point A)



Basic Configuration

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

Frequency Domain: World 5 GHz *

Radio Mode: End Point B *

Channel Bandwidth: 20 MHz

Auto Channel Selection: Enabled

Active Channel: 135 (5675 MHz)

Network Name: MY_NETWORK (1-32) Characters

End Point A Name:

IP Configuration*

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

Default Gateway IP Address*

IP Address: 169.254.128.132

* Reboot is required

Notes:

1. Change in *Radio Mode* will reset Wireless and WORP parameters to default after reboot.
2. Disable DHCP Server before changing the network configurations such as *IP Address, Subnet Mask, Address Type*.

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

Parameter	Description
Frequency Domain	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. : • 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. — 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. For non-US device, the default frequency domain selected is World 5MHz. For more details on frequency domains, see Frequency Domains and Channels.
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. : *A change in radio mode will reset wireless and WORP parameters to defaults after reboot.*
Channel Bandwidth	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. : *The 40 MHz frequency band is not applicable to MP 800 & 8000 BSU and SU devices, when configured in Legacy Mode.* For more details on supported Channel Bandwidth, see Frequency Domains and Channels.

Parameter	Description
Auto Channel Selection (ACS)	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. : *Irrespective of the ACS status, the BSU/End Point A will automatically select a new channel upon radar detection.*
Preferred Channel	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.
Active Channel	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.
Network Name	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**. : *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.*
Primary BSU Name	Applicable only to an SU. 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.
End Point A Name	Applicable only to an End Point B. 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.

Parameter	Description
Legacy Mode	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. The MP 800 & 8000 clients that provide legacy support are, • MP-8100-SUA • MP-8150-SUR • MP-8150-SUR-100 • MP-8200-SUA • MP-8250-SUR • MP-820-SUA-50^{+} • MP-820-SUA-100 • MP-822-SUA-100 • MP-825-SUR-50^{+} • MP-825-SUR-100 • MP-825-CPE-50 • MP-825-CPE-100 • MP-835-CPE-10 • MP-835-CPE-25 • MP-835-CPE-50 • MP-835-CPE-100 : *MP 800/8000 BSU device in legacy mode can connect to a MP 800/8000 SU device only when configured in legacy mode.*
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 5

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

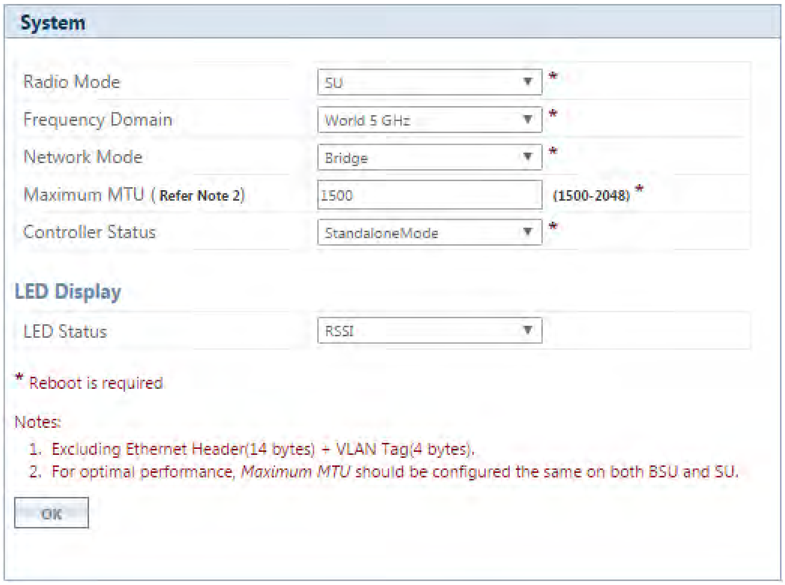
- System
- Network
- Ethernet
- Wireless
- Security
- Quality of Service (QoS)
- RADIUS Based SU QoS Configuration
- VLAN (Bridge Mode Only)
- RADIUS Based SU VLAN Configuration
- Filtering (Bridge Only)
- DHCP
- IGMP Snooping

> ❗ ***: 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:



System

Radio Mode: SU *

Frequency Domain: World 5 GHz *

Network Mode: Bridge *

Maximum MTU (Refer Note 2): 1500 (1500-2048) *

Controller Status: StandaloneMode *

LED Display

LED Status: RSSI

* 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.

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.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Maximum MTU (Maximum Transmission Unit)</td><td>
Given below are the devices and their corresponding MTU configurable range:
<table>
<tr><th>Devices</th><th>MTU Configurable Range</th></tr>
<tr><td>MP-820-SUA-100; MP-820-SUA-50^{+}
MP-822-SUA-100
MP-825-SUR-50^{+}; MP-825-SUR-100
MP-825-CPE-50; MP-825-CPE-100
MP-835-CPE-10; MP-835-CPE-25;
MP-835-CPE-50; MP-835-CPE-100;
MP-820-BSU-100, MP-825-BS3-100
MP-822-BSU-100;QB-825-EPR/LNK-50^{+}
QB-825-EPR/LNK-100;
QB-835-EPR/LNK-25;
QB-835-EPR/LNK-50
QB-826-EPR/LNK-100</td><td>1500 to 2048 bytes</td></tr>
<tr><td>MP-8100-SUA; MP-8150-SUR
MP-8150-SUR-100; MP-8200-BSU-G
MP-8200-SUA; MP-8250-BS9/BS1-G
MP-8200-BSU; MP-8250-BS9; MP-8250-BS1
MP-8250-SUR; QB-8200-EPA-G/LNK-G
QB-8250-EPR-G/LNK-G;
QB-8200-EPA/LNK; QB-8250-EPR/LNK;</td><td>1500 to 1514 bytes</td></tr>
</table>
Maximum Frame Size = Configured MTU + Ethernet Header (14 bytes) + VLAN Header (4 bytes) + Frame Check Sequence (4 bytes)
Maximum Payload = Configured MTU – Feature Header
<table>
<tr><th rowspan="2">Feature</th><th rowspan="2">Feature Header (in bytes)</th><th colspan="2">Maximum Payload (in Bytes)</th></tr>
<tr><th>#
MP-8200-BSU-G
MP-8250-BS9/BS1-G
MP-8200-BSU
MP-8250-BS9/BS1
MP-8100-SUA
MP-8150-SUR
MP-8150-SUR-100
MP-8200-SUA
MP-8250-SUR
QB-8200-EPA-G/LNK-G
QB-8250-EPR-G/LNK-G
QB-8200-EPA/LNK
QB-8250-EPR/LNK</th><th>*
MP-820-SUA-50^{+}
MP-820-SUA-100
MP-822-SUA-100
MP-825-SUR-50^{+}
MP-825-SUR-100
MP-825-CPE-50
MP-825-CPE-100
MP-835-CPE-10
MP-835-CPE-25
MP-835-CPE-50
MP-835-CPE-100
MP-820-BSU-100
MP-822-BSU-100
MP-825-BS3-100
QB-825-EPR/LNK-50^{+}
QB-825-EPR/LNK-100
QB-835-EPR/LNK-25
QB-835-EPR/LNK-50
QB-826-EPR/LNK-100</th></tr>
<tr><td>General or Single VLAN</td><td>0</td><td>1514</td><td>2048</td></tr>
<tr><td>QinQ</td><td>4</td><td>1510</td><td>2044</td></tr>
<tr><td>PPPoE</td><td>8</td><td>1506</td><td>2040</td></tr>
<tr><td>IP Tunneling (IP in IP Encapsulation)</td><td>20</td><td>1494</td><td>2028</td></tr>
<tr><td>IP Tunneling (GRE Encapsulation)</td><td>24</td><td>1490</td><td>2024</td></tr>
</table>
</td></tr>
</table>

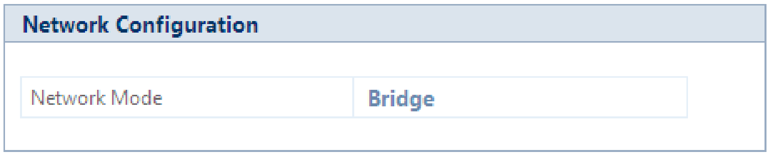
Parameter	Description
	# Assuming that MTU is configured as 1514 ** Assuming that MTU is configured as 2048* For optimal performance, MTU should be configured same on both the ends.
Controller Status	This feature helps the user to manage the device through ProximVision™ Advanced controller which automatically updates the device with the latest firmware, if device is using old firmware. By default, controller status is set to **Standalone Mode**. When set to **Controller Mode**, the device automatically discovers the controller and establishes a secure communication through two-way authentication. : • *Not Applicable to MP-8200-BSU-G; MP-8250-BS9-G; MP-8250-BS1-G; MP-8200-BSU; MP-8250-BS9; MP-8250-BS1; MP-8100-SUA; MP-8150-SUR; MP-8150-SUR-100; MP-8200-SUA; MP-8250-SUR; QB-8200-EPA-G/LNK-G; QB-8250-EPR-G/LNK-G; QB-8200-EPA/LNK and QB-8250-EPR/LNK devices.* • *Controller feature should be enabled in ProximVision™ Advanced also.* • *Appicable only when the device is in Bridge Network Mode.*
LED Status	The configurable options: **Disable**, **RSSI**, and **Sync**. • By default, it is set to **RSSI**. The Received Signal Strength Indicator (RSSI) LEDs indicates that the unit is powered on, and LEDs will glow based on the RSSI value indicating link status. By default, all 5 LEDs will blink at an interval of 1 sec. • If the LED Status is disabled, all LEDs will be turned off. • If it is set to Sync, the third LED behavior of the scaling mask will indicate the Sync status. *: LED Status is applicable only to **82x** MP and QB devices.*
SU Wireless MAC Address	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** > **WORP Statistics** >**Interface 1** > **SU Link Statistics**.

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

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:

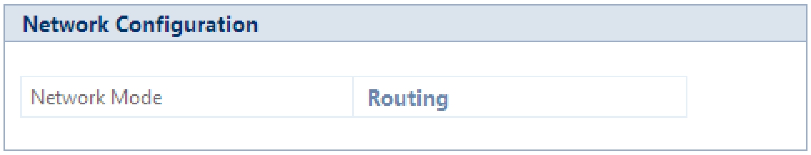


Network Configuration

Network Mode	Bridge

Figure 5-2 Bridge Mode

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



Network Configuration

Network Mode	Routing

Figure 5-3 Routing Mode

5.2.1 IP Configuration

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

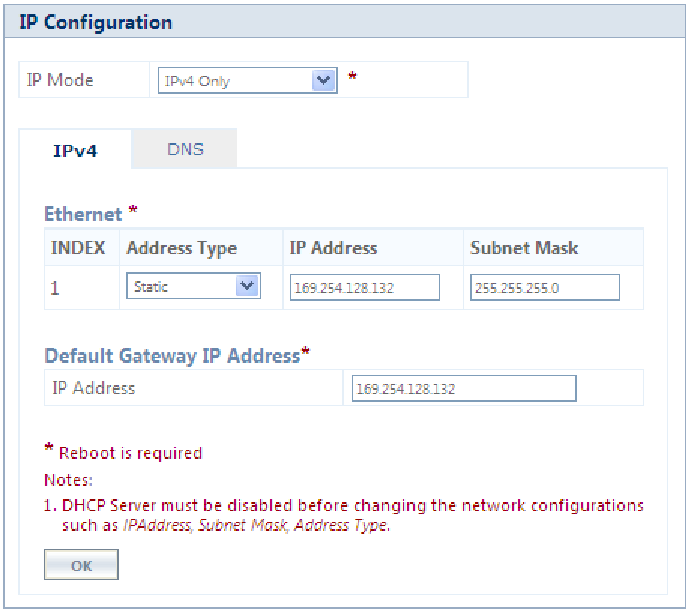
- **IPv4**: IPv4 is the widely used version of Internet Protocol defining the IP address in 32-bit in size.
- **IPv6**: Ipv6 is the latest version of Internet Protocol with new addressing system for more IP addresses than IPv4. The IPv6 address is 128-bit in size.

: 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:



IP Configuration

IP Mode	IPv4 Only *

Ethernet *

INDEX	Address Type	IP Address	Subnet Mask
1	Static	169.254.128.132	255.255.255.0

Default Gateway IP Address*

IP Address	169.254.128.132

* Reboot is required

Notes:

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

Figure 5-4 IPv4 Configuration (Bridge Mode)

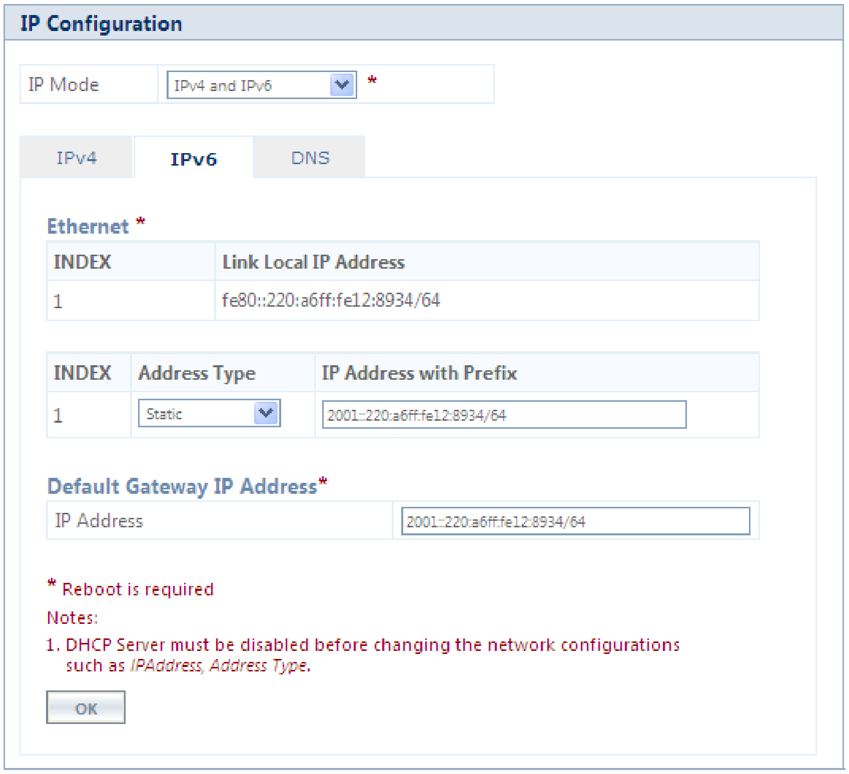
Given below is the table which explains the method to configure IP parameters in Bridge mode:

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.)*	
Address Type	Specifies whether the Ethernet interface parameters are to be configured through Dynamic Host Configuration Protocol (DHCP) or to be assigned statically. 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**.
IP Address	Represents the IP address of the Ethernet interface. 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.
Subnet Mask	Represents the subnet mask of the Ethernet interface. 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.
Default Gateway IP Address	
IP Address	Represents the gateway IP address of the device. 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.

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 *

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 *IPAddress, Address Type*.

Figure 5-5 IPv6 Configuration (Bridge Mode)

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

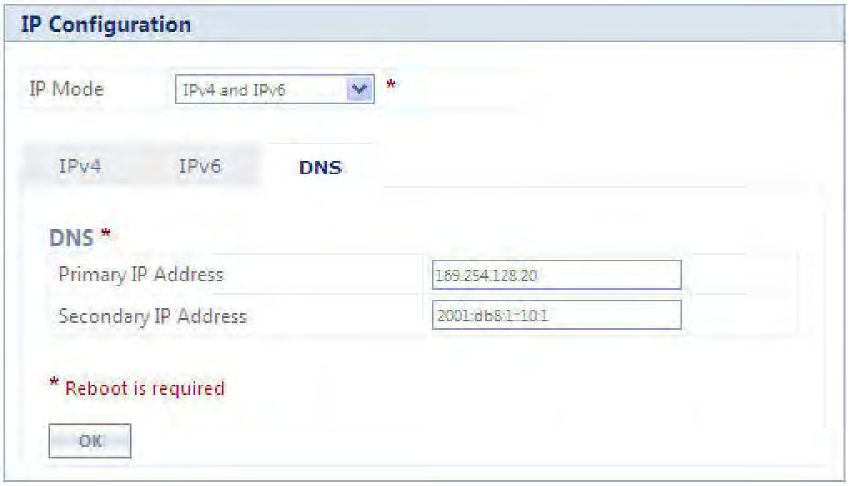
Parameter	Description
IP Mode	Represents the IP Mode of the device. The IP Mode can be set to either **IPv4 Only** or Dual (**IPv4 and IPv6**). By default, the IP Mode is set to **IPv4 Only**. *: A change in IP mode requires device reboot.*
Ethernet (*Please note that the number of Ethernet interfaces 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	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. 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. Select **Static** to configure the device manually. If **Static** is selected, the user should manually configure the network parameters. 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.
IP Address with Prefix	Represents the IP address of the Ethernet interface. For Example: The IP address is represented as 2000::220:a6ff:fe00:1/64, where "/64" is called the IP prefix or network prefix. 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. 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. When the address type is set to **Static**, the IPv6 address should be manually configured along with prefix.
Default Gateway IP Address	
IP Address	Represents the gateway IP address of the device. 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. When the address type is set to **Static**, the gateway IP address should be manually configured (prefix is not required). 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.

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 Mode: IPv4 and IPv6 *

DNS *

Primary IP Address: 169.254.128.20

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

* Reboot is required

Figure 5-6 DNS Configuration (Bridge Mode)

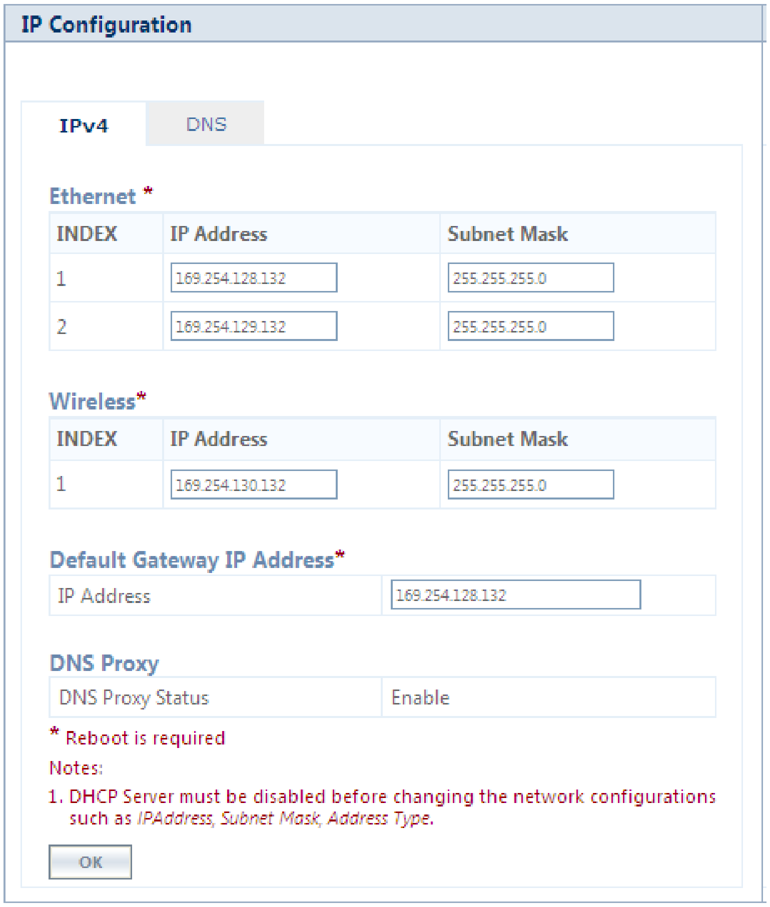
Parameter	Description
Primary and Secondary IP Address	Represents the IP address of the Primary and Secondary DNS Server. Primary and Secondary IP Address can be configured manually irrespective of the IP mode. The DNS address obtained from the DHCP server (Dynamic mode) or from the router advertisement (Auto Mode) is given preference over the manually configured IP Addresses. 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. *: IPv4 addresses will be given preference over IPv6 addresses.*

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

Ethernet *

INDEX	IP Address	Subnet Mask
1	169.254.128.132	255.255.255.0
2	169.254.129.132	255.255.255.0

Wireless*

INDEX	IP Address	Subnet Mask
1	169.254.130.132	255.255.255.0

Default Gateway IP Address*

IP Address	169.254.128.132

DNS Proxy

DNS Proxy Status	Enable

* Reboot is required

Notes:

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

Figure 5-7 IP Configuration (Routing Mode)

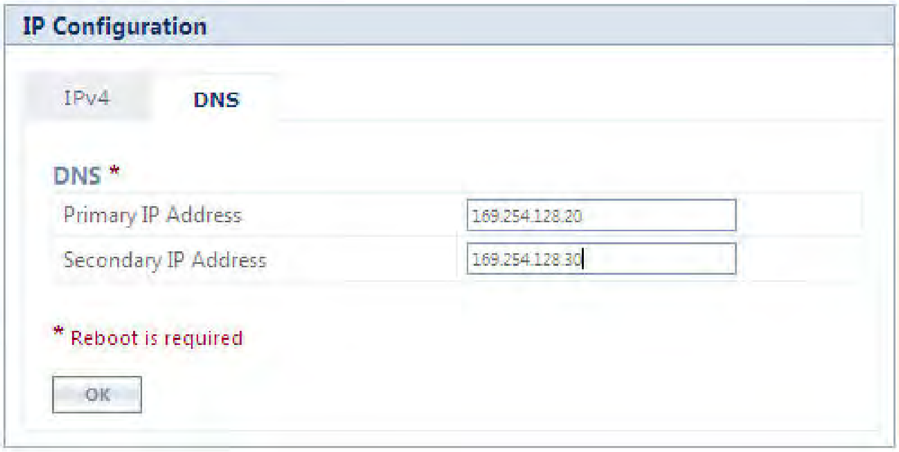
Given below is the table which explains the method to configure IP parameters in Routing mode:

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. : • *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

DNS *

Primary IP Address: 169.254.128.20

Secondary IP Address: 169.254.128.30

* Reboot is required

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**.

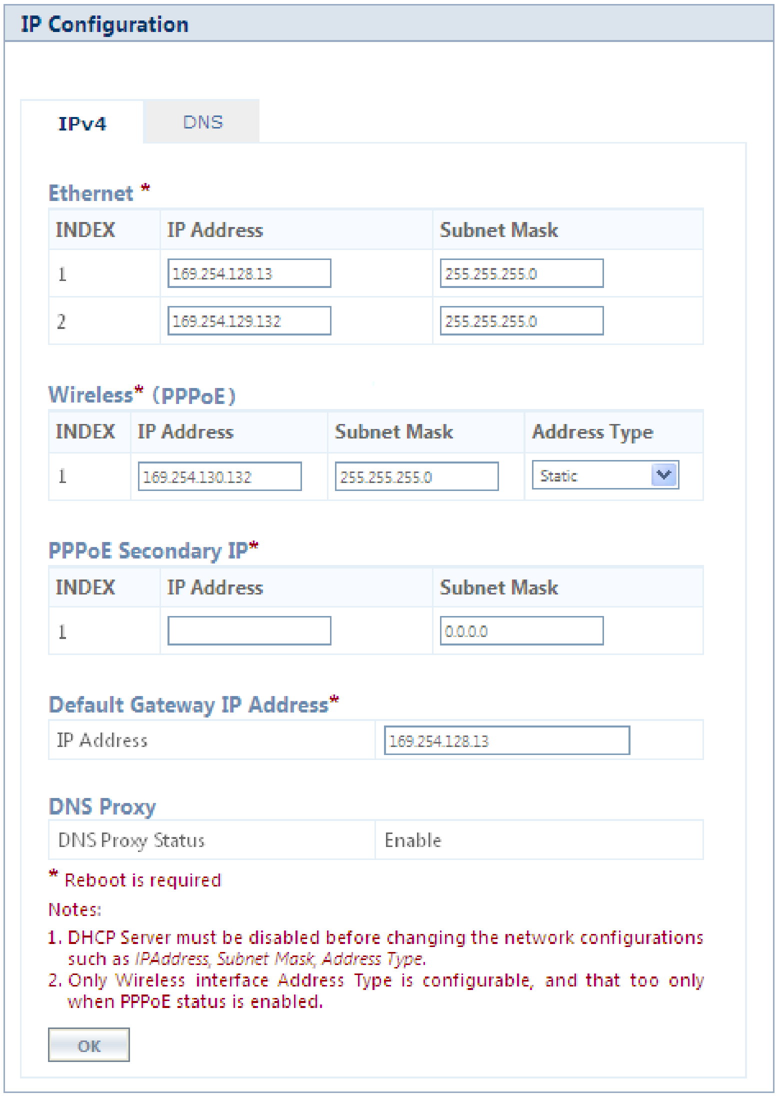
:

- *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

Ethernet *

INDEX	IP Address	Subnet Mask
1	169.254.128.13	255.255.255.0
2	169.254.129.132	255.255.255.0

Wireless* (PPPoE)

INDEX	IP Address	Subnet Mask	Address Type
1	169.254.130.132	255.255.255.0	Static

PPPoE Secondary IP*

INDEX	IP Address	Subnet Mask
1		0.0.0.0

Default Gateway IP Address*

IP Address	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 *IPAddress, 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:

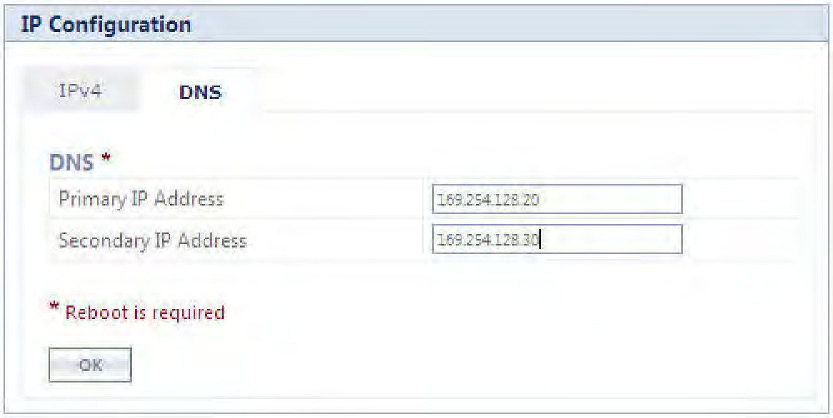
Parameter	Description
Ethernet (Please note that the number of Ethernet interfaces depend on your device.)	
IP Address	Represents the IP address of the Ethernet interface. By default, the static IP address for Ethernet1 is set to 169.254.128.132 and 169.254.129.132 for Ethernet2. You can manually change 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	This parameter specifies whether the wireless interface parameters are to be configured through PPPoE server or to be assigned statically. 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**.
IP Address	Represents the Primary IP address of the wireless interface. 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. 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.
Subnet Mask	Represents the subnet mask of the wireless interface. 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. 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.
PPPoE Secondary IP	
IP Address	Represents the Secondary IP address of the wireless interface. 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. Configure Secondary IP address manually. When PPPoE is disabled, the Secondary IP address is not applicable.
Subnet Mask	Represents the subnet mask of the Secondary IP address. 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.
Default Gateway IP Address	
IP Address	Represents the gateway IP address of the device. 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. 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.

Parameter	Description
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. : • *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:



DNS *

Primary IP Address	169.254.128.20
Secondary IP Address	169.254.128.30

* Reboot is required

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.

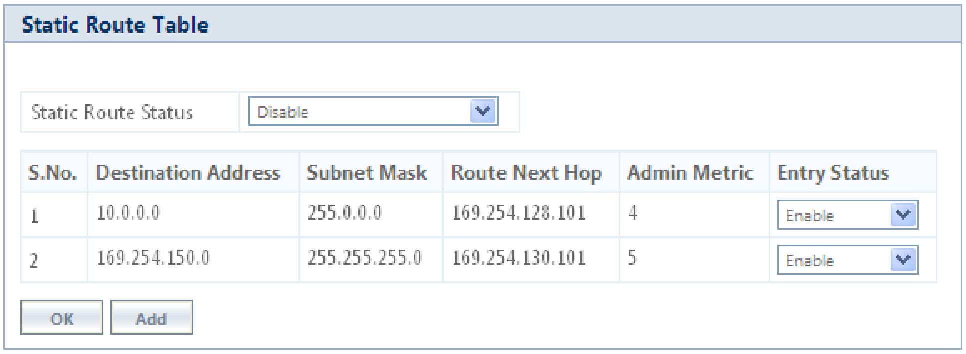
After configuring the required parameters, click **OK**, **COMMIT** and then **REBOOT**.

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

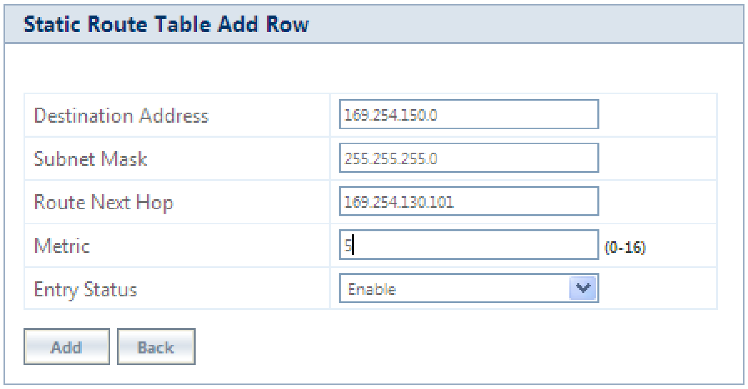
Figure 5-11 Static Route Table

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	169.254.150.0
Subnet Mask	255.255.255.0
Route Next Hop	169.254.130.101
Metric	5 (0-16)
Entry Status	Enable

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.

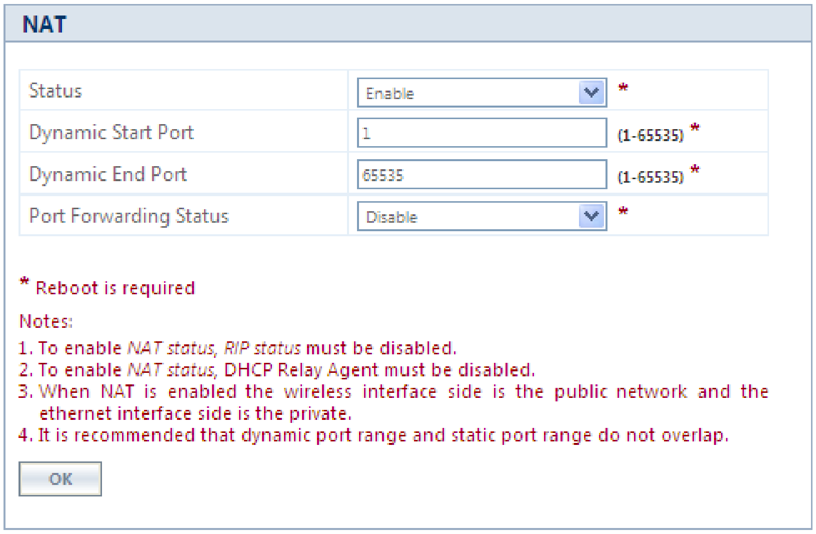
The SU/End Point B device supports both **Dynamic Mapping** (allowing private hosts to access hosts in the public network) and **Static Mapping** (allowing public hosts to access hosts in the private network) are supported.

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 *
Dynamic Start Port	1 (1-65535) *
Dynamic End Port	65535 (1-65535) *
Port Forwarding Status	Disable *

* 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):

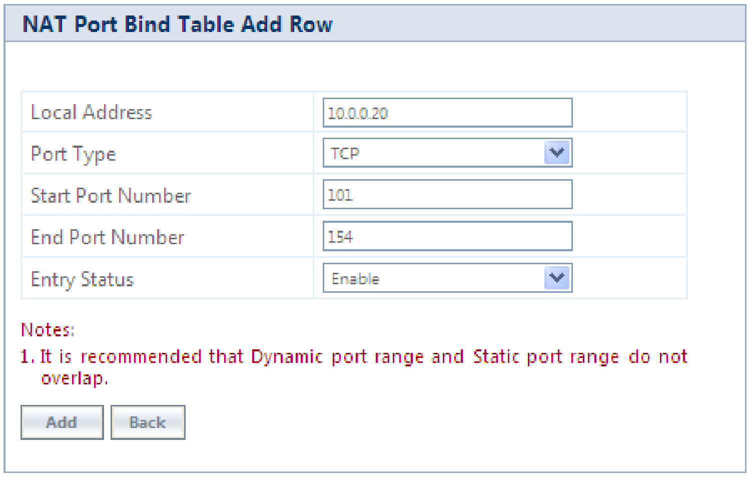
Parameter	Description
Status	This parameter is used to either **enable** or **disable** NAT on an SU or an End Point A.
Dynamic Start Port and Dynamic End Port	Represents the start and end port sessions originated from private to public host. By default, the Dynamic Start Port is configured to **1** and Dynamic End Port is configured to **65535**. Configure the start and end port as desired. : *Care should be taken to avoid overlap of Dynamic Port range and Static Port range.*
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:



NAT Port Bind Table Add Row

Local Address	10.0.0.20
Port Type	TCP
Start Port Number	101
End Port Number	154
Entry Status	Enable

Notes:
1. It is recommended that Dynamic port range and Static port range do not overlap.

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

S.No.	Protocol	Support	Applications
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

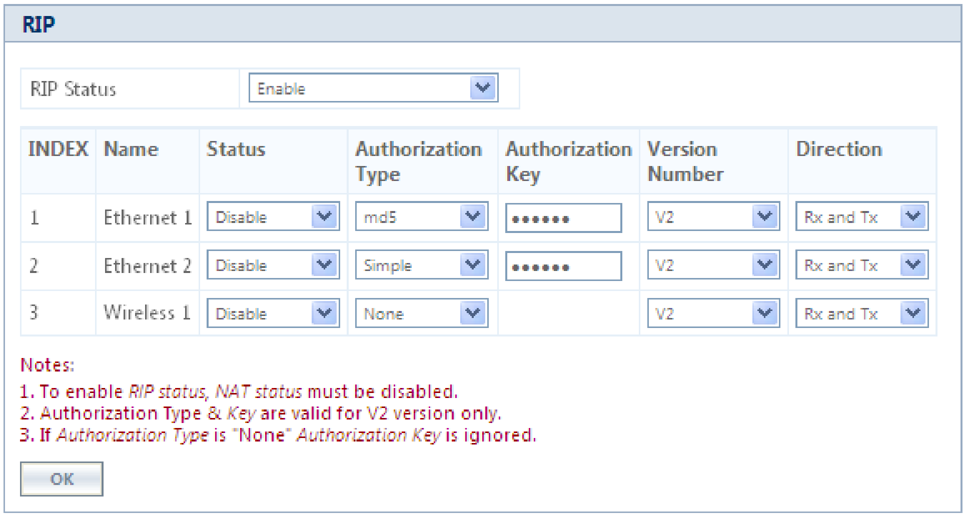
5.2.4 RIP

: 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.

Figure 5-15 RIP

By default, RIP is not enabled on the device. To enabled, 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**.

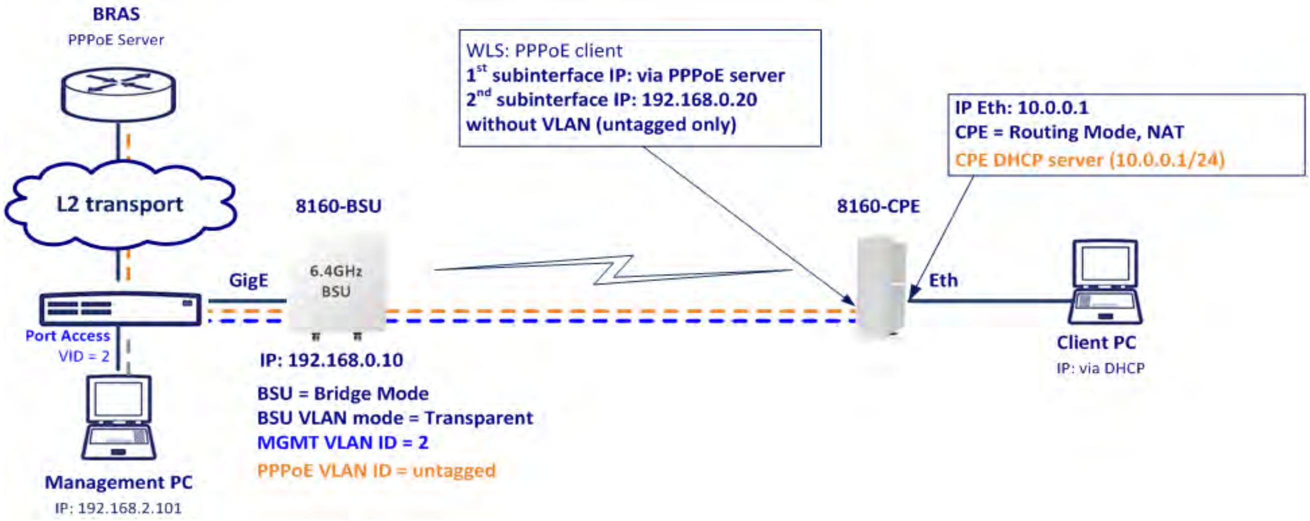


Figure 5-16 PPPoE Architecture

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

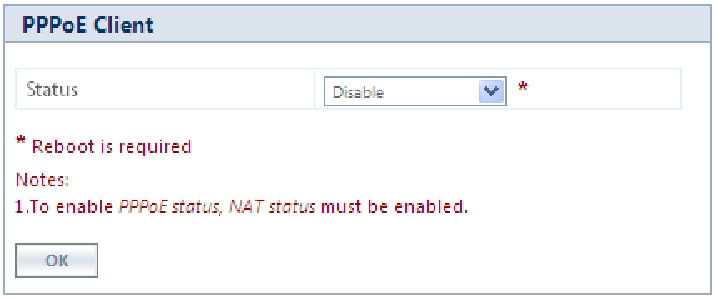
- **Discovery and Session Stage**: In this stage, to initiate a PPPoE session, the PPPoE client discovers a PPPoE server (called Access Concentrator). Once discovered, a session ID is assigned and a session is established.
- **Point-to-point Protocol (PPP) Stages**: The PPP stage comprises the following 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	Disable *

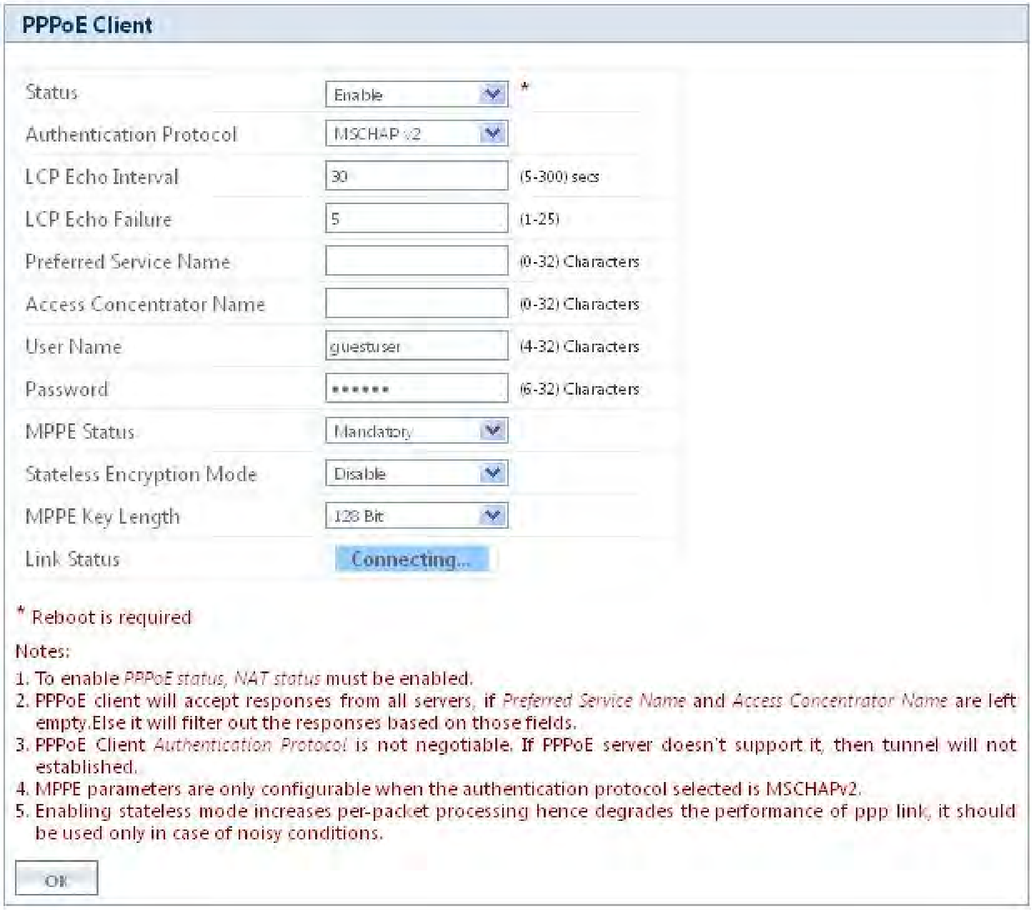
* Reboot is required

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	Enable	*
Authentication Protocol	MSCHAP v2	
LCP Echo Interval	30	(5-300) secs
LCP Echo Failure	5	(1-25)
Preferred Service Name		(0-32) Characters
Access Concentrator Name		(0-32) Characters
User Name	guestuser	(4-32) Characters
Password	••••••	(6-32) Characters
MPPE Status	Mandatory	
Stateless Encryption Mode	Disable	
MPPE Key Length	128 Bit	
Link Status	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	PPPoE supports the following types of user authentication protocols that provide varying levels of security: • **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. By default, the authentication protocol is set to **CHAP**. You can configure the authentication protocol to the desired one and click **OK**.
LCP Echo Interval	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. To configure LCP Echo Interval, enter a time ranging from 5 to 300 seconds. By default, the echo interval is set to **30 seconds**.

Parameter	Description
LCP Echo Failure	This parameter indicates the maximum number of consecutive failures to receive the LCP echo-reply to consider the connection to be down. 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.
Preferred Service Name	Specifies the service which the PPPoE server (Access Concentrators) provides to the PPPoE client. 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.
Access Concentrator Name	Specifies Access Concentrator (PPPoE server) name. 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.
User Name and Password	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. 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. 📝: *User Name and Password parameters are not applicable when the Authentication Protocol is configured as “None”.*

Parameter	Description
MPPE Status	*: MPPE Status parameter is applicable only when the Authentication Protocol is configured as "MSCHAP v2".* Microsoft Point-to-Point Encryption (MPPE) is a protocol for transferring encrypted data over point-to-point links. The PPPoE client negotiates on the encryption parameters based on the MPPE Status configured. The MPPE Status can be configured as following: • **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. Configure the desired status and click **OK**.
Stateless Encryption Mode	*: This parameter is applicable only when **Authentication Protocol** is configured as "MSCHAP v2" and **MPPE Status** is configured as "Mandatory".* When stateless encryption is negotiated, the session key changes for every packet transferred. In stateless mode, the sender must change its key before encrypting and transmitting each packet and the receiver must change its key after receiving, but before decrypting, each packet. When stateful encryption is negotiated, the PPPoE server and the client monitor the synchronization of MPP encryption engine on both the sides. When one of the peer detects that they are out of sync then the peer should transmit a packet with the coherency count set to 0xFF(a flag packet); the sender must change its key before encrypting and transmitting any packet and the receiver must change its key after receiving a flag packet, but before decrypting. To enable stateless encryption, select **Enable**. To enable stateful encryption, select **Disable**. *: Enabling Stateless Encryption impacts throughput. It is useful to enable Stateless encryption when packet drops are more in the wireless link.*

Parameter	Description
MPPE Key Length	: *This parameter is applicable only when **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: • **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.

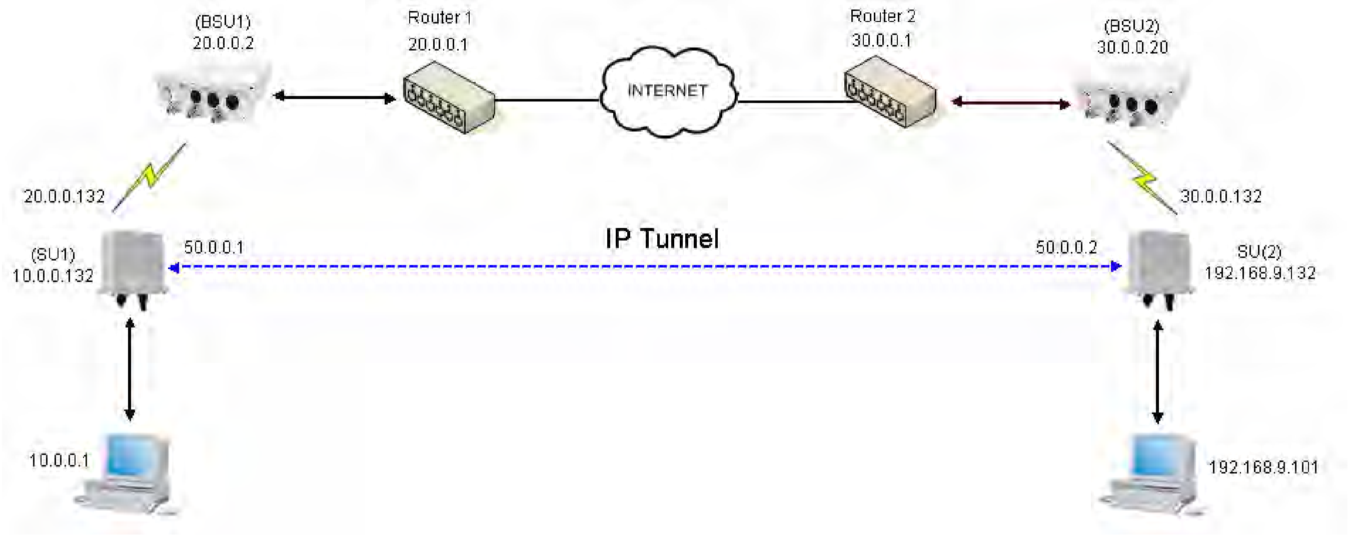


Figure 5-19 An Example: Tunnel Configuration

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 SU1device 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

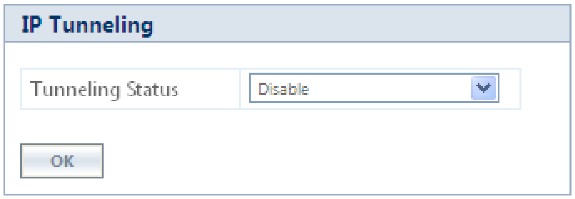
— Remote IP Address = 20.0.0.132

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:

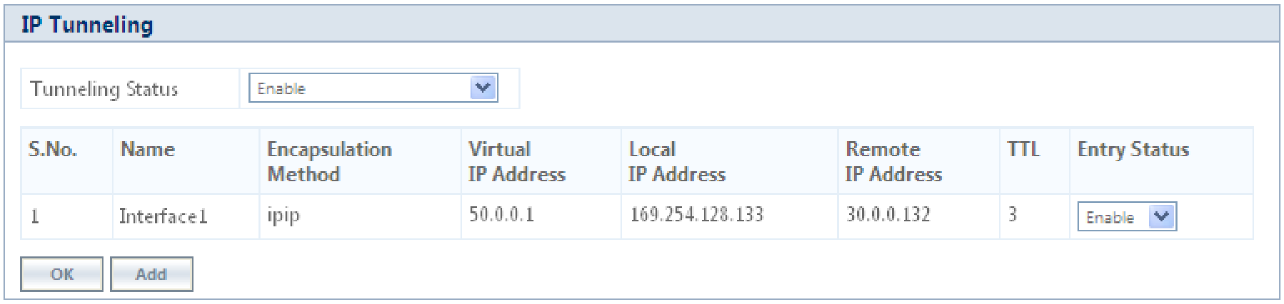


IP Tunneling

Tunneling Status	Disable

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:



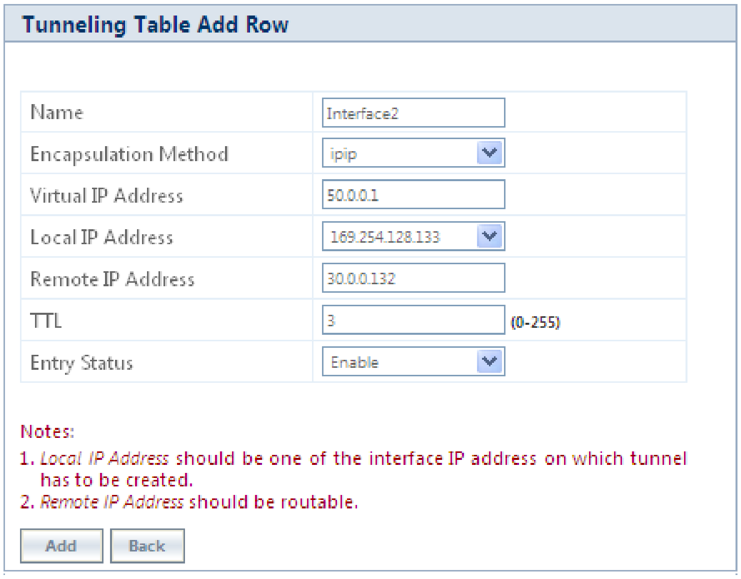
IP Tunneling

Tunneling Status	Enable

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	Interface2
Encapsulation Method	ipip
Virtual IP Address	50.0.0.1
Local IP Address	169.254.128.133
Remote IP Address	30.0.0.132
TTL	3 (0-255)
Entry Status	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	The device supports two types of network tunnels: • **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. Select the tunnel type as either **ipip** or **gre**.
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**.

:

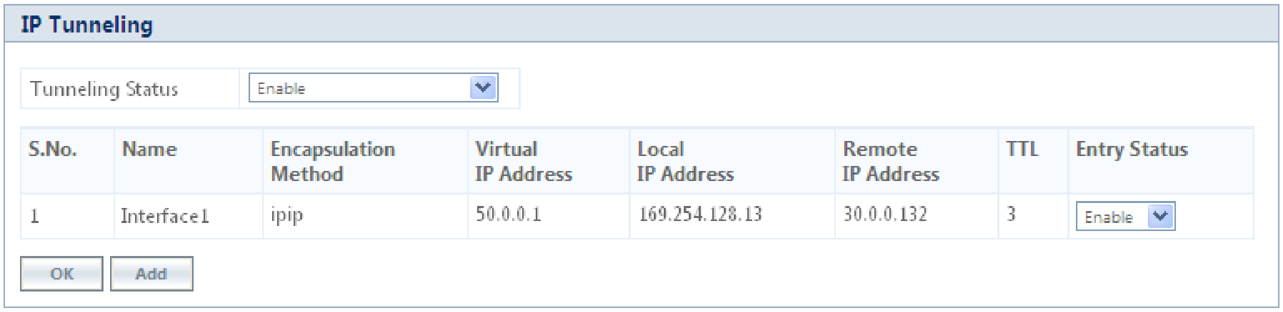
- *You can create a maximum of 16 tunnels.*

- *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.



IP Tunneling

Tunneling Status: Enable

S.No.	Name	Encapsulation Method	Virtual IP Address	Local IP Address	Remote IP Address	TTL	Entry Status
1	Interface1	ipip	50.0.0.1	169.254.128.13	30.0.0.132	3	Enable

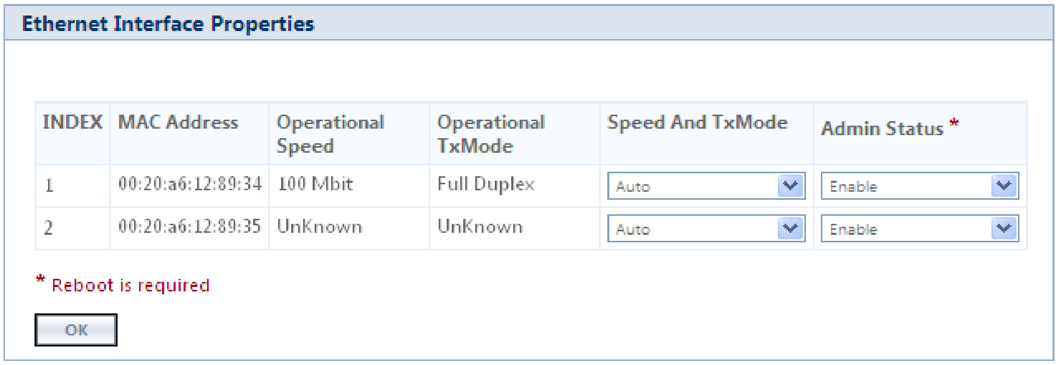
Figure 5-23 IP Tunneling Interfaces

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:



Ethernet Interface Properties

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):

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>MAC Address</td><td>Displays the MAC address of the Ethernet interface.</td></tr>
<tr><td>Operational Speed</td><td>Displays the current operational speed of the Ethernet interface.
Given below is the maximum operational speed of the Ethernet interface product wise:
<table>
<tr><th>Product (s)</th><th>Maximum Speed</th></tr>
<tr><td>• MP-8200-BSU-G
• MP-8250-BS9-G
• MP-8250-BS1-G
• MP-8200-BSU
• MP-8250-BS9
• MP-8250-BS1
• MP-820-BSU-100
• MP-822-BSU-100
• MP-825-BS3-100
• MP-8200-SUA
• MP-8250-SUR
• MP-8100-SUA
• MP-8150-SUR
• MP-8150-SUR-100
• MP-820-SUA-50^{+}
• MP-820-SUA-100
• MP-822-SUA-100
• MP-825-SUR-50^{+}
• MP-825-SUR-100
• QB-8200-EPA-G/LNK-G
• QB-8250-EPR-G/LNK-G
• QB-8200-EPA/LNK
• QB-8250-EPR/LNK
• QB-825-EPR/LNK-50^{+}
• QB-825-EPR/LNK-100</td><td>1 Gbps</td></tr>
<tr><td>• MP-825-CPE-50
• MP-825-CPE-100
• MP-835-CPE-10
• MP-835-CPE-25
• MP-835-CPE-50
• MP-835-CPE-100
• QB-835-EPR/LNK-25
• QB-835-EPR/LNK-50
• QB-826-EPR/LNK-100</td><td>100 Mbps</td></tr>
</table>
</td></tr>
</table>

Parameter	Description
Operational Tx Mode	Displays the current operational transmission mode of the Ethernet interface. It supports two types of transmission modes: • **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. 📝: • *Please ensure the same transmission modes are configured on the transmitter and the receiver device.* • *In case of 82x devices, the **Auto** option will support Gigabit if the other end is capable of supporting it.*
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**.

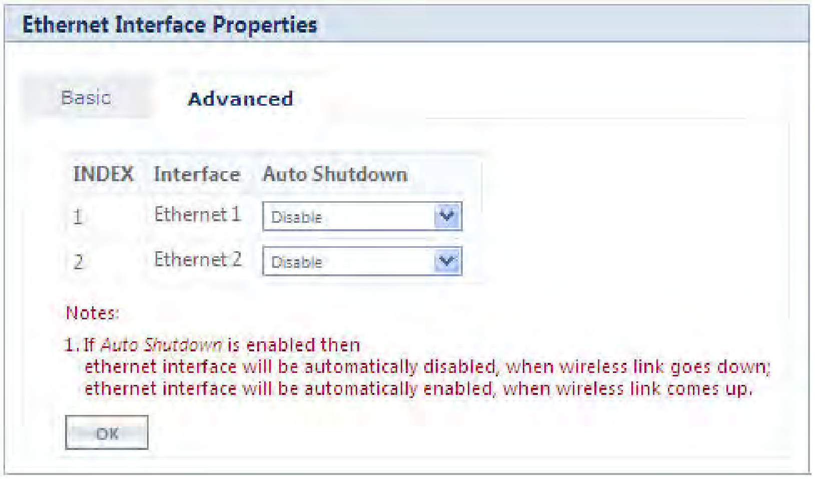
Reboot the device, if you have changed the **Admin Status** configuration.

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-8200-EPA-G/LNK-G, QB-8250-EPR-G/LNK-G, 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:



Ethernet Interface Properties

INDEX	Interface	Auto Shutdown
1	Ethernet 1	Disable
2	Ethernet 2	Disable

Notes:

1. If *Auto Shutdown* is enabled then
ethernet interface will be automatically disabled, when wireless link goes down;
ethernet interface will be automatically enabled, when wireless link comes up.

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	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**. 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. : *This feature works only if **STP/LACP Frames** is set to passthru (See Filtering (Bridge Only))* 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. : *When using second Ethernet port for management, ensure to disable Auto Shutdown for Ethernet2.* For details on how to manage the QuickBridge devices through the second Ethernet port, refer LACP - Device Management.

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
- 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 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.

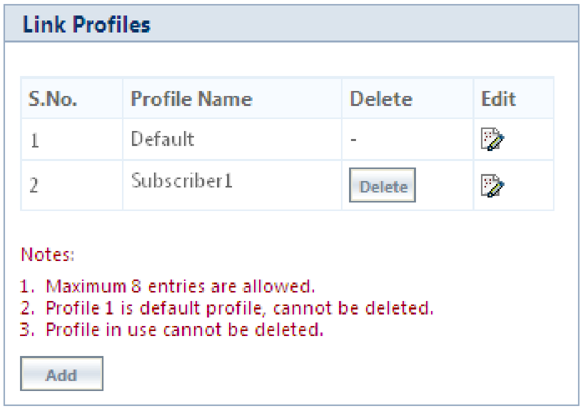
In point-to-multipoint (BSU and SU) devices, you can create a maximum of eight link profiles including the default pre-configured profile. Profiles that are created on the BSU are mapped to the SUs, and vice versa. If BSU/SU is not mapped to any configured profile, it will be mapped to the default profile.

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	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).

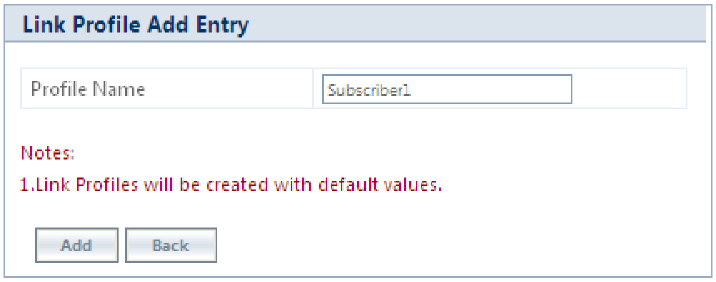
It is intended that all the WORP links that are expected to exhibit similar behavior be grouped under one link profile.

:

- *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:


Link Profile Add Entry

Profile Name	Subscriber1

Notes:
1.Link Profiles will be created with default values.

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**.

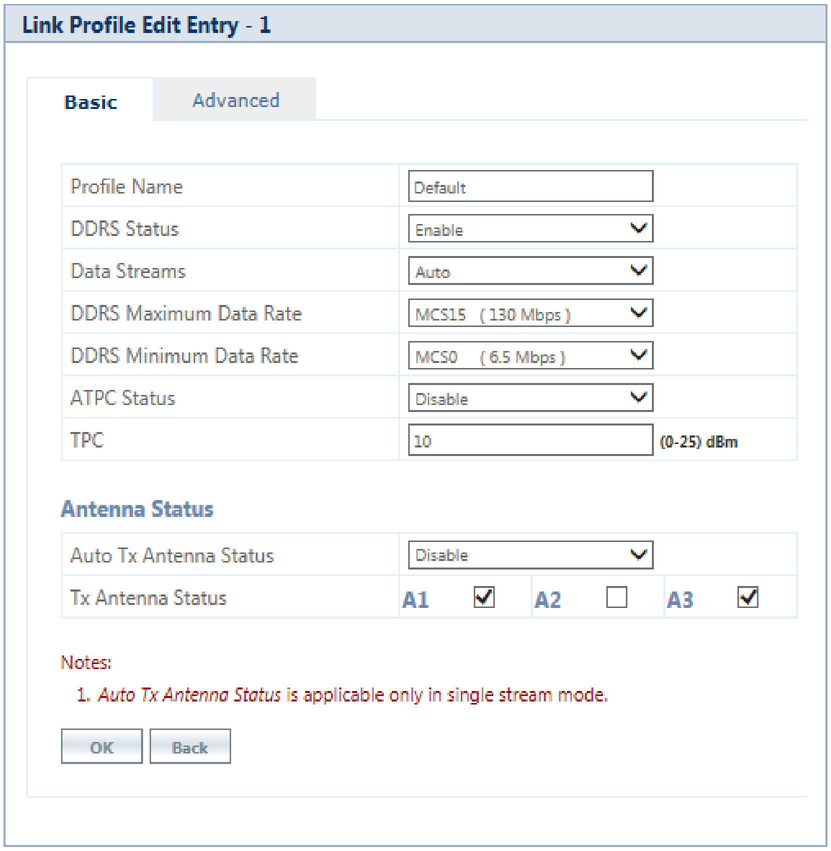
:

- *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 1** screen appears, which is classified under two categories: **Basic** and **Advanced**.



Link Profile Edit Entry - 1

Profile Name	Default
DDRS Status	Enable
Data Streams	Auto
DDRS Maximum Data Rate	MCS15 (130 Mbps)
DDRS Minimum Data Rate	MCS0 (6.5 Mbps)
ATPC Status	Disable
TPC	10 (0-25) dBm

Antenna Status

Auto Tx Antenna Status	Disable
Tx Antenna Status	A1 ☑ A2 □ A3 ☑

Notes:

1. *Auto Tx Antenna Status* is applicable only in single stream mode.

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	Dynamic Data Rate Selection (DDRS) feature adjusts the transmission data rate to an optimal value to provide the best possible throughput according to the current communication conditions and link quality. The factors for adjusting the transmission data rate are, 1. Remote average Signal-to-noise (SNR) ratio 2. Number of retransmissions The **DDRS Status** parameter allows to either enable or disable DDRS per link profile. By default, DDRS is enabled.

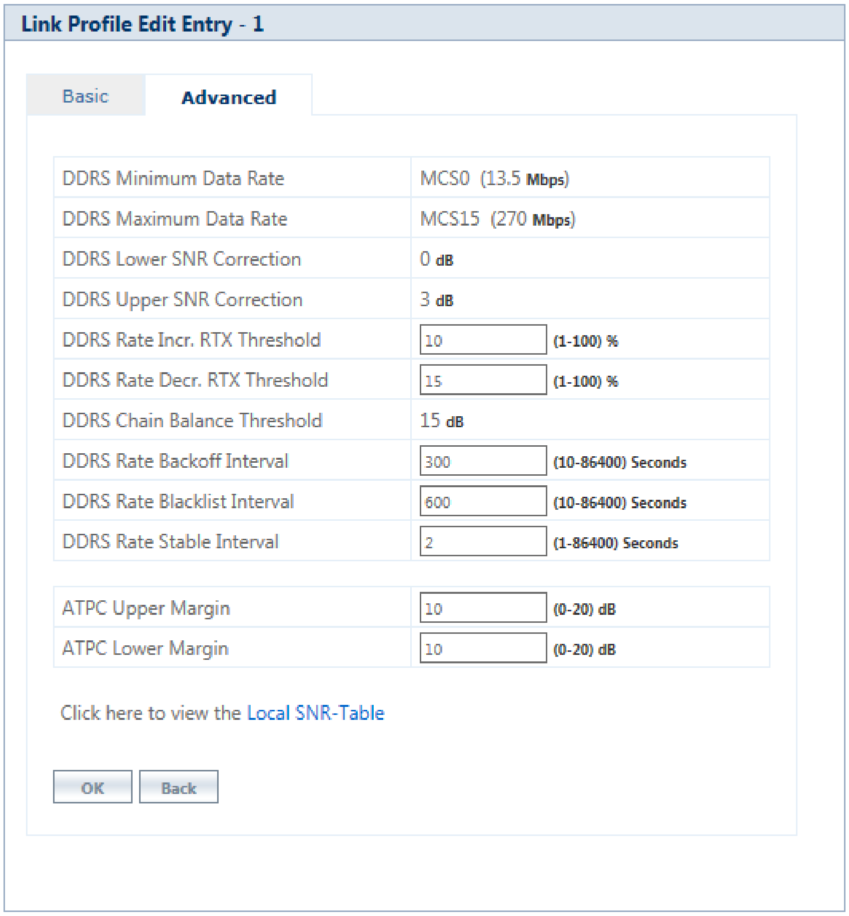
Parameter	Description
Data Streams	Select the data stream as either as **Auto**, **Single** or **Dual**. • **Dual Stream**: Select **Dual**, for higher throughput. • **Single Stream**: Select **Single**, for reliability and longer range. • **Auto Stream**: When configured to **Auto**, DDRS decides the stream modes based on the environmental conditions When DDRS is enabled, based on the selected data stream, DDRS dynamically chooses the data rate. : • *Data Stream mode is not applicable in legacy mode.* • *When DDRS is disabled, Auto stream is not applicable.*
DDRS Minimum Data Rate and DDRS Maximum 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.
Tx Rate	This parameter enables you to manually set the transmission data rate, wh en DDRS is disabled. A change in data streams resets Tx rate to its default value.
ATPC Status	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. Transmit Power Control (TPC) is calculated based on two factors: • Equivalent Isotropically Radiated Power (EIRP) • Maximum Optimal SNR In case of a BSU, when ATPC is enabled, TPC is adjusted on a per link basis. : In 82x /82xx US SKUs, ATPC cannot be disabled for DFS frequencies.

Parameter	Description
TPC	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 dB. *: In case of 82x devices, you can manually set TPC ranging from 0 to 15 dB.* 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 dB**. *:* • *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	Applicable only in single data stream mode. When **Auto Tx Antenna Status** is enabled for single stream, the device automatically selects the antenna port with highest received RSSI for data transmission.
Tx Antenna Status	Applicable only when **Auto Tx Antenna Status** is disabled. 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**. *:* • *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

DDRS Minimum Data Rate	MCS0 (13.5 Mbps)
DDRS Maximum Data Rate	MCS15 (270 Mbps)
DDRS Lower SNR Correction	0 dB
DDRS Upper SNR Correction	3 dB
DDRS Rate Incr. RTX Threshold	10 (1-100) %
DDRS Rate Decr. RTX Threshold	15 (1-100) %
DDRS Chain Balance Threshold	15 dB
DDRS Rate Backoff Interval	300 (10-86400) Seconds
DDRS Rate Blacklist Interval	600 (10-86400) Seconds
DDRS Rate Stable Interval	2 (1-86400) Seconds
ATPC Upper Margin	10 (0-20) dB
ATPC Lower Margin	10 (0-20) dB

Click here to view the Local SNR-Table

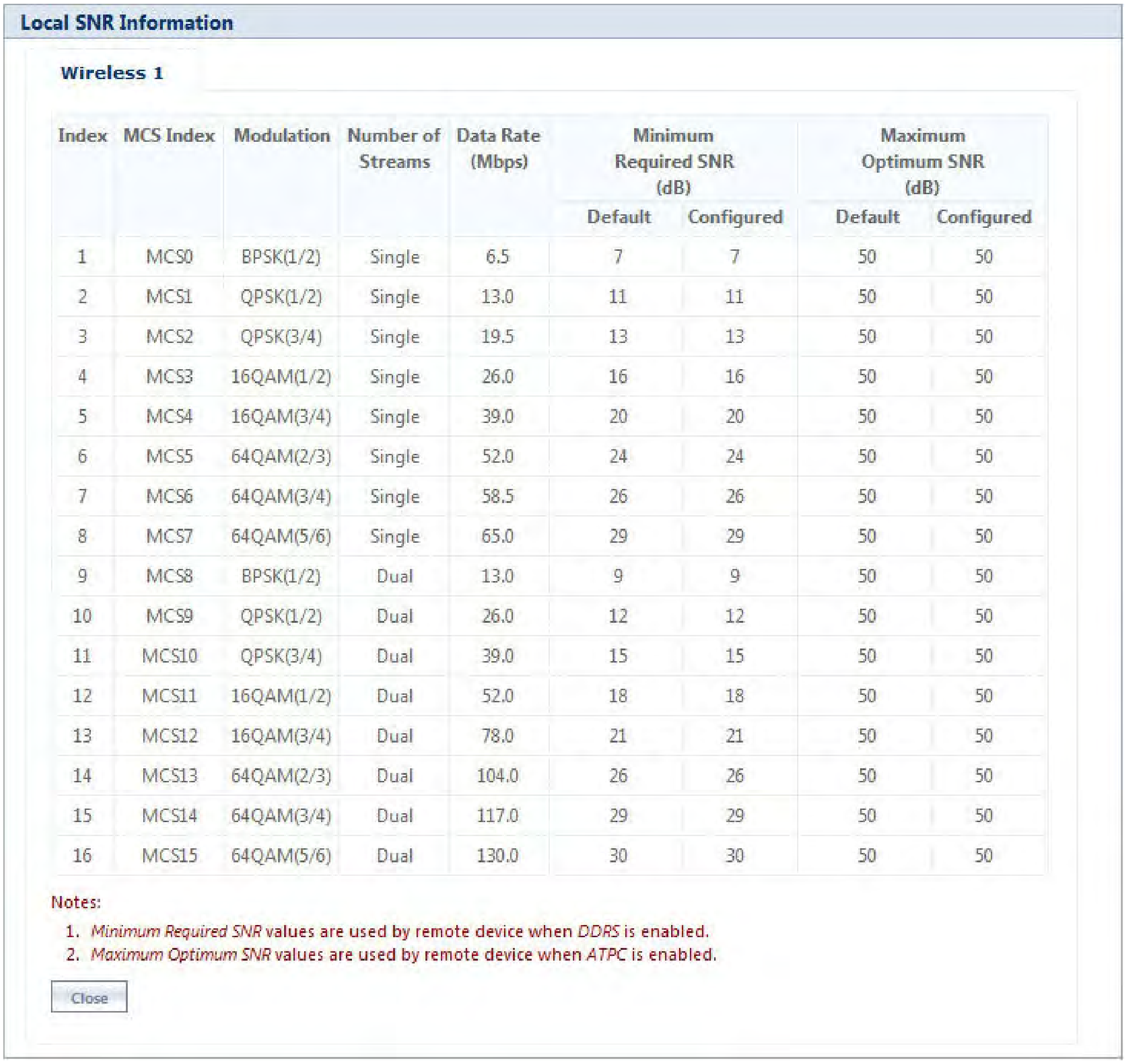
Figure 5-29 Edit a Link Profile (Advanced)

Parameter	Description
DDRS Minimum Data Rate and DDRS Maximum 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	Represents a threshold for the percentage of retransmissions, below which the rate can be increased. By default, it is set to **10%**. 📝: *If the percentage of retransmissions is between “Rate Increment RTX Threshold” and “Rate Decrement RTX Threshold” then the current operation rate is maintained.*
DDRS Rate Decr RTX Threshold	Represents a threshold for percentage of retransmissions, above which the rate can be decreased. By default, it is set to **15%**. 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.
DDRS Chain Balance Threshold	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**. 📝: • *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	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**.
DDRS Rate Blacklist Interval	Applicable when data stream mode is set to **Auto**. 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**. 📝: *DDRS Rate Back Off Interval must be less than the DDRS Rate Blacklist Interval.*
DDRS Rate Stable Interval	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**.

Parameter	Description
ATPC Upper Margin and Lower Margin	SNR Upper Limit = Maximum Optimal SNR SNR Initial = SNR Upper Limit – ATPC Upper Margin SNR Lower Limit = SNR Initial – ATPC Lower Margin 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. By default, the **ATPC Lower Margin** and **ATPC Upper Margin** is 10 dB. To configure, type a value ranging from 0 to 20 dB.

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



Local SNR Information

Wireless 1

Index	MCS Index	Modulation	Number of Streams	Data Rate (Mbps)	Minimum Required SNR (dB)		Maximum Optimum SNR (dB)	
					Default	Configured	Default	Configured
1	MCS0	BPSK(1/2)	Single	6.5	7	7	50	50
2	MCS1	QPSK(1/2)	Single	13.0	11	11	50	50
3	MCS2	QPSK(3/4)	Single	19.5	13	13	50	50
4	MCS3	16QAM(1/2)	Single	26.0	16	16	50	50
5	MCS4	16QAM(3/4)	Single	39.0	20	20	50	50
6	MCS5	64QAM(2/3)	Single	52.0	24	24	50	50
7	MCS6	64QAM(3/4)	Single	58.5	26	26	50	50
8	MCS7	64QAM(5/6)	Single	65.0	29	29	50	50
9	MCS8	BPSK(1/2)	Dual	13.0	9	9	50	50
10	MCS9	QPSK(1/2)	Dual	26.0	12	12	50	50
11	MCS10	QPSK(3/4)	Dual	39.0	15	15	50	50
12	MCS11	16QAM(1/2)	Dual	52.0	18	18	50	50
13	MCS12	16QAM(3/4)	Dual	78.0	21	21	50	50
14	MCS13	64QAM(2/3)	Dual	104.0	26	26	50	50
15	MCS14	64QAM(3/4)	Dual	117.0	29	29	50	50
16	MCS15	64QAM(5/6)	Dual	130.0	30	30	50	50

Notes:

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

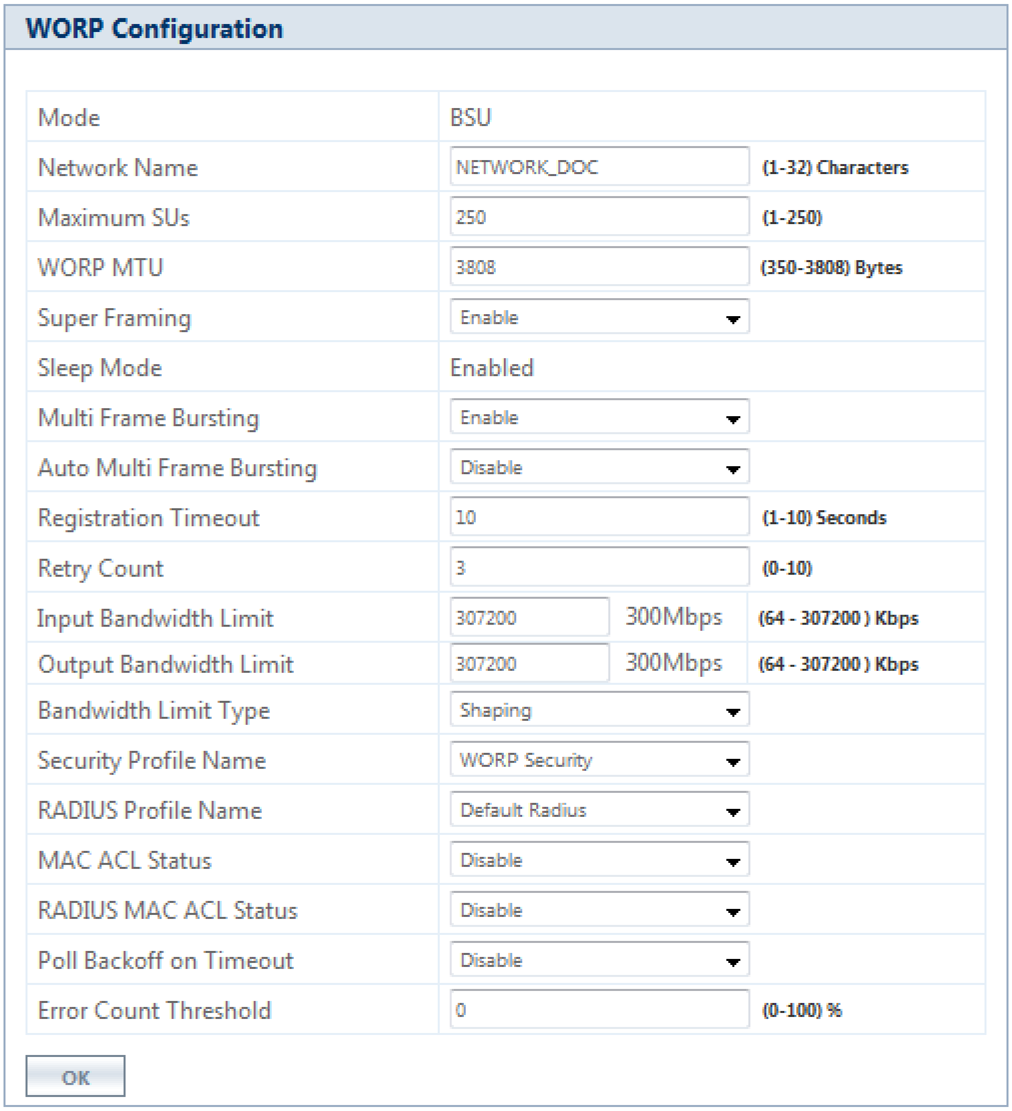
Figure 5-30 An Example - SNR Information

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.

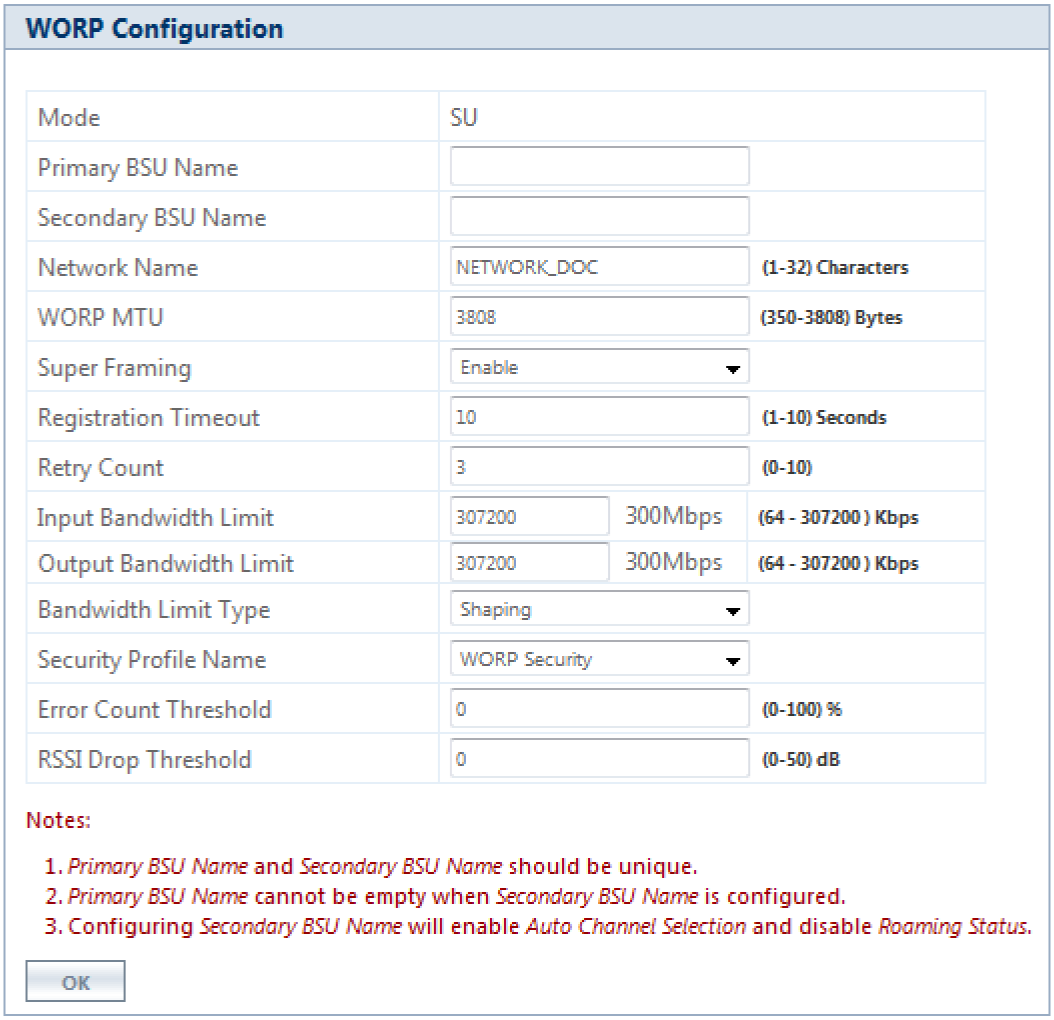
To configure the WORP properties, navigate to **ADVANCED CONFIGURATION > Wireless > Interface1 > WORP**. The **WORP Configuration** screen appears:



WORP Configuration

Mode	BSU	
Network Name	NETWORK_DOC	(1-32) Characters
Maximum SUs	250	(1-250)
WORP MTU	3808	(350-3808) Bytes
Super Framing	Enable	
Sleep Mode	Enabled	
Multi Frame Bursting	Enable	
Auto Multi Frame Bursting	Disable	
Registration Timeout	10	(1-10) Seconds
Retry Count	3	(0-10)
Input Bandwidth Limit	307200 300Mbps	(64 - 307200) Kbps
Output Bandwidth Limit	307200 300Mbps	(64 - 307200) 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) %

Figure 5-31 WORP Configuration (BSU)



WORP Configuration

Mode	SU	
Primary BSU Name		
Secondary BSU Name		
Network Name	NETWORK_DOC	(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	307200 300Mbps	(64 - 307200) Kbps
Output Bandwidth Limit	307200 300Mbps	(64 - 307200) Kbps
Bandwidth Limit Type	Shaping	
Security Profile Name	WORP Security	
Error Count Threshold	0	(0-100) %
RSSI Drop Threshold	0	(0-50) dB

Notes:

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 Status*.

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	Applicable only to an SU. 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. : *This is the system name as configured on a BSU.*

Parameter	Description
Secondary BSU Name	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. 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. • *The Primary and the Secondary BSU names should be unique.* • *The Secondary BSU name is the 'System Name' of the BSU used as a secondary BSU.* • *Frequency Domain, Channel Bandwidth and Channel Offset should be same for all BSUs which participate in redundancy.* • *If the BSU that participates in redundancy, operates in a channel that is blacklisted, SU will not switch.* • *An SU will switch to a BSU only when the BSU has not reached its maximum SU limit.* • *When Secondary BSU name is configured, Roaming is not applicable.* • *When Secondary BSU name is configured, Automatic Channel Selection is automatically enabled on the SU.*
End Point A Name	Applicable only to an End Point B. 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.
Network Name	It is a unique name of given to a logical network. Devices only within this logical network can establish wireless connection. The Network Name can be of 1 to 32 characters in length. By default it is **MY_NETWORK**.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Max SUs</td><td>Represents the maximum number of SUs that can register with a BSU.
Given below are the base stations and the maximum number of subscribers supported by each of them:
<table>
<tr><th>Base Station</th><th>Maximum Number of Subscribers</th></tr>
<tr><td>MP-8200-BSU-G/ MP-8200-BSU</td><td>250</td></tr>
<tr><td>MP-8250-BS9-G/ MP-8250-BS9</td><td>250</td></tr>
<tr><td>MP-8250-BS1-G/ MP-8250-BS1</td><td>250</td></tr>
<tr><td>MP-820-BSU-100</td><td>32</td></tr>
<tr><td>MP-822-BSU-100</td><td>32</td></tr>
<tr><td>MP-825-BS3-100</td><td>32</td></tr>
</table>
📝<i>: Applicable only to the BSU.</i></td></tr>
<tr><td>WORP MTU</td><td>WORP MTU (Maximum Transmission Unit) is the largest size of the data payload in wireless frame that can be transmitted. The MTU size can range from <b>350 to 3808</b> bytes for High throughput modes and <b>350 to 2304</b> bytes for legacy mode. The default and maximum value of the WORP MTU is <b>3808</b> bytes for higher throughput and <b>2304</b> bytes for legacy mode.</td></tr>
<tr><td>Super Framing</td><td>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.</td></tr>
<tr><td>Sleep Mode</td><td>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 on a BSU; however, in Sync mode, by default it is enabled and it cannot be disabled.
📝<i>: Applicable only to the BSU.</i></td></tr>
</table>

Parameter	Description
Multi Frame Bursting	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 compilation of the burst, the receiver response by sending the acknowledgment. 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). : *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.*
Auto Multi Frame Bursting	Auto Multi Frame Bursting feature takes effect only when Multi Frame Bursting feature is enabled. 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. : *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.*
Registration Timeout	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**.
Retry Count	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**.
Input Bandwidth Limit and Output Bandwidth Limit	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. : *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)
Bandwidth Limit Type	Specifies the action performed when the traffic utilization exceeds the configured input or output limits. By default it is set to **Shaping**. • **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.*

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

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

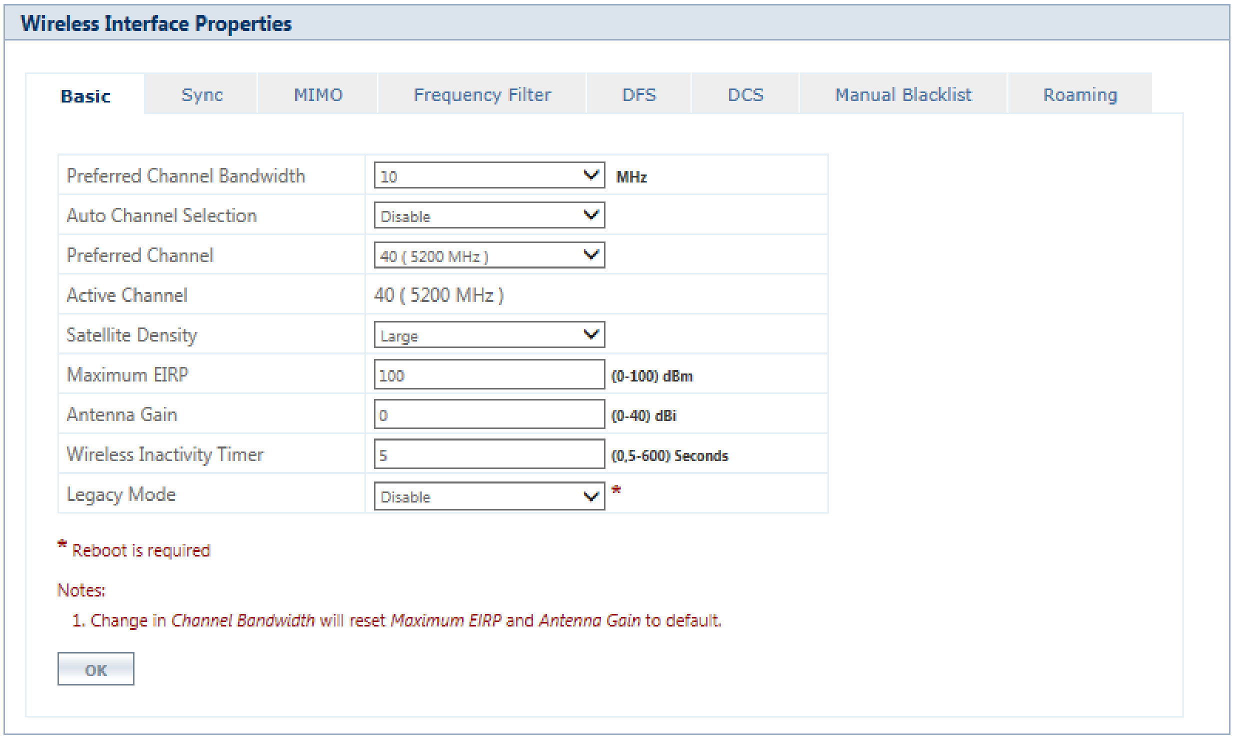
5.4.3 Wireless Interface Properties

To configure the wireless interface properties, navigate to **ADVANCED CONFIGURATION** > **Wireless** > **Interface 1** > **Properties**.

The Wireless Interface Properties screen is classified under the following categories: **Basic**, **Sync**, **MIMO**, **Frequency Filter**, **DFS**, **DCS**, **Manual Blacklist**, and **Roaming**.The parameters displayed in the **Wireless Interface Properties** screen may vary according to the device type.

5.4.3.1 Basic

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



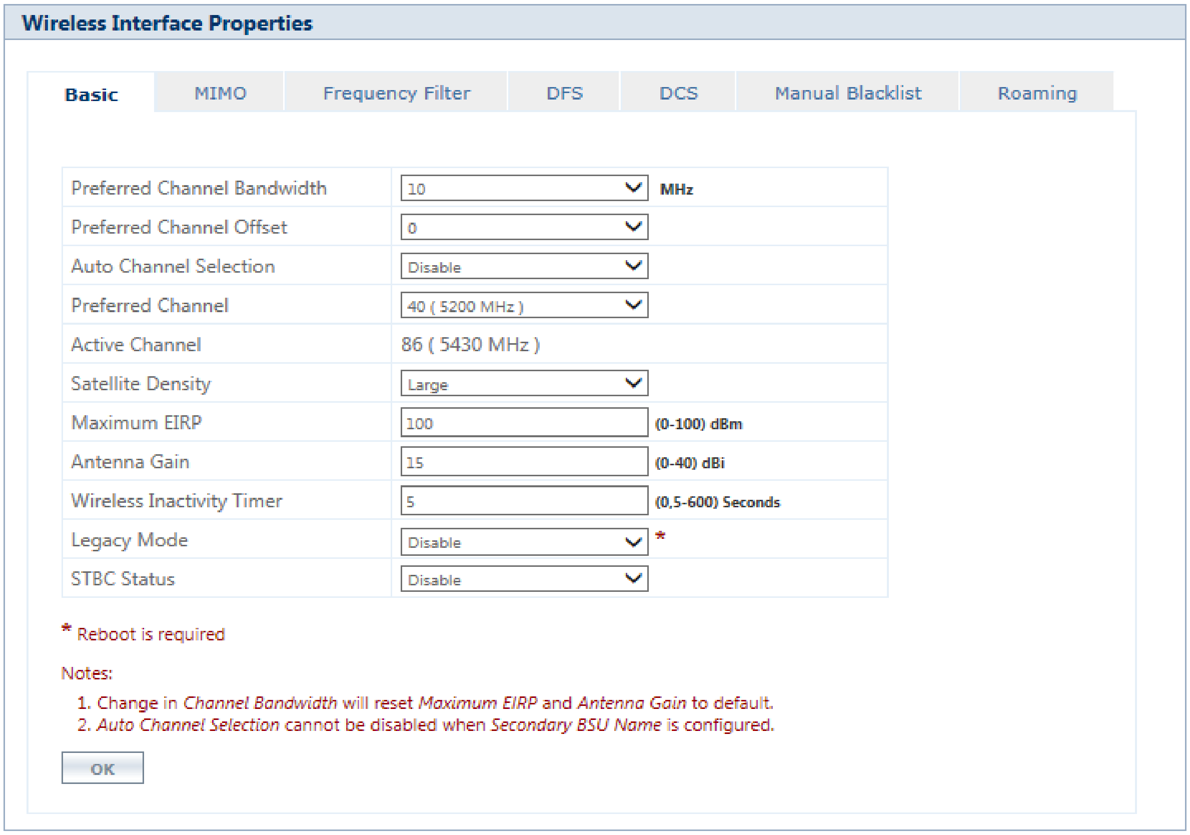
Preferred Channel Bandwidth	10 MHz
Auto Channel Selection	Disable
Preferred Channel	40 (5200 MHz)
Active Channel	40 (5200 MHz)
Satellite Density	Large
Maximum EIRP	100 (0-100) dBm
Antenna Gain	0 (0-40) dBi
Wireless Inactivity Timer	5 (0,5-600) Seconds
Legacy Mode	Disable *

* Reboot is required

Notes:

1. Change in *Channel Bandwidth* will reset *Maximum EIRP* and *Antenna Gain* to default.

Figure 5-33 Wireless Interface Properties (BSU)



Preferred Channel Bandwidth	10	MHz
Preferred Channel Offset	0	
Auto Channel Selection	Disable	
Preferred Channel	40 (5200 MHz)	
Active Channel	86 (5430 MHz)	
Satellite Density	Large	
Maximum EIRP	100	(0-100) dBm
Antenna Gain	15	(0-40) dBi
Wireless Inactivity Timer	5	(0,5-600) Seconds
Legacy Mode	Disable	*
STBC Status	Disable	

* Reboot is required

Notes:

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

Figure 5-34 Wireless Interface Properties (SU)

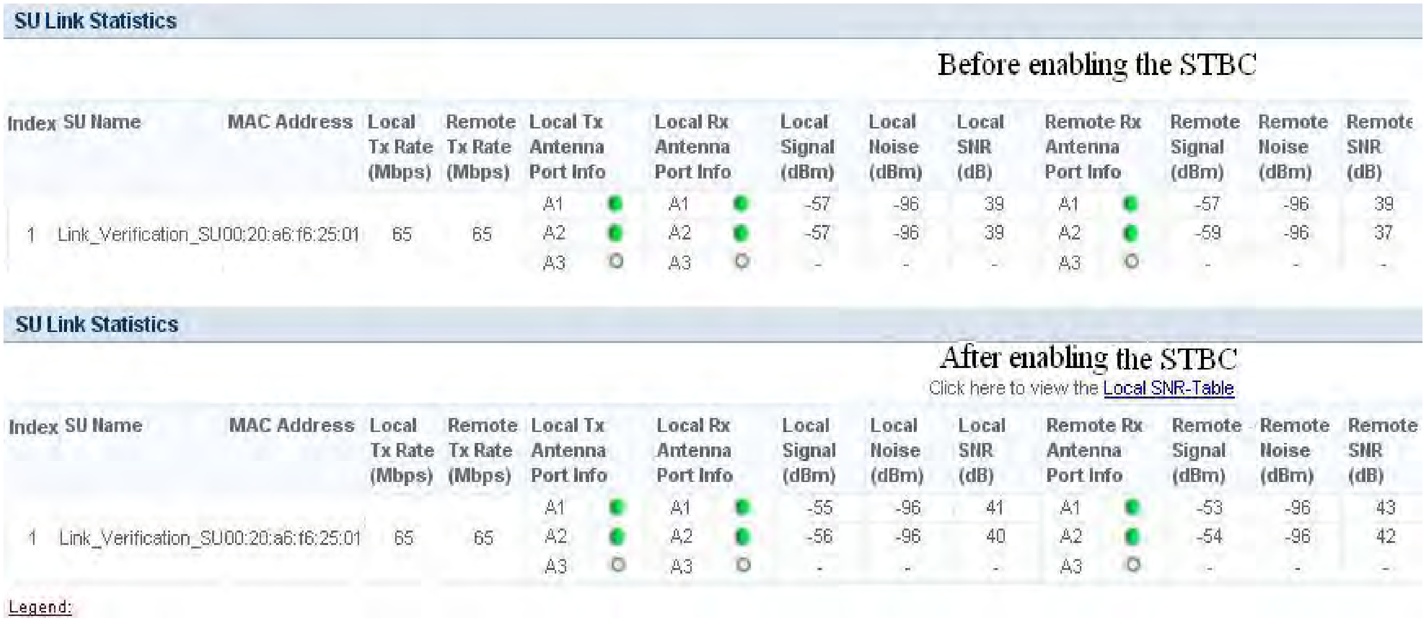
The parameters under the Basic tab are described and tabulated below.

Parameter	Descriptions
Preferred Channel Bandwidth	By default it is 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. 📝: • *40 MHz channel bandwidth is not applicable in Legacy mode.* • *A change in Preferred Channel Bandwidth will reset the Tx Rate, Maximum EIRP, and Antenna Gain to default value.* For more details, see Frequency Domains and Channels.

Parameter	Descriptions
Preferred Channel Offset	📝: *Applicable only to MP-820-BSU-100; MP-822-BSU-100; MP-825-BS3-100; MP-820-SUA-50$^+$; MP-820-SUA-100; MP-822-SUA-100; MP-825-SUR-50$^+$; MP-825-SUR-100; MP-825-CPE-50; MP-825-CPE-100; MP-835-CPE-10; MP-835-CPE-25; MP-835-CPE-50; MP-835-CPE-100; QB-825-EPR/LNK-50$^+$; QB-825-EPR/LNK-100; QB-835-EPR/LNK-25; QB-835-EPR/LNK-50 and QB-826-EPR/LNK-100 devices.* This parameter helps to change the operating channel center frequency. If the predefined center frequencies are not desirable, the user can shift the center frequency to suit the requirement by configuring the Preferred Channel Offset. By default it is set to **0**. The configurable range: **-2** to **+2** MHz. For example, consider a channel number 100 with the center channel frequency set to 5500 MHz. If the Preferred Channel Offset is set to 0 MHz, the center channel frequency remains at 5500 MHz. If you configure this to 2MHz then the center channel frequency will change to 5502MHz. Similarly if it is set to -2MHz, the center channel frequency will change to 5498 MHz. 📝: • *Even though the center channel frequency is changed, the channel number still remains same, in this case 100.* • *This parameter is not available for 82xx SU.*
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	This parameter 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. 📝: *This parameter is not applicable for a SU (82xx & 82x series) as ACS is always enabled.*
Active Channel	A read-only parameter that displays the current operating channel. 📝: *Active Channel can be different from the Preferred Channel if radar or other interference is detected and the channel is blacklisted.*

<table>
<tr><th>Parameter</th><th>Descriptions</th></tr>
<tr><td>Satellite Density</td><td>
<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 <b>Large</b>. The Medium, Small, Mini, and Micro settings are appropriate for higher noise environments; whereas, Large is appropriate for a lower noise environment. A long distance link can have difficulty in maintaining a connection with a small density setting because the wanted signal can disappear under the threshold. Consider both noise level and distance between the peers in a link when configuring this setting. The threshold should be chosen higher than the noise level, but sufficiently below the signal level. A safe value is 10dB below the present signal strength.</p>
<p>If the Signal-to-Noise Ratio (SNR) is not sufficient, you may need to set a lower data rate or use antennas with higher gain to increase the margin between wanted and unwanted signals. In a point-to-multipoint link, the BSU or End Point A should have a density setting suitable for an SU or End Point B, especially the ones with the lowest signal levels (longest links). Take care when configuring a remote interface; check the available signal level first.</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>
<tr><th>Interference Signal</th><th>Radio Behavior</th></tr>
<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>
</table>
<p>Given below are the Sensitivity Threshold Values corresponding to various Satellite Density values:</p>
<table>
<tr><th>Satellite Density</th><th>Receive Sensitivity Threshold</th><th>Defer Threshold</th></tr>
<tr><td>Large</td><td>3</td><td>28</td></tr>
<tr><td>Medium</td><td>9</td><td>33</td></tr>
<tr><td>Small</td><td>17</td><td>43</td></tr>
<tr><td>Mini</td><td>25</td><td>53</td></tr>
<tr><td>Micro</td><td>33</td><td>59</td></tr>
<tr><td>Disabled</td><td>0-63</td><td>28</td></tr>
</table>
</td></tr>
</table>

Parameter	Descriptions
	: 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. *: 'Defer Threshold' is not applicable for the Sync enabled devices.*
Sensitivity	Sensitivity is identical to Receive Sensitivity Threshold. Please refer the table given above for the Receive Sensitivity Threshold values. By means of the Satellite Density only specific Receive Sensitivity Threshold values can be set. By using the Sensitivity parameter tune the Receive Sensitivity Threshold values in the SNR range of (0-63) and its default value is 0. *: Sensitivity parameter is visible only if the Satellite Density is set to **Disable.***
STBC Status	STBC (Space Time Block Coding) is a provision to transmit multiple copies of a single data-stream to different antenna ports. After obtaining the data, the receiver compares, aggregates and processes it, to minimize the data loss. This redundancy in data increases the reliability of the data-transmission and therefore helps to improve the overall data transfer in the hostile RF environments. By default STBC is disabled. *: STBC is applicable only to 82x products and it works only when a single data-stream is used for transmission.*



SU Link Statistics

Before enabling the STBC

Index	SU Name	MAC Address	Local Tx Rate (Mbps)	Remote Tx Rate (Mbps)	Local Tx Antenna Port Info		Local Rx Antenna Port Info		Local Signal (dBm)	Local Noise (dBm)	Local SNR (dB)	Remote Rx Antenna Port Info		Remote Signal (dBm)	Remote Noise (dBm)	Remote SNR (dB)
1	Link_Verification_SU	00:20:a6:f6:25:01	65	65	A1	●	A1	●	-57	-96	39	A1	●	-57	-96	39
					A2	●	A2	●	-57	-96	39	A2	●	-59	-96	37
					A3	○	A3	○	-	-	-	A3	○	-	-	-

SU Link Statistics

After enabling the STBC

Click here to view the Local SNR-Table

Index	SU Name	MAC Address	Local Tx Rate (Mbps)	Remote Tx Rate (Mbps)	Local Tx Antenna Port Info		Local Rx Antenna Port Info		Local Signal (dBm)	Local Noise (dBm)	Local SNR (dB)	Remote Rx Antenna Port Info		Remote Signal (dBm)	Remote Noise (dBm)	Remote SNR (dB)
1	Link_Verification_SU	00:20:a6:f6:25:01	65	65	A1	●	A1	●	-55	-96	41	A1	●	-53	-96	43
					A2	●	A2	●	-56	-96	40	A2	●	-54	-96	42
					A3	○	A3	○	-	-	-	A3	○	-	-	-

Legend:

<table>
<tr><th>Parameter</th><th>Descriptions</th></tr>
<tr><td>Max EIRP</td><td>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.
Given below are the default maximum EIRP values that are set according to regulatory domain:
<table>
<tr><th rowspan="2">Regulatory Domain</th><th colspan="2">Maximum EIRP (dBm)</th></tr>
<tr><th>PTP Mode</th><th>PTMP Mode</th></tr>
<tr><td>United States 5 GHz</td><td>53</td><td>36</td></tr>
<tr><td>United States 5.8 GHz</td><td>53</td><td>36</td></tr>
<tr><td>World 5 GHz</td><td>100</td><td>100</td></tr>
<tr><td>World 4.9 GHz</td><td>100</td><td>100</td></tr>
<tr><td>Canada 5 GHz</td><td>30</td><td>30</td></tr>
<tr><td>Europe 5.8 GHz</td><td>36</td><td>36</td></tr>
<tr><td>Europe 5.4 GHz</td><td>30</td><td>30</td></tr>
<tr><td>Russia 5 GHz</td><td>100</td><td>100</td></tr>
<tr><td>Thaiwan 5 GHz</td><td>36</td><td>36</td></tr>
<tr><td>Canada 5.8 GHz</td><td>53</td><td>36</td></tr>
<tr><td>Japan 4.9 GHz</td><td>37</td><td>37</td></tr>
<tr><td>UK 5.8 GHz</td><td>36</td><td>36</td></tr>
<tr><td>World 5.9 GHz</td><td>100</td><td>100</td></tr>
<tr><td>US2 (5.3 & 5.8) GHz</td><td>53</td><td>36</td></tr>
<tr><td>India 5.8 GHz</td><td>36</td><td>36</td></tr>
<tr><td>Brazil 5.4 GHz</td><td>30</td><td>30</td></tr>
<tr><td>Brazil 5.8 GHz</td><td>100</td><td>32</td></tr>
<tr><td>Australia 5.4 GHz</td><td>30 (20 and 40 MHz)</td><td>30 (20 and 40 MHz)</td></tr>
<tr><td>Australia 5.8 GHz</td><td>36</td><td>36</td></tr>
<tr><td>Unites states 4.9 GHz</td><td>33(20MHz)
30 (10 MHz)
27 (5 MHz)</td><td>33(20MHz)
30 (10 MHz)
27 (5 MHz)</td></tr>
<tr><td>Canada 4.9 GHz</td><td>33 (20 and 40 MHz)
30 (10 MHz)
27 (5 MHz)</td><td>33 (20 and 40 MHz)
30 (10 MHz)
27 (5 MHz)</td></tr>
<tr><td>Legacy 5 GHz</td><td>100</td><td>100</td></tr>
<tr><td>Japan 5.6 GHz</td><td>100</td><td>100</td></tr>
</table>
</td></tr>
</table>

Parameter	Descriptions

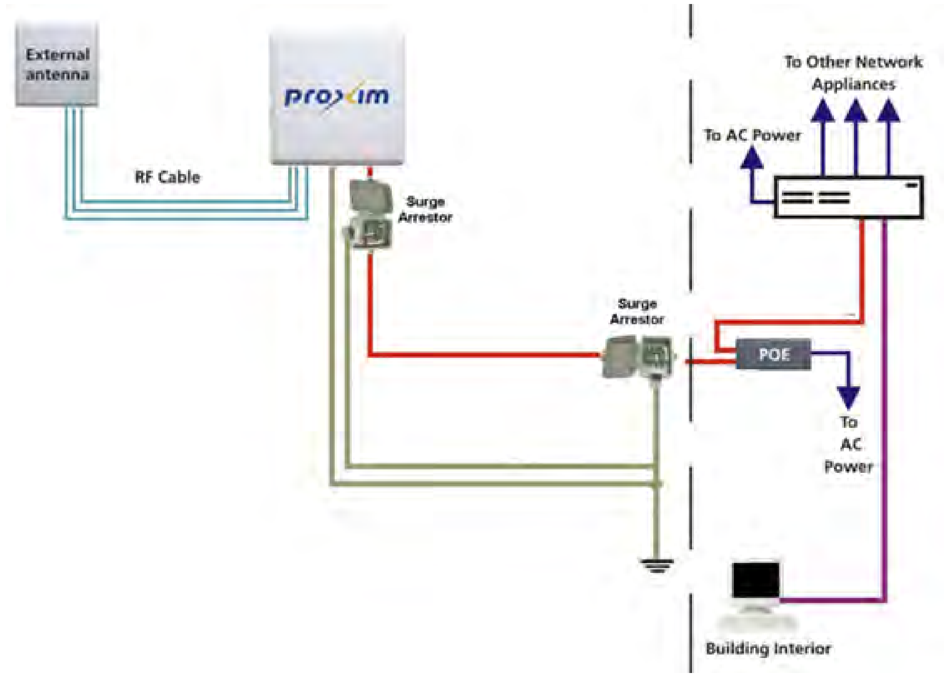
Regulatory Domain	Maximum EIRP (dBm)	
	PTP Mode	PTMP Mode
World 5.8 GHz	100	100
Indonesia 5.7 GHz	100	100
US3 (5.2 & 5.8) GHz	53	36
Egypt 5.8 GHz	36	36
Thailand 5.2 GHZ	23	23
Thailand 5.6 GHz	30	30
US4 (4.9 & 5) GHz	53	36
Industry Canada (IC) 5.2 GHz	23	23

Frequency Domains applicable for 81xx Products

Regulatory Domain	Maximum EIRP (dBm)	
	PTP Mode	PTMP Mode
United States 2.4 GHz	32	36 (BSU) 32(SU)
World 2.4 GHz	100	100
World 2.3 GHz	100	100
World 2.5 GHz	100	100
Europe 2.4 GHz	20	20

📝:

- *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
Antenna Gain	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.  External antenna proxim RF Cable Surge Arrestor Surge Arrestor To Other Network Appliances To AC Power POE To AC Power Building Interior Calculate the antenna gain as follows: **Antenna Gain to be configured** = Antenna Gain of the antenna used - Cable Loss 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. Given this case, Configurable Antenna Gain = [23 dBi – 1 dB] = 22 dBi Maximum Radio Power = EIRP – Configured Antenna Gain = 30 dBm – 22 dBi = 8 dBm 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.

<table>
<tr><th>Parameter</th><th>Descriptions</th></tr>
<tr><td></td><td>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, <b>Radar signals may go undetected.</b> If the configured antenna gain is lower than the actual antenna gain, <b>False Radar may be detected.</b>

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.

Given below are the default Antenna Gain, for devices with integrated antenna:
<table>
<tr><th>Product (s)</th><th>Antenna Gain</th></tr>
<tr><td>MP-8250-BS1-G/ MP-8250-BS1</td><td>23 dBi</td></tr>
<tr><td>MP-8150-SUR-100</td><td>21 dBi</td></tr>
<tr><td>MP-8250-BS9-G/ MP-8250-BS9</td><td>16 dBi</td></tr>
<tr><td>MP-822-BSU-100
MP-822-SUA-100
MP-825-BS3-100
MP-825-SUR-50^{+}
MP-825-SUR-100
MP-825-CPE-50
MP-825-CPE-100
MP-835-CPE-10
MP-835-CPE-25
MP-835-CPE-50
MP-835-CPE-100</td><td>15 dBi</td></tr>
<tr><td>QB-8250-EPR-G/LNK-G
QB-8250-EPR/LNK</td><td>23 dBi</td></tr>
<tr><td>QB-825-EPR/LNK-50^{+}
QB-825-EPR/LNK-100
QB-835-EPR/LNK-25
QB-835-EPR/LNK-50
QB-826-EPR/LNK-100</td><td>15 dBi</td></tr>
</table>
</td></tr>
<tr><td>Wireless Inactivity Timer</td><td>Resets the wireless interface if there is no change in the Tx and Rx Packet Count in the specified interval of time. The default value is set to <b>5 seconds</b> (disabled if set to 0 seconds) and can be configured between 5 to 600 seconds.</td></tr>
</table>

Parameter	Descriptions
Legacy Mode	By default, Legacy Mode is disabled. When enabled, the MP 800 & 8000 BSU and SU devices can inter-operate with the legacy products of the Tsunami® MP.11 family. The MP 800 & 8000 devices that provide legacy support are, • MP-8100-SUA • MP-8150-SUR • MP-8150-SUR-100 • MP-8200-SUA • MP-8250-SUR • MP-820-SUA-50$^+$ • MP-820-SUA-100 • MP-822-SUA-100 • MP-825-SUR-50$^+$ • MP-825-SUR-100 • MP-825-CPE-50 • MP-825-CPE-100 • MP-835-CPE-10 • MP-835-CPE-25 • MP-835-CPE-50 • MP-835-CPE-100 *: MP 800/8000 BSU device in legacy mode can connect to a MP 800/8000 SU device only when configured in legacy mode.*

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.

5.4.3.2 Sync

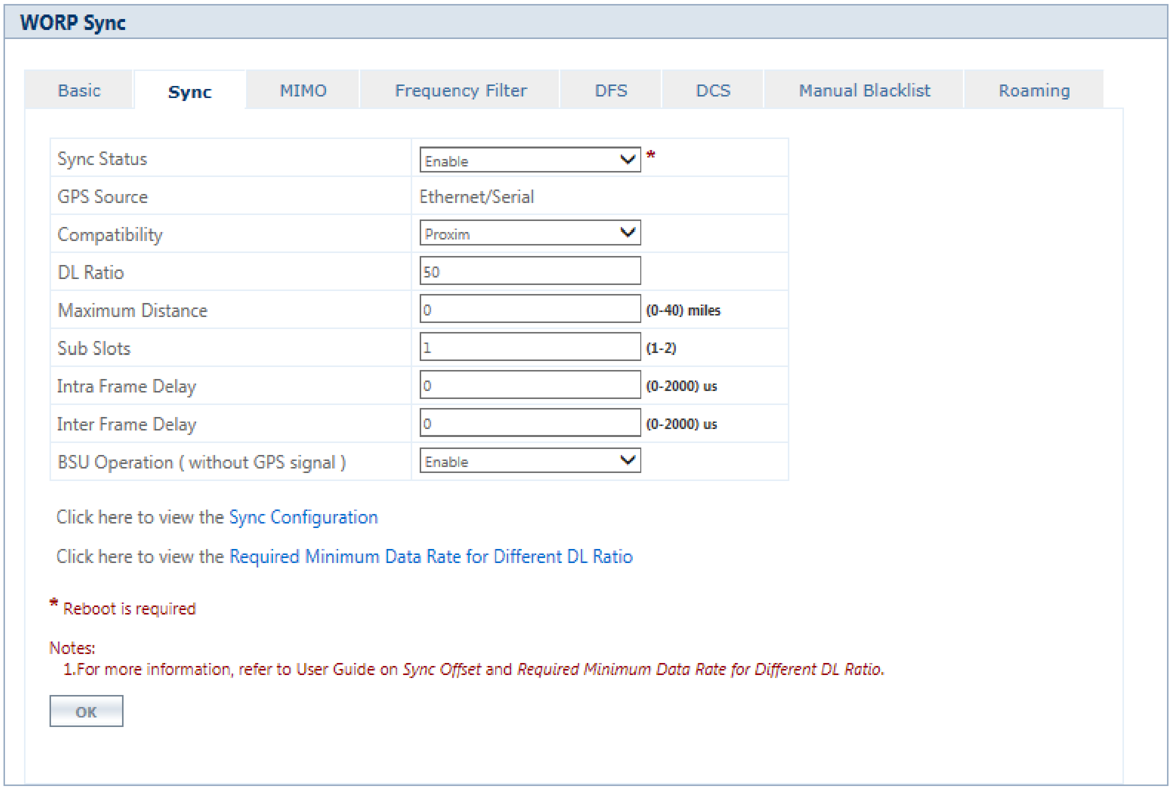
WORP Sync is a TDMA (Time Division Multiple Access) based implementation of the Proxim's proprietary Wireless Outdoor Routing Protocol which eliminates the co-location interference. With WORP Sync, all the BSU's transmission and reception are time-synchronized by means of GPS Synchronization techniques. This eliminates the co-location interference and improves the overall performance of the network.

: Sync tab is applicable only for a BSU and by default, it is in disabled state. Sync Status can be set to Enable/Disable by selecting an option from the drop-down menu.

For a BSU, Set the **Sync Status** to Enable, to configure or modify the Sync parameters.

Under the Sync tab, by default **Compatibility** is set to **Proxim**. Using the drop-down menu you can also select **Cambium-PMP** or **ePMF**. Based on the option selected, the corresponding WORP Sync screen appears as shown below.

5.4.3.2.1 Proxim



WORP Sync

Sync Status	Enable *
GPS Source	Ethernet/Serial
Compatibility	Proxim
DL Ratio	50
Maximum Distance	0 (0-40) miles
Sub Slots	1 (1-2)
Intra Frame Delay	0 (0-2000) us
Inter Frame Delay	0 (0-2000) us
BSU Operation (without GPS signal)	Enable

Click here to view the Sync Configuration

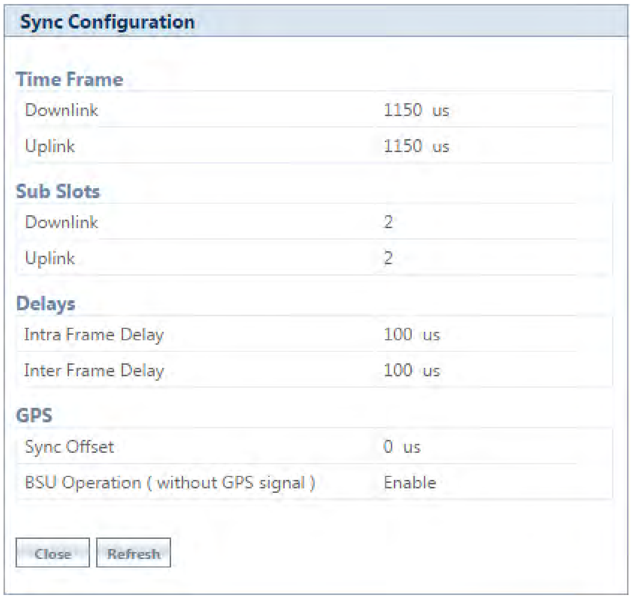
Click here to view the Required Minimum Data Rate for Different DL Ratio

* Reboot is required

Notes:
1.For more information, refer to User Guide on *Sync Offset* and *Required Minimum Data Rate for Different DL Ratio.*

Figure 5-35 WORP Sync (Proxim)

After configuring all the parameters, click **OK** and **COMMIT** the changes.To view the latest configuration, click on **Sync Configuration** at the bottom left corner of the WORP Sync screen. The following Sync configuration screen appears for Proxim mode.

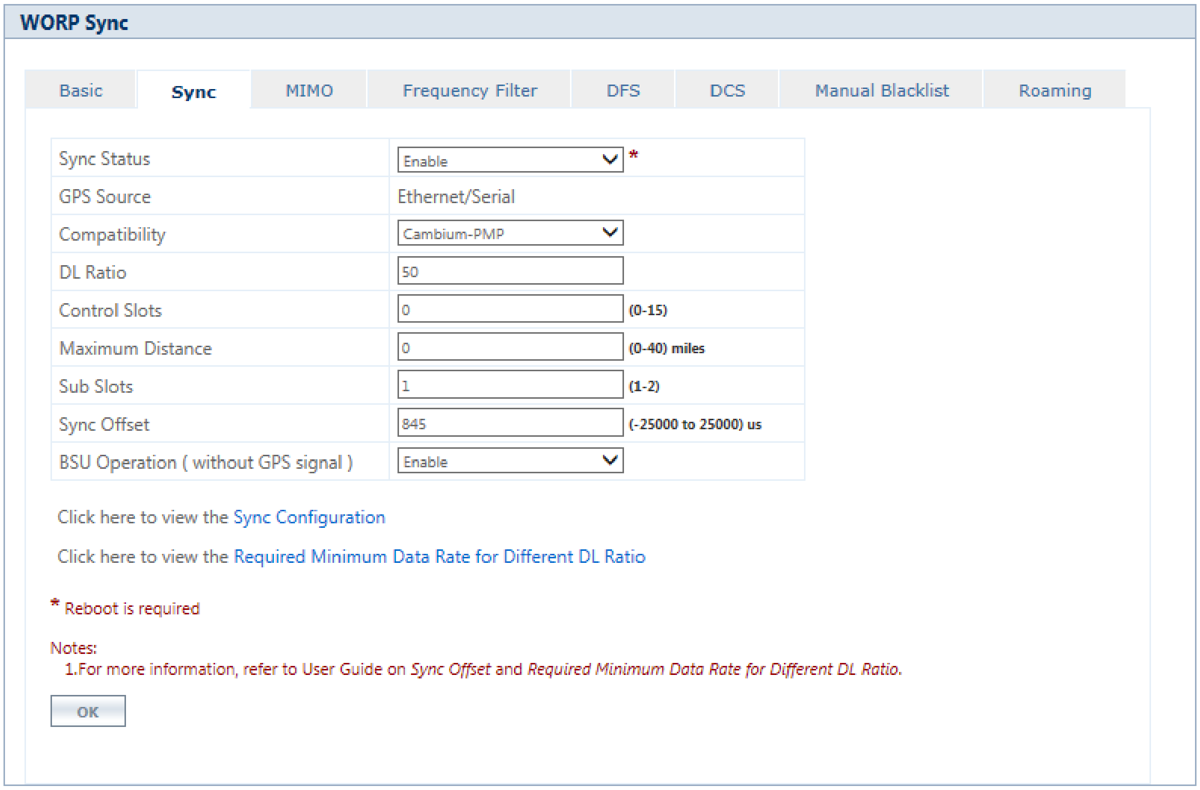


Sync Configuration

Time Frame	
Downlink	1150 us
Uplink	1150 us
Sub Slots	
Downlink	2
Uplink	2
Delays	
Intra Frame Delay	100 us
Inter Frame Delay	100 us
GPS	
Sync Offset	0 us
BSU Operation (without GPS signal)	Enable

Figure 5-36 Sync Configuration (Proxim)

5.4.3.2.2 Cambium-PMP



Sync Status	Enable *
GPS Source	Ethernet/Serial
Compatibility	Cambium-PMP
DL Ratio	50
Control Slots	0 (0-15)
Maximum Distance	0 (0-40) miles
Sub Slots	1 (1-2)
Sync Offset	845 (-25000 to 25000) us
BSU Operation (without GPS signal)	Enable

Click here to view the Sync Configuration

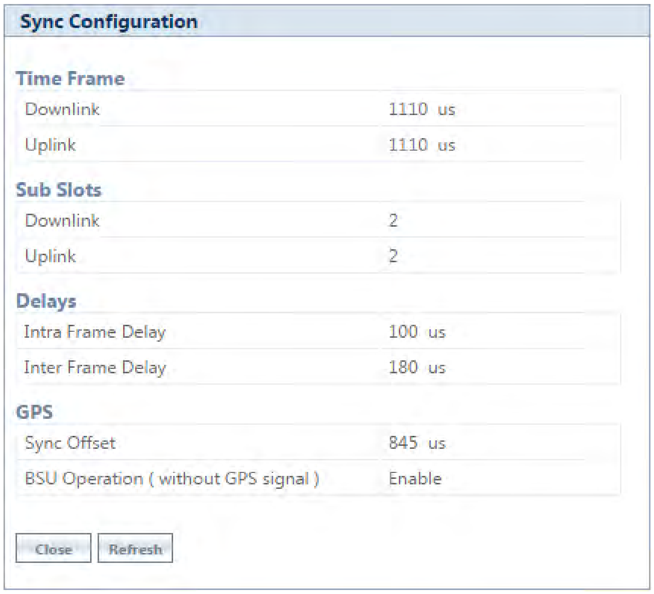
Click here to view the Required Minimum Data Rate for Different DL Ratio

* Reboot is required

Notes:
1.For more information, refer to User Guide on *Sync Offset* and *Required Minimum Data Rate for Different DL Ratio*.

Figure 5-37 WORP Sync (Cambium-PMP)

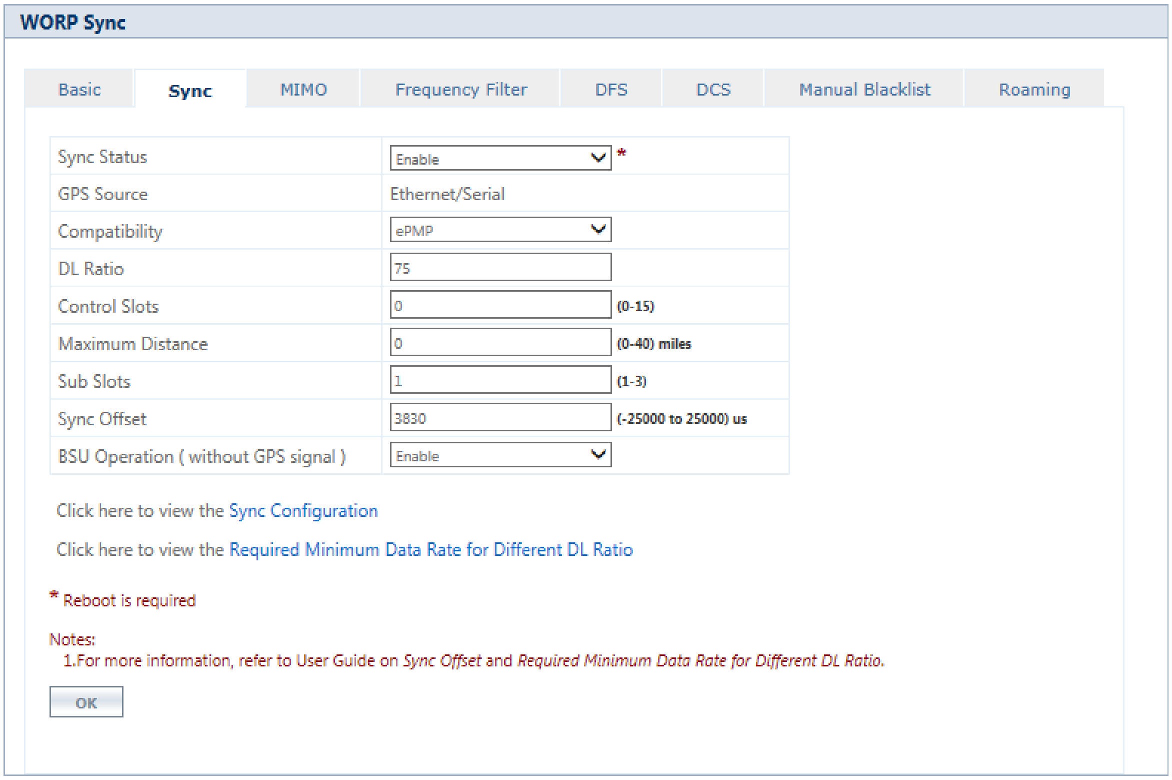
After configuring all the parameters, click **OK** and **COMMIT** the changes.To view the latest configuration, click on **Sync Configuration** at the bottom left corner of the WORP Sync screen. The following Sync configuration screen appears for Proxim/Cambium-PMP compatibility mode.



Time Frame	
Downlink	1110 us
Uplink	1110 us
Sub Slots	
Downlink	2
Uplink	2
Delays	
Intra Frame Delay	100 us
Inter Frame Delay	180 us
GPS	
Sync Offset	845 us
BSU Operation (without GPS signal)	Enable

Figure 5-38 Sync Configuration (Cambium-PMP)

5.4.3.2.3 ePMP



WORP Sync

Sync Status	Enable	*
GPS Source	Ethernet/Serial	
Compatibility	ePMP	
DL Ratio	75	
Control Slots	0	(0-15)
Maximum Distance	0	(0-40) miles
Sub Slots	1	(1-3)
Sync Offset	3830	(-25000 to 25000) us
BSU Operation (without GPS signal)	Enable	

Click here to view the Sync Configuration

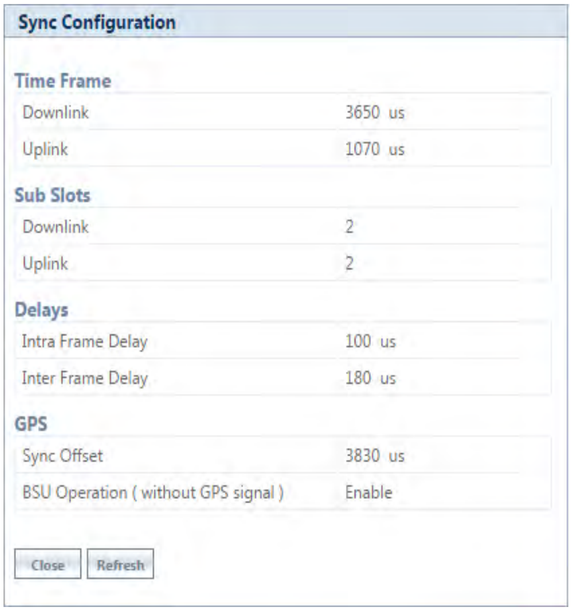
Click here to view the Required Minimum Data Rate for Different DL Ratio

* Reboot is required

Notes:
1.For more information, refer to User Guide on *Sync Offset* and *Required Minimum Data Rate for Different DL Ratio*.

Figure 5-39 WORP Sync (ePMP)

After configuring all the parameters, click **OK** and **COMMIT** the changes.To view the latest configuration, click on **Sync Configuration** at the bottom left corner of the WORP Sync screen. The following Sync configuration screen appears for Proxim/Cambium-PMP/ePMP compatibility mode.

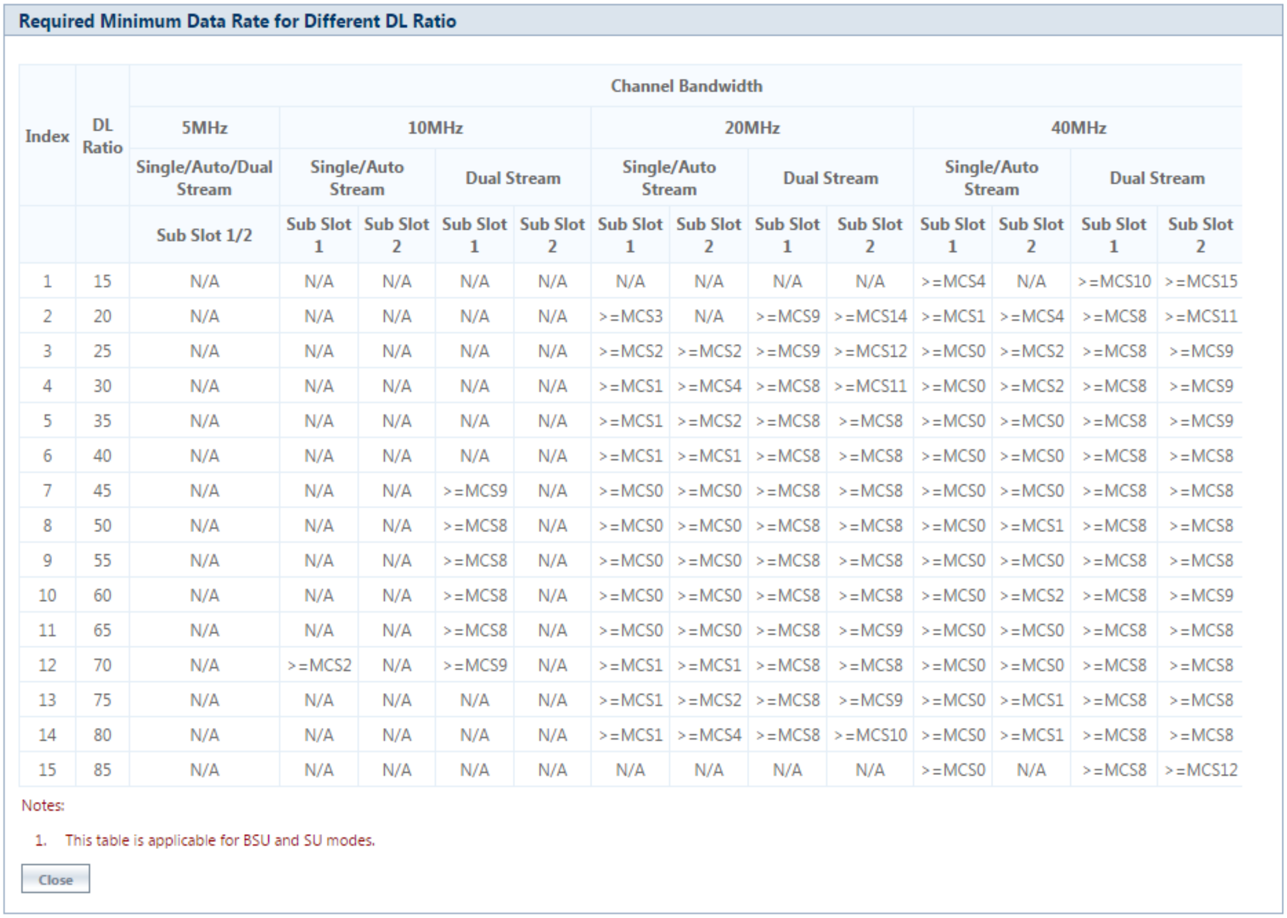


Sync Configuration

Time Frame	
Downlink	3650 us
Uplink	1070 us
Sub Slots	
Downlink	2
Uplink	2
Delays	
Intra Frame Delay	100 us
Inter Frame Delay	180 us
GPS	
Sync Offset	3830 us
BSU Operation (without GPS signal)	Enable

Figure 5-40 Sync Configuration (ePMP)

To view the Sync configuration support for **PROXIM/Cambium-PMP/ePMP** compatibility modes at different data rates for various bandwidths, click on **Required Minimum Data Rate for Different DL Ratio** at the bottom left corner of the WORP Sync screen. The following screen appears for Proxim/Cambium-PMP compatibility mode.



Required Minimum Data Rate for Different DL Ratio

Index	DL Ratio	Channel Bandwidth												
		5MHz	10MHz				20MHz				40MHz			
		Single/Auto/Dual Stream	Single/Auto Stream		Dual Stream		Single/Auto Stream		Dual Stream		Single/Auto Stream		Dual Stream	
		Sub Slot 1/2	Sub Slot 1	Sub Slot 2	Sub Slot 1	Sub Slot 2	Sub Slot 1	Sub Slot 2	Sub Slot 1	Sub Slot 2	Sub Slot 1	Sub Slot 2	Sub Slot 1	Sub Slot 2
1	15	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	>=MCS4	N/A	>=MCS10	>=MCS15
2	20	N/A	N/A	N/A	N/A	N/A	>=MCS3	N/A	>=MCS9	>=MCS14	>=MCS1	>=MCS4	>=MCS8	>=MCS11
3	25	N/A	N/A	N/A	N/A	N/A	>=MCS2	>=MCS2	>=MCS9	>=MCS12	>=MCS0	>=MCS2	>=MCS8	>=MCS9
4	30	N/A	N/A	N/A	N/A	N/A	>=MCS1	>=MCS4	>=MCS8	>=MCS11	>=MCS0	>=MCS2	>=MCS8	>=MCS9
5	35	N/A	N/A	N/A	N/A	N/A	>=MCS1	>=MCS2	>=MCS8	>=MCS8	>=MCS0	>=MCS0	>=MCS8	>=MCS9
6	40	N/A	N/A	N/A	N/A	N/A	>=MCS1	>=MCS1	>=MCS8	>=MCS8	>=MCS0	>=MCS0	>=MCS8	>=MCS8
7	45	N/A	N/A	N/A	>=MCS9	N/A	>=MCS0	>=MCS0	>=MCS8	>=MCS8	>=MCS0	>=MCS0	>=MCS8	>=MCS8
8	50	N/A	N/A	N/A	>=MCS8	N/A	>=MCS0	>=MCS0	>=MCS8	>=MCS8	>=MCS0	>=MCS1	>=MCS8	>=MCS8
9	55	N/A	N/A	N/A	>=MCS8	N/A	>=MCS0	>=MCS0	>=MCS8	>=MCS8	>=MCS0	>=MCS0	>=MCS8	>=MCS8
10	60	N/A	N/A	N/A	>=MCS8	N/A	>=MCS0	>=MCS0	>=MCS8	>=MCS8	>=MCS0	>=MCS2	>=MCS8	>=MCS9
11	65	N/A	N/A	N/A	>=MCS8	N/A	>=MCS0	>=MCS0	>=MCS8	>=MCS9	>=MCS0	>=MCS0	>=MCS8	>=MCS8
12	70	N/A	>=MCS2	N/A	>=MCS9	N/A	>=MCS1	>=MCS1	>=MCS8	>=MCS8	>=MCS0	>=MCS0	>=MCS8	>=MCS8
13	75	N/A	N/A	N/A	N/A	N/A	>=MCS1	>=MCS2	>=MCS8	>=MCS9	>=MCS0	>=MCS1	>=MCS8	>=MCS8
14	80	N/A	N/A	N/A	N/A	N/A	>=MCS1	>=MCS4	>=MCS8	>=MCS10	>=MCS0	>=MCS1	>=MCS8	>=MCS8
15	85	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	>=MCS0	N/A	>=MCS8	>=MCS12

Notes:

1. This table is applicable for BSU and SU modes.

Figure 5-41 Required Minimum Data Rate for Different DL Ratio & Sub-slot configurations

The WORP Sync screen parameters are described and tabulated below:

Parameter	Descriptions
Sync Status	By default it is enabled on a BSU.
GPS Source	This parameter will change based on the GPS source. • Set to **Serial** if **Garmin module** is used. • Set to **Ethernet** if **CTM2 module** (**CMM or CMM Micro**) is used. : *For **82xx** series, it is a read-only parameter as the hardware pin configuration for Serial and Ethernet ports remain the same; however, for **82x series**, it is a variable parameter due to the varied hardware pin configuration.*

<table>
<tr><th>Parameter</th><th>Descriptions</th></tr>
<tr><td>Compatibility</td><td>
<p>By default it is set to <b>Proxim</b>. It is used when the network cluster has only Proxim BSUs.</p>
<p>Set <b>Cambium-PMP</b> if the devices have to co-exist with Cambium-PMP Base Stations in the network. If this option is selected, configure the <b>Sync offset</b> field.</p>
<p>Set <b>ePMP</b> if the devices have to co-exist with Cambium-ePMP Base Stations in the network. If this option is selected, configure the <b>Sync offset</b> field.</p>
<p>: <i>Cambium doesnot support the synchronization of the co-located PMP and ePMP base stations on the same tower.</i></p>
<p>The time frame for the various options are given below:</p>
<table>
<tr><th>Compatibility Mode</th><th>Time Frame (micro sec)</th></tr>
<tr><td>Proxim</td><td>2500</td></tr>
<tr><td>Cambium-PMP</td><td>2500</td></tr>
<tr><td>ePMP</td><td>5000</td></tr>
</table>
</td></tr>
<tr><td>DL Ratio</td><td>
<p>This parameter specifies the time allocated for <b>downlink</b> transmission in terms of percentage, for <b>uplink</b> transmission, it is internally derived based on the DL ratio.</p>
<p>For <b>Proxim</b> and <b>Cambium-PMP</b> compatibility modes:</p>
<p>UL (Uplink) Ratio = 100 - DL (Downlink) Ratio</p>
<p>Delays = Inter Frame Delay + Intra Frame Delay</p>
<p>DL Time Frame = ((Time Frame - Delays) * DL ratio)) / 100</p>
<p>UL Time Frame = ((Time Frame - Delays) * UL ratio)) / 100</p>
<p>By default it is set to <b>50</b>. The configurable values: <b>15</b> - <b>85</b>;It will be in multiples of 5.</p>
<p>For <b>ePMP</b> compatibility mode:</p>
<p>UL (Uplink) Ratio = 100 - DL (Downlink) Ratio
DL Time Frame = ((Time Frame * DL ratio) / 100) - Intra Frame Delay
UL Time Frame = ((Time Frame * UL ratio) / 100) - Inter Frame Delay</p>
<p>By default it is set to 75. The configurable values are: 30, 50, 75</p>
</td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Descriptions</th></tr>
<tr><td>Sub Slots</td><td>The Sub-slots values for all the compatibility modes are tabulated below:
<table><tr><th>Compatibility Mode</th><th>Default Value</th><th>Configurable Values</th></tr><tr><td>Proxim</td><td>1</td><td>1&2</td></tr><tr><td>Cambium-PMP</td><td>1</td><td>1&2</td></tr><tr><td>ePMP</td><td>1</td><td>1,2 & 3</td></tr></table>
: <i>Before configuring the sub-slot value to more than, 2 - please check the <b>Minimum required data rate Table 5-41</b>, to know, if it supports the corresponding DL ratio or not. Exempting this would lead to issues related to link establishment through WORP. Also, configure the DDRS minimum data rate as per the table, when the DDRS is enabled.</i></td></tr>
<tr><td>Inter Frame Delay</td><td>This parameter specifies the time interval between two time frames.</td></tr>
<tr><td>Intra Frame Delay</td><td>This parameter specifies the time interval between DL (Downlink) and UL (Uplink) time frames.</td></tr>
<tr><td>Control Slots</td><td>This parameter is applicable only to <b>Cambium-PMP & ePMP</b> compatibility modes. By default, it is set to <b>0</b>. The configurable values: <b>0</b> - <b>15</b>.
Intra Frame Delay = 100 + (Control Slots * 10)</td></tr>
<tr><td>Max Distance</td><td>By default it is set to <b>0</b>. The configurable values: <b>0</b> - <b>40</b> miles.
Inter Frame Delay =100 + (max_distance -2) * 10</td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Descriptions</th></tr>
<tr><td>Sync offset</td><td>
The Sync offset values are tabulated below:

The values given in the first table are applicable for the <b>Cambium-PMP</b> compatibility mode:
<table>
<tr><th rowspan="2">Sync Hardware Module</th><th colspan="2">8200 Sync Offset Value ((µs) in microseconds)</th><th colspan="2">820 Sync Offset Value ((µs) in microseconds)</th></tr>
<tr><th>30% and 50% DL</th><th>75%DL</th><th>30% and 50% DL</th><th>75%DL</th></tr>
<tr><td>CMM</td><td>3470</td><td>3870</td><td>3440</td><td>3840</td></tr>
<tr><td>CTM2</td><td>3420</td><td>3820</td><td>3390</td><td>3790</td></tr>
<tr><td>GPS 16x</td><td>3590</td><td>3990</td><td>3560</td><td>3960</td></tr>
</table>

The values given in the tables below are applicable for the <b>ePMP</b> compatibility mode:
<b>For MP-8200 devices</b>
<table>
<tr><th></th><th>30% DL</th><th>50% DL</th><th>75% DL</th></tr>
<tr><td>16x GPS</td><td>3590</td><td>3590</td><td>3990</td></tr>
<tr><td>CTM2</td><td>3420</td><td>3420</td><td>3820</td></tr>
<tr><td>CMM</td><td>3470</td><td>3470</td><td>3870</td></tr>
</table>

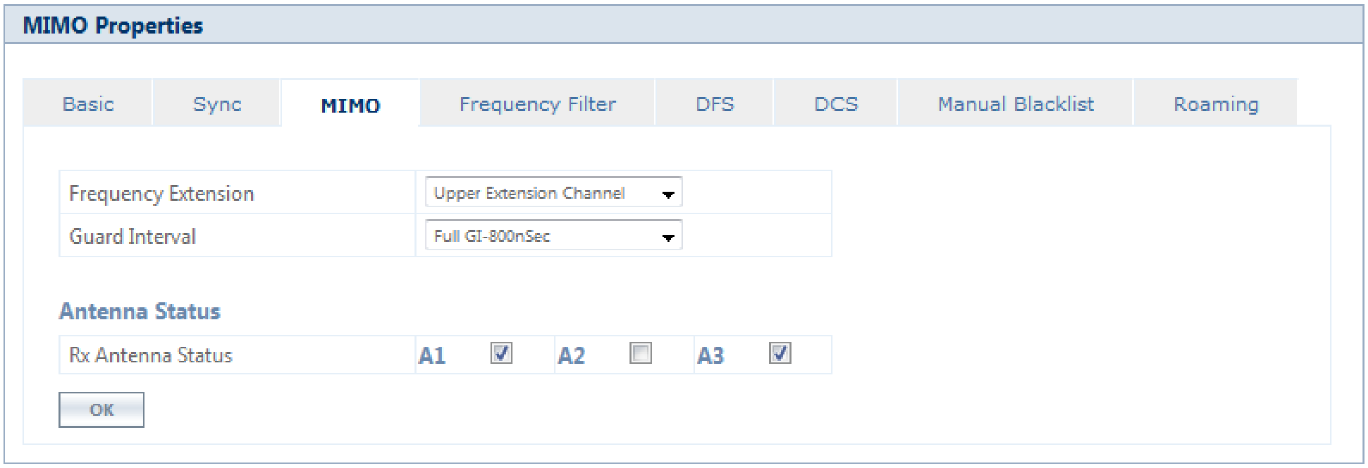
<b>For MP-820 devices</b>
<table>
<tr><th></th><th>30% DL</th><th>50% DL</th><th>75% DL</th></tr>
<tr><td>16x GPS</td><td>3560</td><td>3560</td><td>3960</td></tr>
<tr><td>CTM2</td><td>3390</td><td>3390</td><td>3790</td></tr>
<tr><td>CMM</td><td>3440</td><td>3440</td><td>3840</td></tr>
</table>
</td></tr>
<tr><td>BSU Operation (without GPS signal)</td><td>
This parameter defines the BSU operation when the GPS signal is not available. By default it is set to <b>Enable</b>. The configurable options: <b>Enable</b> and <b>Disable</b>, for both the options, GPS pulse is used for time synchronization.
<ul>
<li><b>Enable</b>:
<ul>
<li>The BSU operates normally even if five consecutive GPS pulses are missed as the internal clock synchronizes itself with the last received pulse.</li>
<li>In case of no GPS pulse at all, the internal clock is used.</li>
</ul></li>
<li><b>Disable</b>: If five consecutive GPS pulses are missed, the BSU is disabled to avoid interference to the nearby sectors.</li>
</ul>
</td></tr>
</table>

:

- *WORP Sync version supports fixed data rates and DDRS (Dynamic Data Rate Selection).*
- *In Cambium-PMP & ePMP mode, configure the Control Slots value based on the configuration of the Cambium devices. The Control Slots and Maximum Distance configuration values are internally required to calculate the Intra and Inter Frame Delays, and also to ensure proper synchronization timing between the Proxim and Cambium systems.*

5.4.3.3 MIMO

The **MIMO Properties** tab allows you to configure the Multiple-Input-Multiple-Output (MIMO) parameters to achieve high throughput and longer range. The **MIMO** screen appears as shown below.



Frequency Extension: Upper Extension Channel

Guard Interval: Full GI-800nSec

Antenna Status

Rx Antenna Status: A1 ☑ A2 □ A3 ☑

Figure 5-42 MIMO Properties

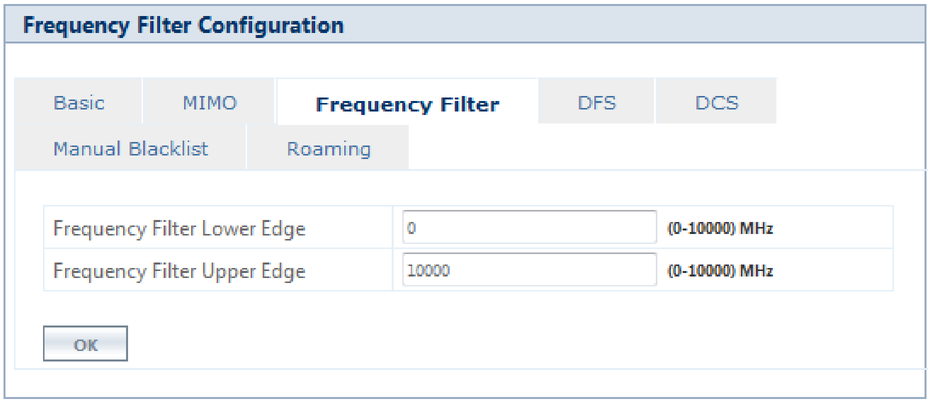
Parameter	Description
Frequency Extension	Frequency Extension is applicable only when the Channel Bandwidth is set to 40 MHz. While choosing 40MHz bandwidth, you can select either 40 PLUS (Upper Extension Channel) or 40 MINUS (Lower Extension Channel). 40 PLUS means the center frequency calculation is 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.

Parameter	Description
Guard Interval	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. In 802.11 standards, when 40 MHz Channel Bandwidth is configured then Short GI can be used to improve the overall performance and throughout. By default, Full GI is enabled for 5 MHz, 10 MHz and 20 MHz channels. : • *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	Allows the user to select the antenna(s) for receiving data. Select the check-box against each antenna(s) for receiving data and click **OK**. : *Atleast two Rx antenna ports should be enabled when data stream is dual or auto.*

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

5.4.3.4 Frequency Filter

The **Frequency Filter** tab allows you to configure 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. The **Frequency Filter Configuration** screen appears as shown below.



Frequency Filter Lower Edge	0	(0-10000) MHz
Frequency Filter Upper Edge	10000	(0-10000) MHz

Figure 5-43 Frequency Filter Configuration

The frequency range limit for the filter lower and upper edge is **0 - 10000 MHz**; by default, the lower frequency edge is set to 0 MHz and the upper frequency edge is set to 10000 MHz. Configure the values and Click **OK** and then **COMMIT**.

5.4.3.5 Dynamic Frequency Selection (DFS)

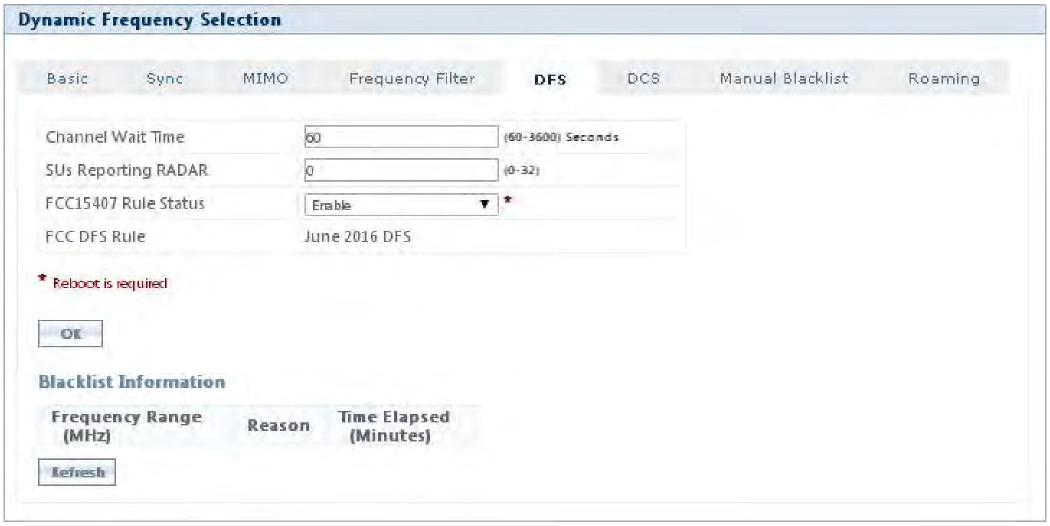
The Tsunami® products support Dynamic Frequency Selection (DFS) for FCC, IC, and ETSI regulatory domains per FCC Part 15 Rules for U-NII devices, IC RSS-210, and ETSI EN 301-893 regulations, respectively. These rules and regulations require that the devices operating in the 5 GHz band must use DFS to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

: For US DFS countries:

- *Units deployed after June 2016, United States 5.3 GHz and 5.4 GHz band follows the DFS FCC15407 Rule.*
- *Units sold or deployed before June 2016, the user can either use the existing DFS Rule or configure the DFS FCC15407 Rule from the drop-down menu. After configuration click **OK**, **COMMIT** and then **REBOOT**.*

5.4.3.5.1 DFS in BSU or End Point A mode

Under the **DFS** tab for a BSU / End Point A, you can configure and view the following parameters.



Dynamic Frequency Selection

Channel Wait Time	60	(60-3600) Seconds
SUs Reporting RADAR	0	(0-32)
FCC15407 Rule Status	Enable ▼	*
FCC DFS Rule	June 2016 DFS	

* Reboot is required

Blacklist Information

Frequency Range (MHz)	Reason	Time Elapsed (Minutes)

Figure 5-44 Dynamic Frequency Selection (BSU / End Point A)

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.

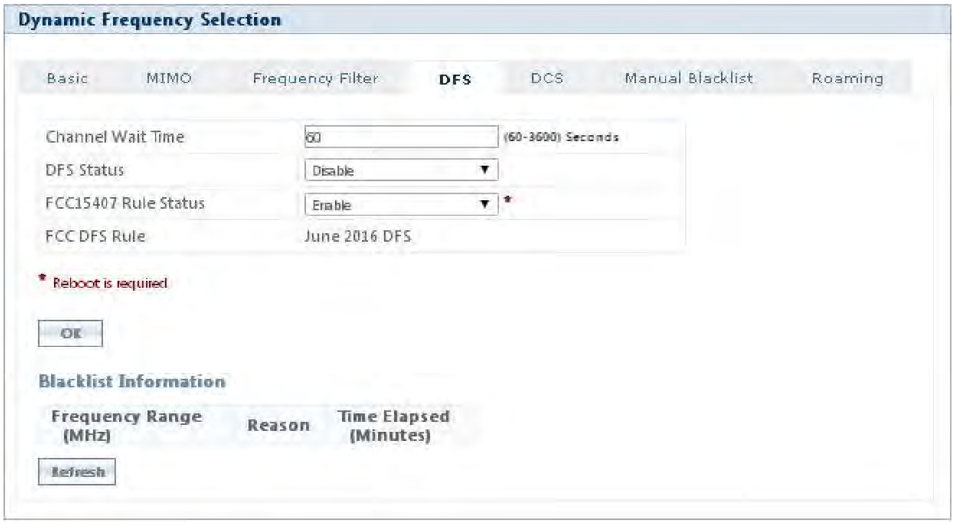
   - If ACS is enabled, then the device scans all the channels and selects the channel with the best RSSI to be the operational channel.
3. Once the operating channel is selected, the device scans the channel for the presence of the RADAR for a duration of the configured Channel Wait Time (by default, configured 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 PointA's channel and associates automatically.*

5.4.3.5.2 DFS in SU or End Point B Mode

Under the **DFS** tab for a SU / End Point B, you can configure and view the following parameters.



Channel Wait Time	60 (60-3600) Seconds
DFS Status	Disable
FCC15407 Rule Status	Enable *
FCC DFS Rule	June 2016 DFS

* Reboot is required

Blacklist Information

Frequency Range (MHz)	Reason	Time Elapsed (Minutes)

Figure 5-45 Dynamic Frequency Selection (SU / End Point B)

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.*

Parameter	Description
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.

For detailed information on DFS enabled countries, see Frequency Domains and Channels.

Blacklist Information

The parameters under Blacklisted Information are described in the table given below.

Parameter	Description
Frequency Range	Indicates the blacklisted channel in terms of frequency range.

Parameter	Description
Reason	Specifies the reason for blacklisting a frequency range. Following are the reasons for blacklisting a frequency range: **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, frequencies that are not usable because they fall in the other, radar / manual blacklisted frequency range. For example, if channel 110 is blacklisted, then channels 107 to 113 will become unusable for 20 MHz bandwidth. That is, in terms of frequency range, (5540 - 5560) MHz is blacklisted. 5. **Manual**: A frequency range is manually blacklisted by the administrator.
Time Elapsed	This parameter specifies the time elapsed since the frequency range was blacklisted due to radar / interference. When the frequency range is blacklisted it will be white listed after 30 minutes. This parameter is applicable for radar and interference blacklisted frequency range only.

Click **Refresh**, to view updated / refreshed blacklisted frequency range.

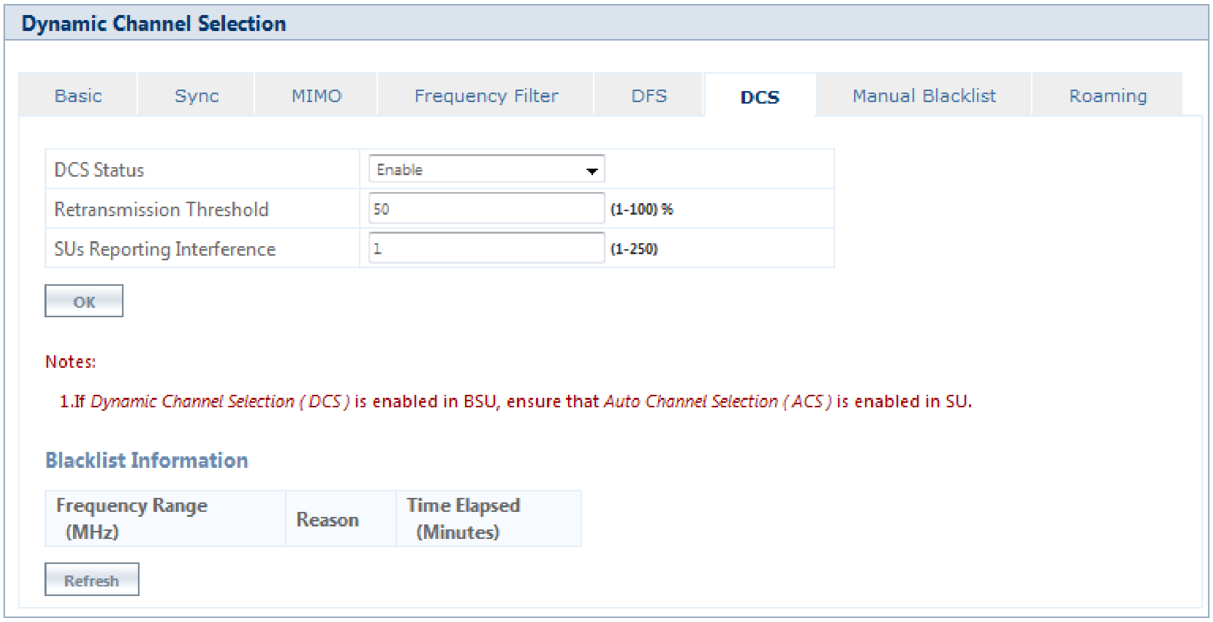
After configuring the required parameters, click **OK** and then **COMMIT**.

5.4.3.6 Dynamic Channel Selection (DCS)

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 without terminating the link.

5.4.3.6.1 DCS in BSU / End Point A Mode

Under the **DCS** tab for a BSU / End Point A, you can configure and view the following parameters.



Dynamic Channel Selection

DCS Status	Enable	
Retransmission Threshold	50	(1-100) %
SUs Reporting Interference	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

Frequency Range (MHz)	Reason	Time Elapsed (Minutes)

Figure 5-46 Dynamic Channel Selection (BSU or End Point A)

Explained below is the DCS functionality and the way it operates on (BSU / End Point A) devices.

- **DCS Status** can be set to enable/disable by selecting an option from the drop-down menu. By default, it is in disabled state.
- When DCS is enabled, the device periodically monitors the channel for link quality. In case of interference, this feature automatically changes the current operating channel.
- The channel change is triggered,
  - When the percentage of retransmissions computed exceeds the configured **Retransmission Threshold** value.

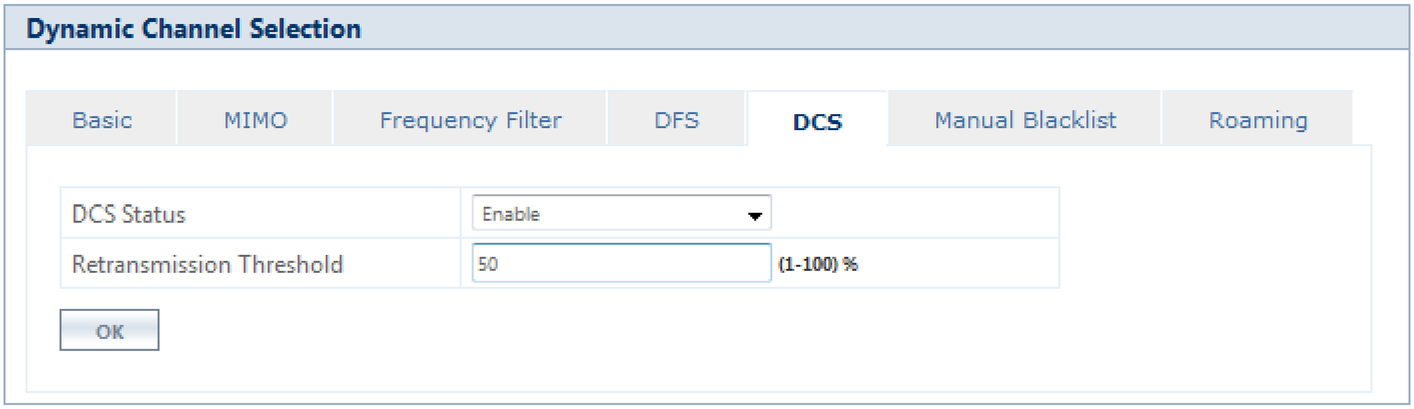
    (**or**)
  - The number of SUs reporting bad channel equals or exceeds the configured **SUs Reporting Interference** value.
- If one of the above conditions is satisfied then the current operating channel will be blacklisted for 30 Minutes (due to interference), and the BSU will switch to the next available channel.
- 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.*
- *For DCS to work, the channel list should have more than one available channel.*

5.4.3.6.2 DCS in SU / End Point B Mode

Under the **DCS** tab for a SU / End Point B, you can configure and view the following parameters.



DCS Status	Enable
Retransmission Threshold	50 (1-100) %

Figure 5-47 Dynamic Channel Selection (SU or End Point B)

Explained below is the DCS functionality and the way it operates on (SU / End Point B) devices.

- **DCS Status** can be set to enable/disable by selecting an option from the drop-down menu. 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 above the threshold, the SU continues to operate in the same channel.
  - If the link quality is bad, the SU will trigger DCS message with reason code as interference to the connected BSU.

: *SU will not blacklist the channels due to interference.*

Given below is the table which explains **Dynamic Channel Selection** (**DCS**) parameters and the method to configure the configurable parameter(s):

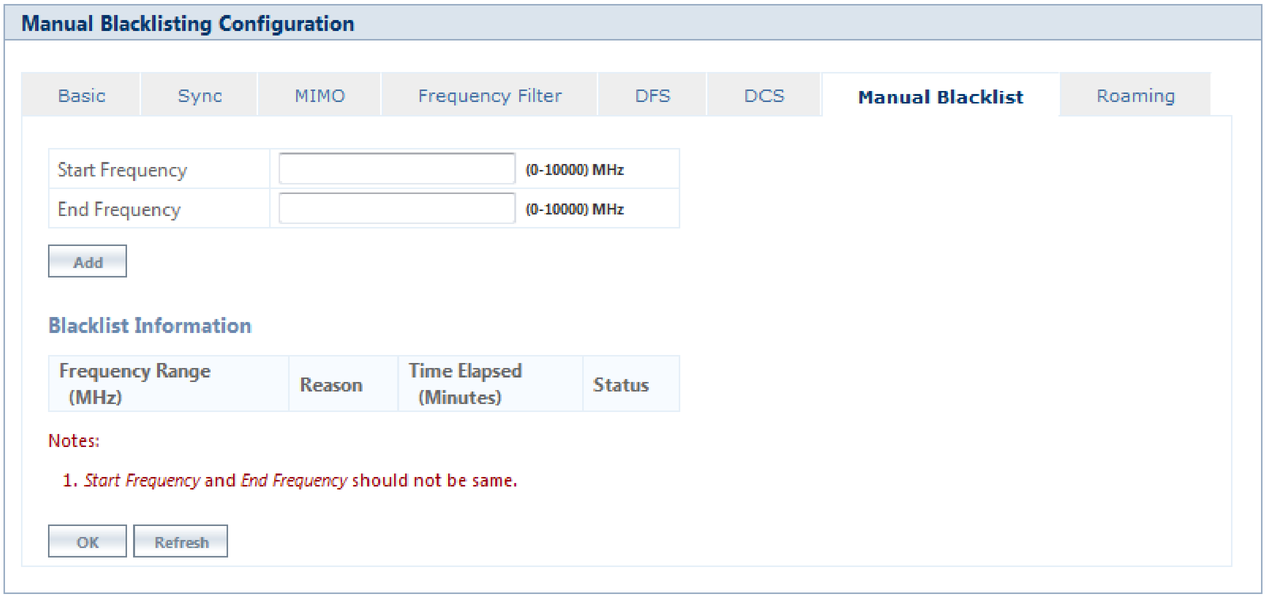
Parameter	Description
Dynamic Channel Selection (DCS) Status	This parameter is used to enable DCS on the device. By default, DCS is disabled. To enable, select **Enable** and Click **OK**.
Retransmission Threshold	This parameter enables to configure the retransmission threshold percentage on the device. 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. By default, the retransmission percentage is set to **50**.
SUs Reporting Interference	Applicable only to BSU. The BSU decides to blacklist the operating channel based on the value configured for this parameter. If the number of SUs reporting interference (Between BSU and SU) equals or exceeds the configured value of this parameter then the channel is blacklisted. Else, it continues to operate in the same channel. By default, **Bad Link Threshold** value is set to **1**.
Blacklist Information	Refer **Blacklist Information**, for detailed explanation.

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

Click **Refresh**, to view updated / refreshed blacklisted frequency range.

5.4.3.7 Manual Blacklist

Manual Blacklisting enables you to manually blacklist one or more channels in terms of frequency range for the following reasons: radar, interference, and to reduce the number of channels to scan. The **Manual Blacklist** screen appears as shown below.



Start Frequency (0-10000) MHz
End Frequency (0-10000) MHz

Blacklist Information

Frequency Range (MHz)	Reason	Time Elapsed (Minutes)	Status

Notes:

1. *Start Frequency* and *End Frequency* should not be same.

Figure 5-48 Manual Blacklist

To manually blacklist a frequency range, enter the start and end frequency in the **Start Frequency** and **End Frequency** boxes respectively. Next, click **Add**. All the selected frequency ranges are added to the **Blacklist Information** table. After configuring the required parameters, click **OK** and then **COMMIT**. Click **Refresh**, to view updated/refreshed manually blacklisted frequency range. For detailed explanation of Blacklist Information, please refer **Blacklist Information**.

However, there are few conditions to be followed while manually blacklisting a channel:

- 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, at least one channel or its sub-channels that are part of the current channel bandwidth should be available for operation. That is, all the frequencies cannot be blacklisted.

✎:

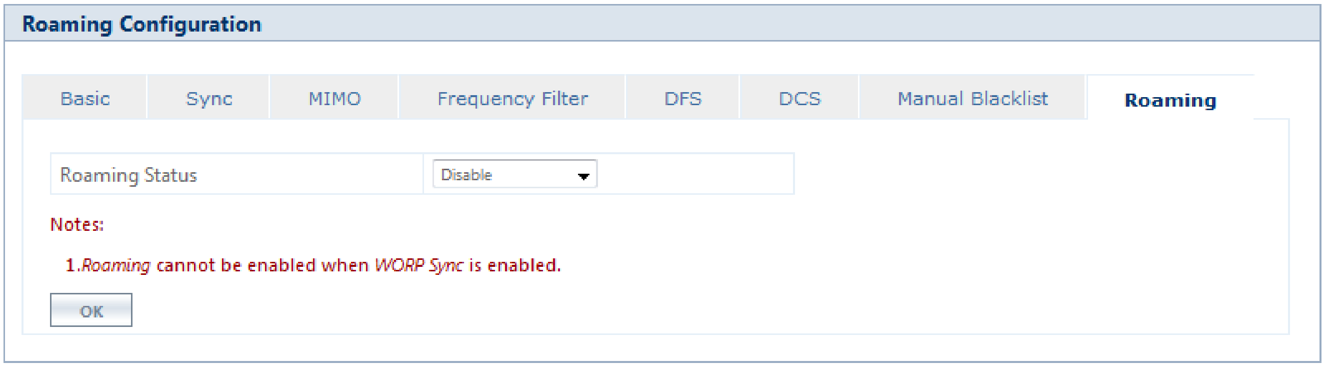
- *Only manually blacklisted frequencies can be de-blacklisted.*
- *If a manually blacklisted frequency range overlaps with the operating channel then the WORP link will be terminated and the BSU will trigger channel selection procedure.*
- *Manually blacklisted frequency information is not exchanged between the BSU and SU as it local to the device.*

5.4.3.8 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.

✎: *Roaming feature is not applicable to devices operating in* ***WORP Sync*** *mode; by default, it is disabled.*

The Roaming Configuration screen appears as follows.

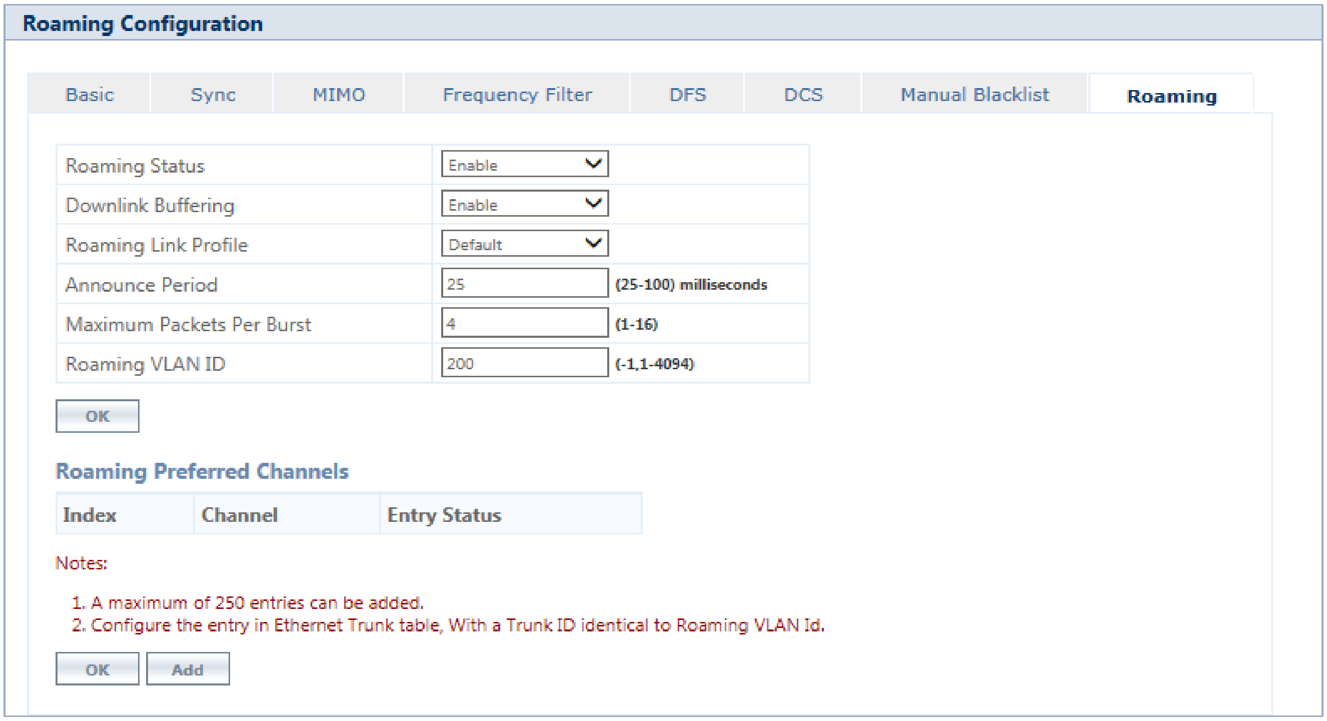


Roaming Status: Disable

Notes:

1. *Roaming* cannot be enabled when *WORP Sync* is enabled.

Figure 5-49 Roaming (WORP Sync Mode)



Roaming Status	Enable	
Downlink Buffering	Enable	
Roaming Link Profile	Default	
Announce Period	25	(25-100) milliseconds
Maximum Packets Per Burst	4	(1-16)
Roaming VLAN ID	200	(-1,1-4094)

Roaming Preferred Channels

Index	Channel	Entry Status

Notes:

1. A maximum of 250 entries can be added.
2. Configure the entry in Ethernet Trunk table, With a Trunk ID identical to Roaming VLAN Id.

Figure 5-50 Roaming

Parameter	Description
Roaming Status	The Roaming feature can either be enabled or disabled on a BSU. By default, it is disabled. When the roaming status is enabled on a BSU, the other roaming parameters such as Roaming Link Profile, Downlink Buffering, Announce Period, Maximum Packets Per Burst and Roaming VLAN ID are configurable. These parameters are used by the registered SU when any of the roaming procedure starts. ✎: *Roaming can be enabled on the BSU, independent of the roaming status of the SU.*
Downlink Buffering	This parameter provides support to buffer the downlink traffic from BSU to SU. This buffered traffic is sent to the Roaming SU through a newly associated BSU, using the Inter BSU protocol.
Roaming Link Profile	This parameter enables you to configure a roaming link profile for the roaming enabled SUs. 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. When roaming is disabled on the BSU, the SUs are mapped to the corresponding profile from the SU Profiles list.

Parameter	Description
Announce Period	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. When roaming is disabled on a BSU, the Announce period is set to 150 milliseconds. : *Reducing the Announce Period improves the roaming time and may result in lower throughput.*
Max. Packets Per Burst	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. When roaming is disabled on a BSU, the maximum packets per burst is set to 4. : • *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.*
Roaming VLAN ID	This parameter enables the user to configure the VLAN ID for Roaming management frames. By default, the Roaming VLAN ID is set to -1 which indicates no tag is added to the Roaming management frame. To set VLAN tag to the Roaming management frame, enter a value ranging from 1 to 4094.
After configuring the above parameters, click **OK** and then **COMMIT**.	

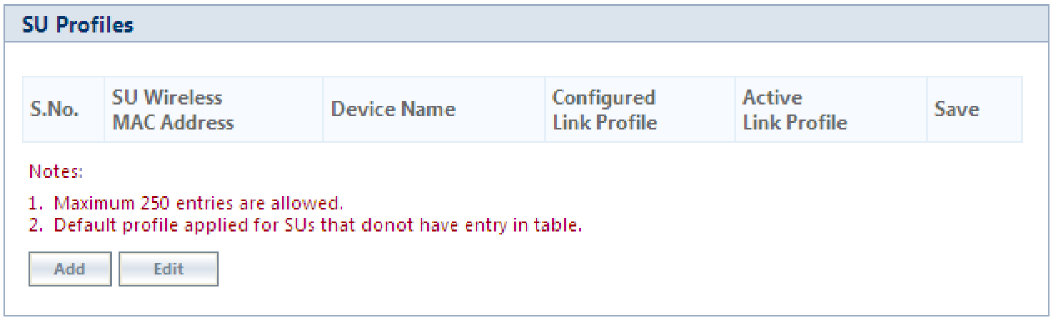
5.4.4 BSU / SU Profiles

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.

5.4.4.1 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:



SU Profiles

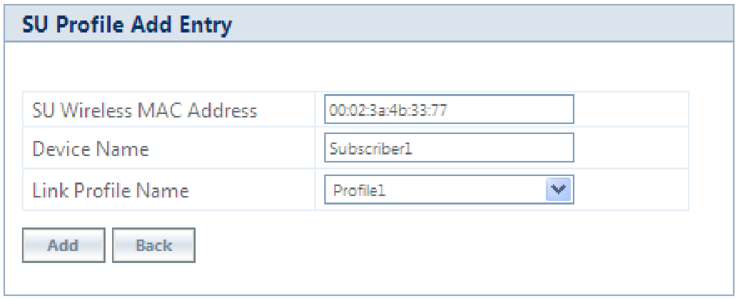
S.No.	SU Wireless MAC Address	Device Name	Configured Link Profile	Active Link Profile	Save

Notes:

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

Figure 5-51 SU Profiles

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



SU Profile Add Entry

SU Wireless MAC Address	00:02:3a:4b:33:77
Device Name	Subscriber1
Link Profile Name	Profile1

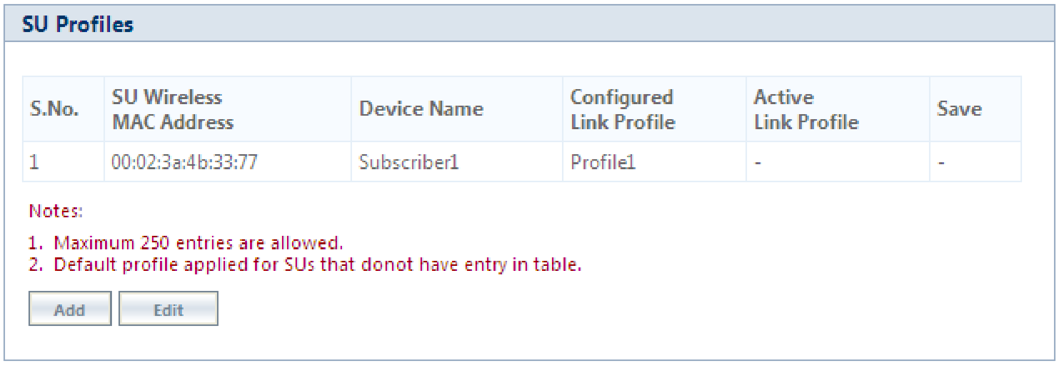
Figure 5-52 Add an SU Profile Entry

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

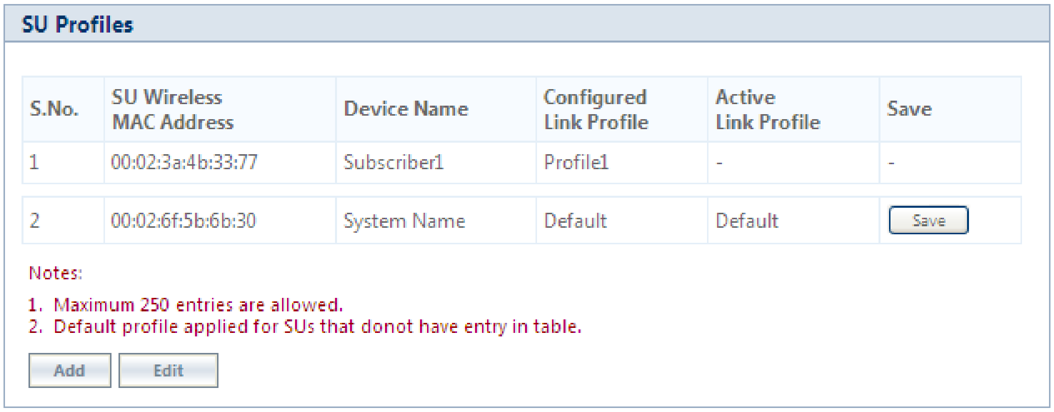
S.No.	SU Wireless MAC Address	Device Name	Configured Link Profile	Active Link Profile	Save
1	00:02:3a:4b:33:77	Subscriber1	Profile1	-	-

Notes:

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

Figure 5-53 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	Save

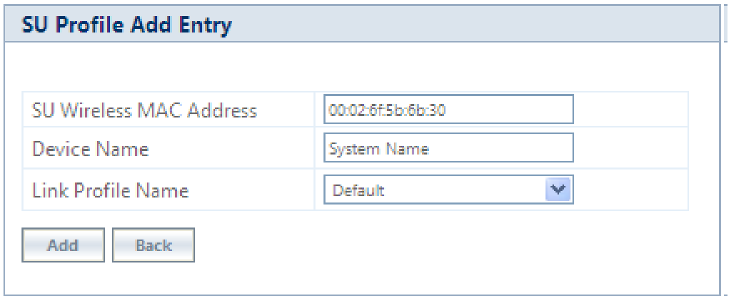
Notes:

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

Figure 5-54 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:

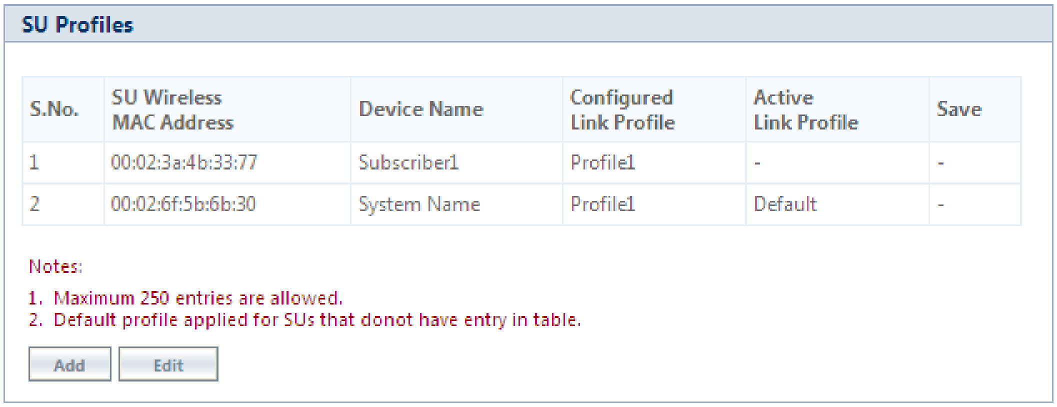


SU Profile Add Entry

SU Wireless MAC Address	00:02:6f:5b:6b:30
Device Name	System Name
Link Profile Name	Default

Figure 5-55 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

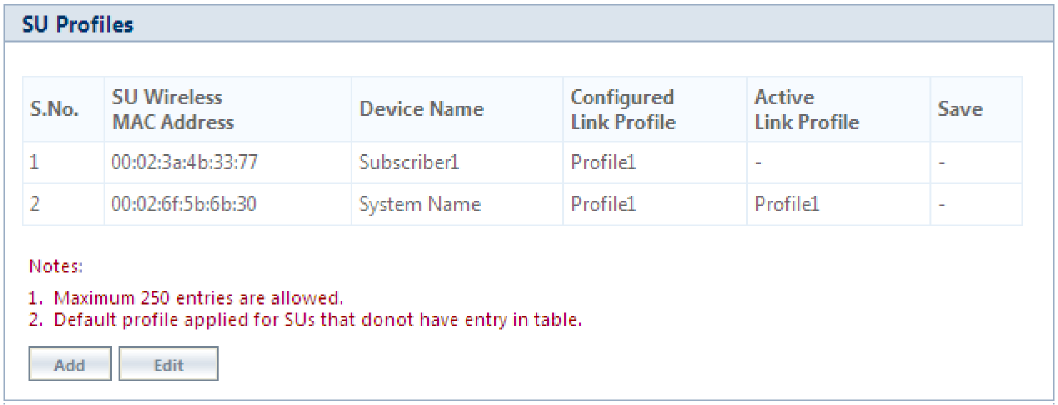
S.No.	SU Wireless MAC Address	Device Name	Configured Link Profile	Active Link Profile	Save
1	00:02:3a:4b:33:77	Subscriber1	Profile1	-	-
2	00:02:6f:5b:6b:30	System Name	Profile1	Default	-

Notes:

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

Figure 5-56 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:

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

Figure 5-57 Active SU Link Profile

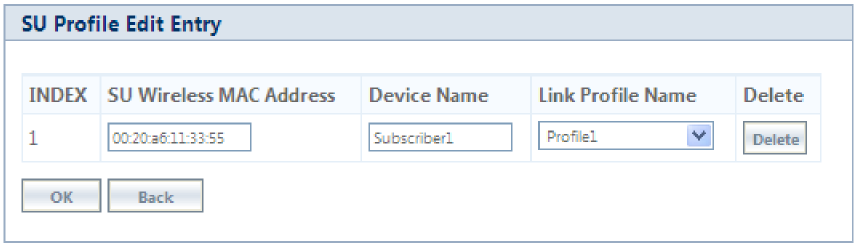
:

- *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.*

5.4.4.2 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

Figure 5-58 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.*

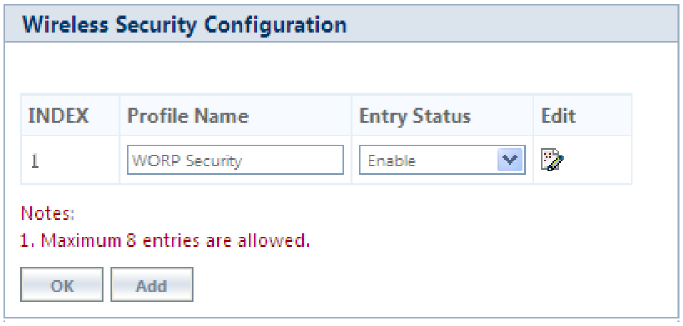
5.5 Security

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.

Figure 5-59 Wireless Security Configuration

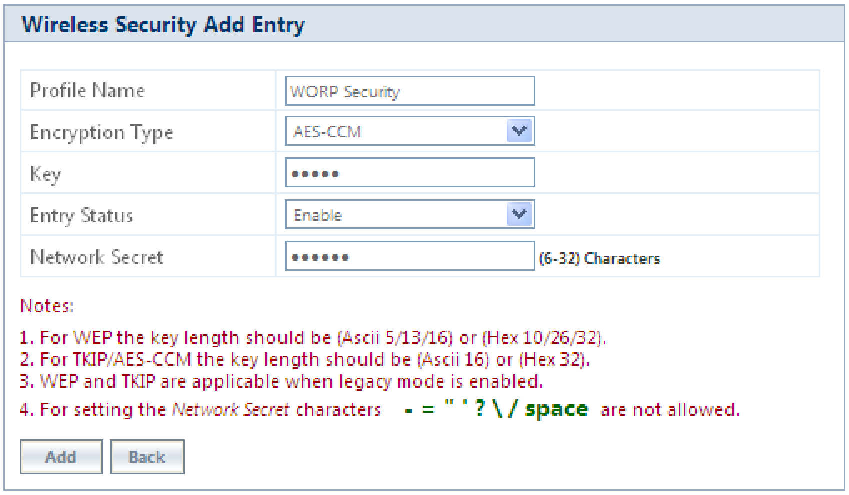
Given below is the table which explains Wireless Security parameters:

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.

Figure 5-60 Creating a New Security Profile

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

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Profile Name</td><td>A name to uniquely identify a security profile name.</td></tr>
<tr><td>Encryption Type</td><td>Select encryption type as either <b>None, WEP, TKIP</b> or <b>AES-CCM</b>.
1. <b>None</b> - If the encryption type is selected as None, then there exist no security to the data frames transmitted over the wireless medium.
2. <b>WEP (Wired Equivalent Privacy)</b> - Represents the <b>WEP</b> Encryption type, which uses RC4 stream cipher for confidentiality and CRC-32 for integrity. The supported key lengths for WEP are 5/13/16 ASCII characters or 10/26/32 Hexadecimal digits.
– <b>Key1 / Key 2 / Key 3 / key 4</b>: You can configure a maximum of four WEP keys. Enter 5/13/16 ASCII Characters or 10/26/32 Hexadecimal digits for WEP keys.
– <b>Transmit Key:</b> Select one out of the four keys described above as the default transmit key, which is used for encrypting and transmitting the data.
3. <b>TKIP</b> - Represents the <b>TKIP</b> Encryption type, which uses RC4 stream cipher for confidentiality. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism. It uses 128-bit keys for encryption. The key length for TKIP is 16 ASCII characters or 32 Hexadecimal digits.
– <b>Key1 / Key 2 / Key 3 / key 4</b>: You can configure a maximum of four TKIP keys. Enter 16 ASCII characters or 32 Hexadecimal digits.
– <b>Transmit Key:</b> Select one out of the four keys described above as the default transmit key, which is used for encrypting and transmitting the data.
4. <b>AES-CCM</b> - Represents CCM Protocol with AES Cipher restricted to 128 bits.
• <b>Key</b>: Enter 16 ASCII characters or 32 Hex Digits for AES-CCM encryption keys.</td></tr>
<tr><td>Entry status</td><td>Enables you to either <b>Enable</b> or <b>Disable</b> the security profile on the device. By default, it is enabled.</td></tr>
<tr><td>Network Secret</td><td>Enter the WORP 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.</td></tr>
<tr><td colspan="2">:
• <i>You can create a maximum of eight security profiles.</i>
• <i>A QuickBridge supports <b>AES-CCM</b> encryption type only.</i>
• <i>Special characters like - = \ " ' ? / space are not allowed while configuring the keys.</i>
• <i>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.</i>
• <i>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.</i>
• <i>WEP and TKIP Encryption types are supported only in legacy modes.</i>
• <i>The encryption mode should not be selected as AES-CCM while the device is interoperating with legacy Tsunami® MP.11 family devices.</i></td></tr>
</table>

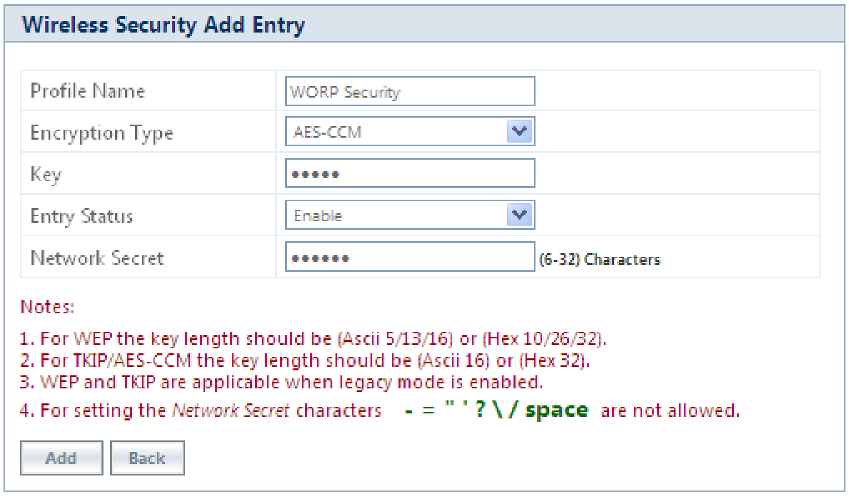
After configuring the required parameters, click **Add** and then **COMMIT**.

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	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.

Figure 5-61 Wireless Security Edit Row

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

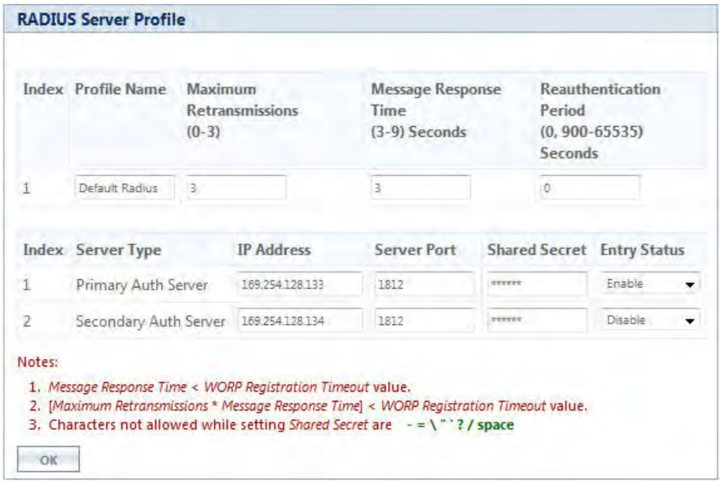
5.5.2 RADIUS

: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	Maximum Retransmissions (0-3)	Message Response Time (3-9) Seconds	Reauthentication Period (0, 900-65535) Seconds
1	Default Radius	3	3	0

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

Notes:

1. *Message Response Time* < *WORP Registration Timeout* value.
2. [*Maximum Retransmissions* * *Message Response Time*] < *WORP Registration Timeout* value.
3. Characters not allowed while setting *Shared Secret* are - = \ " ' ? / space

Figure 5-62 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: 1. Primary RADIUS Server 2. Secondary RADIUS Server The secondary RADIUS server serves as backup when the primary RADIUS server is down or not reachable.

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,

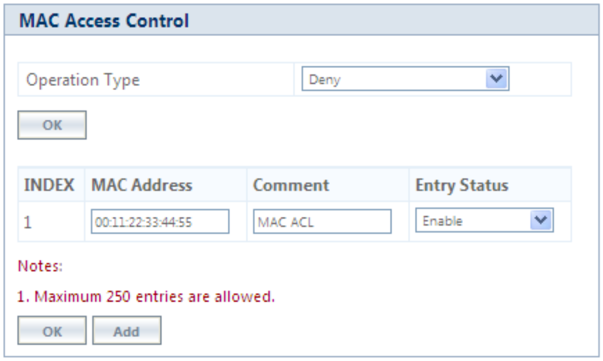
1. **Message Response Time** should always be less than **WORP Registration Timeout**.
2. If **Max Retransmissions** is configured as **Zero**, then retransmissions do not occur.
3. The value of **Max Retransmissions** multiplied by **Message Response Time** should be less than **WORP Registration Timeout**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

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

Notes:

1. Maximum 250 entries are allowed.

Figure 5-63 MAC Access Control Configuration

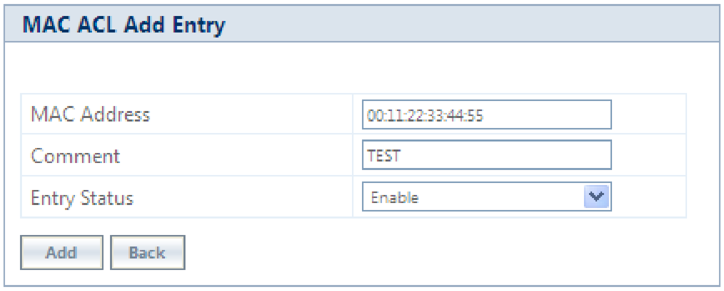
Select the Operation Type as either **Allow** or **Deny**.

- **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

Figure 5-64 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 = 0xffffffffffff, mask = 0xffffffffffff)
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=46(0x2E), ToS high=46(0x2E), 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
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

Committed Information Rate (CIR)	Scheduling Type	Traffic Priority	Absolute Priority
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 alloted (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:

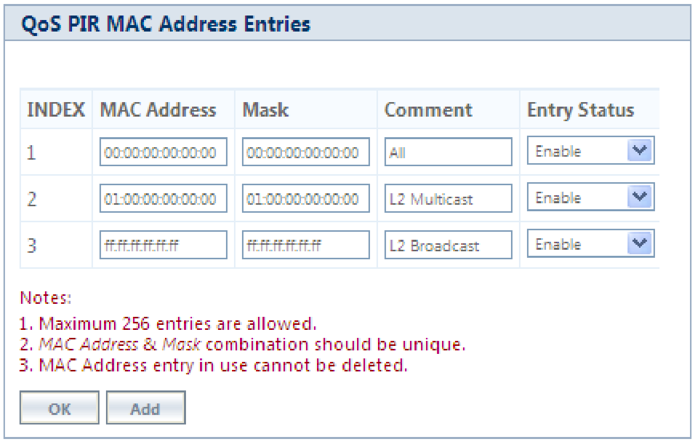
1. If new MAC Address, IP Address, and/or TCP/UDP Port are necessary, define the PIR MAC Address, IP Address and/or TCP/UDP Port Entries.

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
2	01:00:00:00:00:00	01:00:00:00:00:00	L2 Multicast	Enable
3	ff:ff:ff:ff:ff:ff	ff:ff:ff:ff:ff:ff	L2 Broadcast	Enable

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

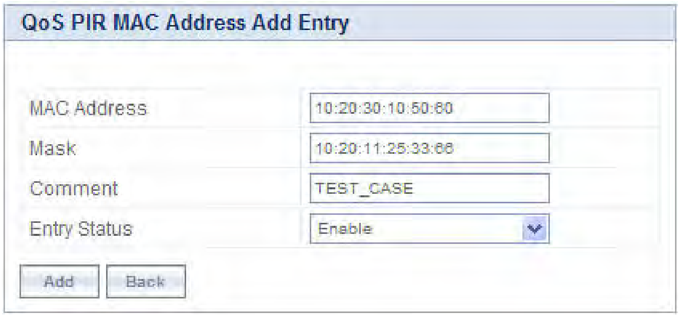
Figure 5-65 QoS PIR MAC Address Entries

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	10:20:30:10:50:60
Mask	10:20:11:25:33:66
Comment	TEST_CASE
Entry Status	Enable

Figure 5-66 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

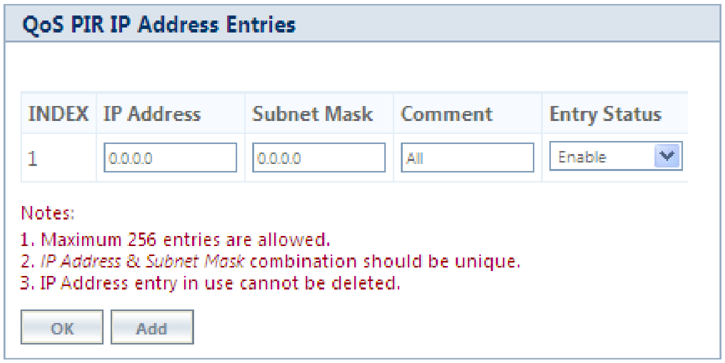
   MAC Mask: 01:00:00:00:00:00
5. **Creating Matching Profile for range of MAC Address (00:20:A6:00:00:01 to 00:20:A6:00:00:FF)**

   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

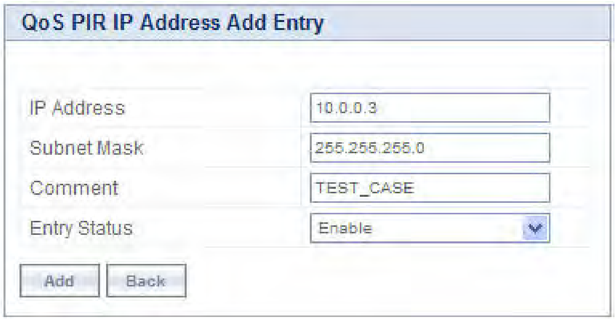
Notes:
1. Maximum 256 entries are allowed.
2. *IP Address* & *Subnet Mask* combination should be unique.
3. IP Address entry in use cannot be deleted.

Figure 5-67 QoS PIR IP Address Entries

To Add a New PIR IP Address Entry,

a. Navigate to **ADVANCED CONFIGURATION > QoS > PIR List > IP Address Entries**. The **QoS PIR IP Address Entries** screen appears

b. 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

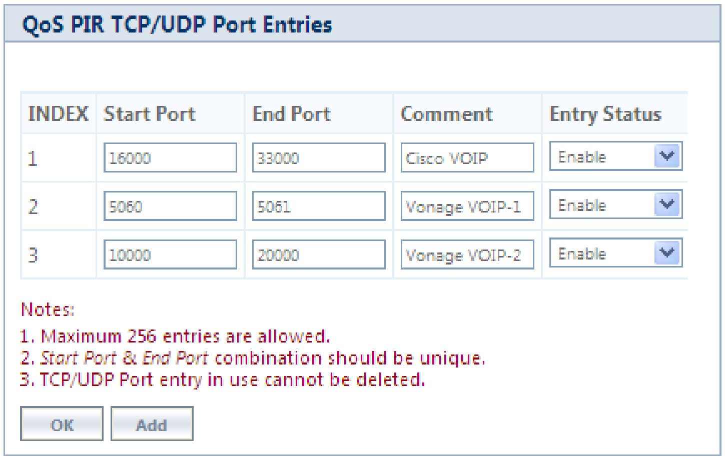
IP Address	10.0.0.3
Subnet Mask	255.255.255.0
Comment	TEST_CASE
Entry Status	Enable

Figure 5-68 QoS PIR IP Address Add Entry

c. 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

1. 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.
2. 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

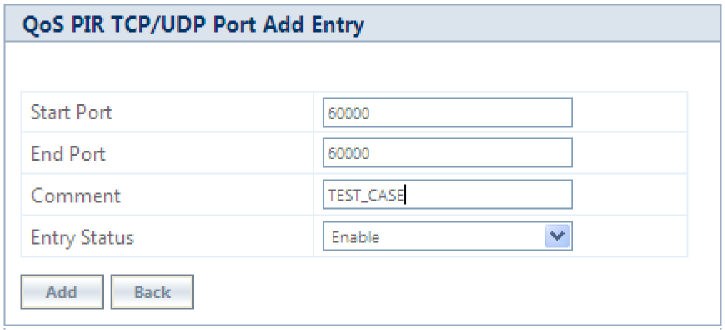
Notes:
1. Maximum 256 entries are allowed.
2. *Start Port* & *End Port* combination should be unique.
3. TCP/UDP Port entry in use cannot be deleted.

Figure 5-69 QoS PIR TCP/UDP Port Entries

To Add a New PIR TCP/UDP Port Entry,

a. Navigate to **ADVANCED CONFIGURATION > QoS > PIR List > TCP/UDP Port Entries**. The **QoS PIR TCP/UDP Port Entries** screen appears.

b. 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

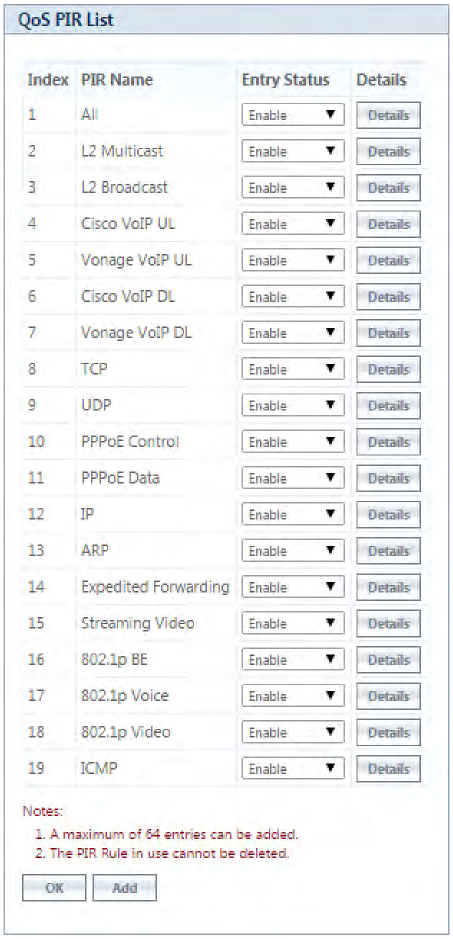
Start Port	60000
End Port	60000
Comment	TEST_CASE
Entry Status	Enable

Figure 5-70 QoS PIR TCP/UDP Port Add Entry

c. 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

1. 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.
2. Click **OK**.



QoS PIR List

Index	PIR Name	Entry Status	Details
1	All	Enable	Details
2	L2 Multicast	Enable	Details
3	L2 Broadcast	Enable	Details
4	Cisco VoIP UL	Enable	Details
5	Vonage VoIP UL	Enable	Details
6	Cisco VoIP DL	Enable	Details
7	Vonage VoIP DL	Enable	Details
8	TCP	Enable	Details
9	UDP	Enable	Details
10	PPPoE Control	Enable	Details
11	PPPoE Data	Enable	Details
12	IP	Enable	Details
13	ARP	Enable	Details
14	Expedited Forwarding	Enable	Details
15	Streaming Video	Enable	Details
16	802.1p BE	Enable	Details
17	802.1p Voice	Enable	Details
18	802.1p Video	Enable	Details
19	ICMP	Enable	Details

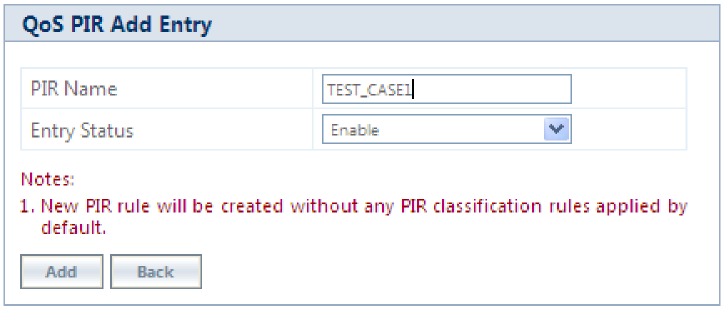
Notes:
1. A maximum of 64 entries can be added.
2. The PIR Rule in use cannot be deleted.

Figure 5-71 QoS PIR Entries

To Add a New PIR Rule,

a. Navigate to **ADVANCED CONFIGURATION > QoS > PIR List.** The **QoS PIR Entries** screen appears.

b. Click **Add** on the **QoS PIR Entries** screen to add a new entry. The following screen appears for configuring the New PIR Entry.



QoS PIR Add Entry

PIR Name	TEST_CASE1
Entry Status	Enable

Notes:

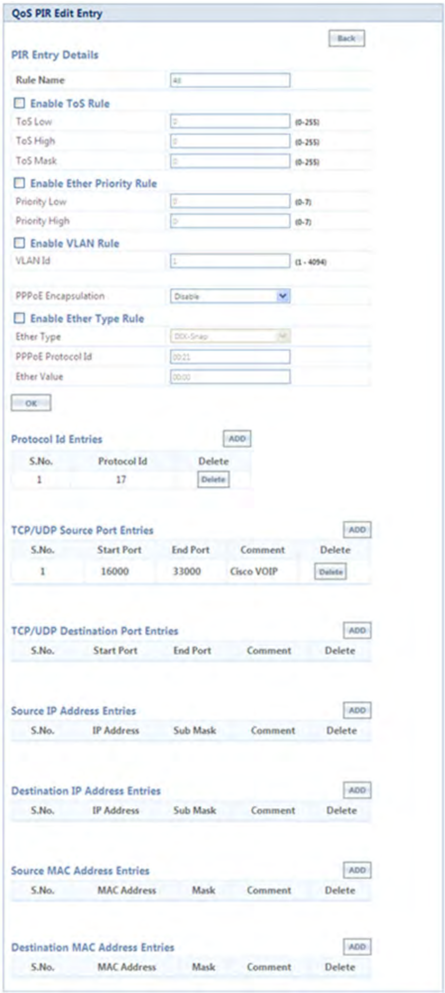
1. New PIR rule will be created without any PIR classification rules applied by default.

Figure 5-72 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	[illegible]	
□ Enable ToS Rule		
ToS Low	[illegible]	(0-255)
ToS High	[illegible]	(0-255)
ToS Mask	[illegible]	(0-255)
□ Enable Ether Priority Rule		
Priority Low	[illegible]	(0-7)
Priority High	[illegible]	(0-7)
□ Enable VLAN Rule		
VLAN Id	1	(1 - 4094)
PPPoE Encapsulation	Disable	
□ Enable Ether Type Rule		
Ether Type	DIX-Snap	
PPPoE Protocol Id	00:21	
Ether Value	00:00	

Protocol Id Entries

S.No.	Protocol Id	Delete
1	17	Delete

TCP/UDP Source Port Entries

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

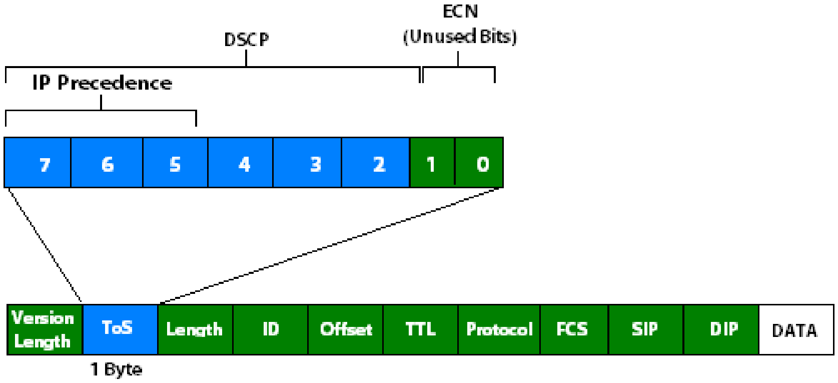
Source MAC Address Entries

S.No.	MAC Address	Mask	Comment	Delete

Destination MAC Address Entries

S.No.	MAC Address	Mask	Comment	Delete

Figure 5-73 QoS PIR Edit Entry

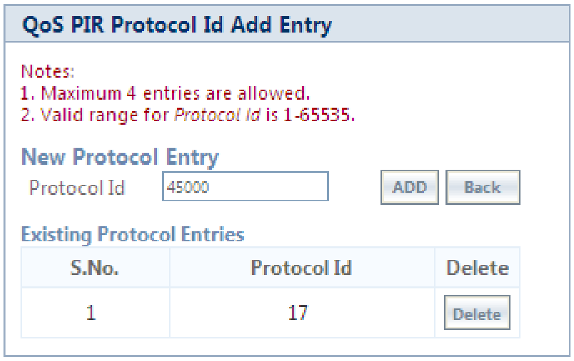
Parameter	Description
Rule Name	This parameter specifies the Name of the Packet Identification Rule (PIR) and can have a length of 1-32 characters.
ToS Rule	This parameter is used to enable or disable a TOS rule. When ToS rule is enabled, configure the values for the following to specify the ToS-related configuration: • ToS Low • ToS High • ToS Mask In ToS Configuration, enter the decimal value of entire ToS 1 byte in "ToS Low" and "ToS High" parameters of the PIR rule.  ECN (Unused Bits) DSCP IP Precedence 7 6 5 4 3 2 1 0 Version Length ToS Length ID Offset TTL Protocol FCS SIP DIP DATA 1 Byte **Figure 5-74 IP Header Format** 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) Consider the following while configuring PIR TOS parameters: 1. 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) **For Example:** To configure ToS Low and Tos High values, when the DSCP packet value is 10: - 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 **Configure:** - ToS Low = 40 - ToS High = 40 2. To prioritize the traffic based on range of DSCP value, configure "ToS low" and "ToS High" to a range. **For Example:** To configure ToS Low and ToS High values, when the DSCP packet is in range of 10 to 20, configure: - ToS Low = 40 (DSCP = 10 (Binary 001010) + ECN = 0 (Binary 00)) - ToS High = 80 (DSCP = 20 (Binary 010100) + ECN = 0 (Binary 00))

Parameter	Description
	3. To prioritize DSCP packets based on IP-Precedence/DSCP value/ToS value, configure "ToS Mask". a. **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). b. **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). c. **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	This parameters is used to enable or disable 802.1p priority rule. Enter the values for the following to specify 802.1p priority configuration: • Priority Low • Priority High
VLAN Rule	This parameters allows to enable or disable VLAN rule. Enter the VLAN ID when the VLAN rule is enabled.
PPPoE Encapsulation	This parameter is used to classify PPPoE traffic. • *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.* • *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".* • *Ether Value is not valid when PPPoE Encapsulation is enabled.*
Ether Type Rule	This parameters is used to enable or disable Ether Type rule. Enter the values for the following to specify the Ether Type rule related configuration: • Ether Type • PPPoE Protocol Id • Ether Value : • *PPPoE Protocol Id is not valid if PPPoE Encapsulation is disabled.* • *Ether Value is not valid if PPPoE Encapsulation is enabled.*

5.6.2.1.2 Adding Protocol ID

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

b. 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: 45000

Existing Protocol Entries

S.No.	Protocol Id	Delete
1	17	Delete

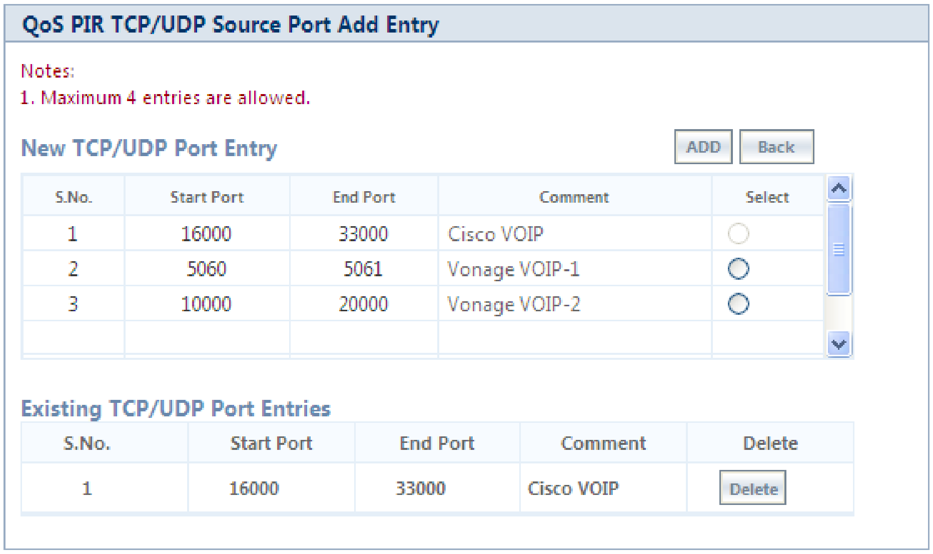
Figure 5-75 QoS PIR Protocol ID

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	○
2	5060	5061	Vonage VOIP-1	○
3	10000	20000	Vonage VOIP-2	○

Existing TCP/UDP Port Entries

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

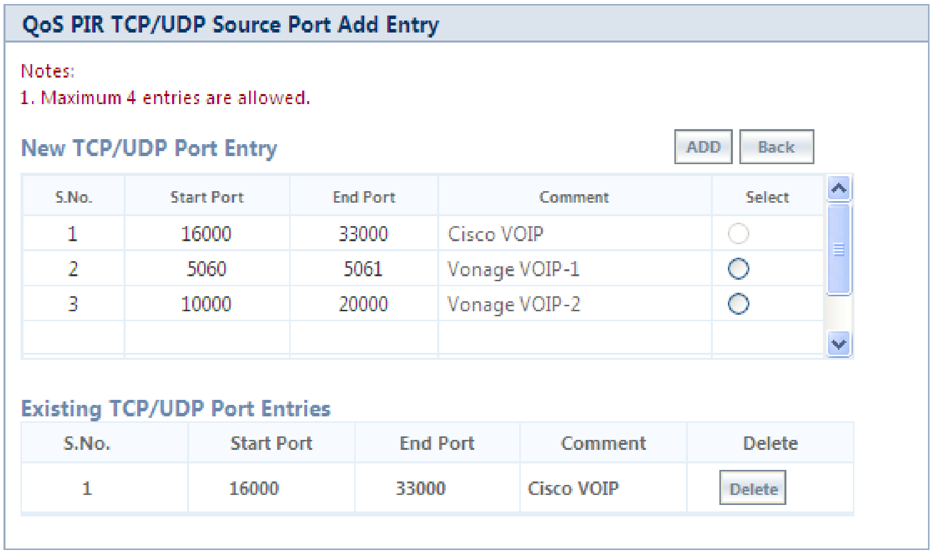
Figure 5-76 QoS PIR TCP/UDP Source Port Add Entry

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

S.No.	Start Port	End Port	Comment	Select
1	16000	33000	Cisco VOIP	○
2	5060	5061	Vonage VOIP-1	○
3	10000	20000	Vonage VOIP-2	○

Existing TCP/UDP Port Entries

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

Figure 5-77 QoS PIR TCP/UDP Destination Port Add Entry

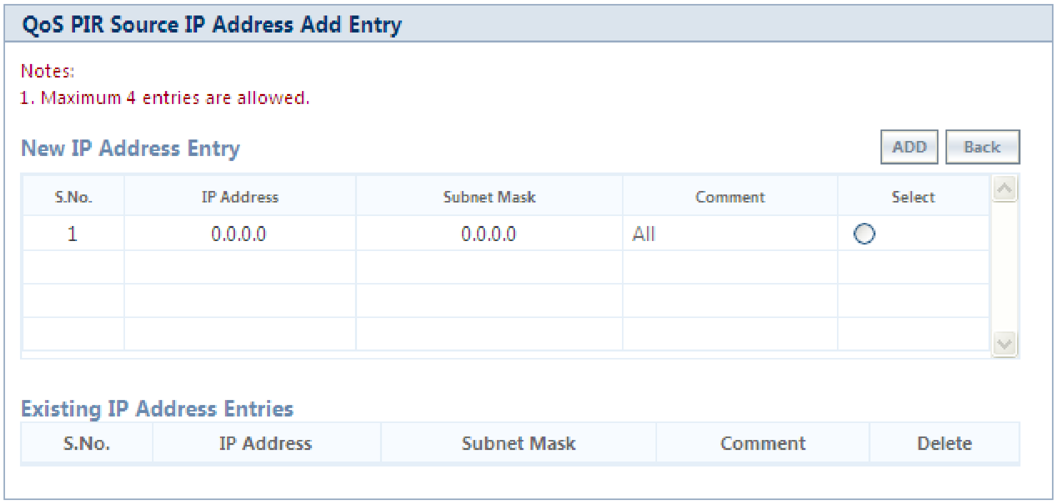
c. All the entries present in the PIR TCP/UDP Port Entries are displayed in the TCP/UDP Port Entry Table. Select the appropriate radio button and click **Add**. When an entry is added for a specific PIR, it gets displayed in the existing TCP/UDP Port Entries table. For deleting an entry, click **Delete**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

S.No.	IP Address	Subnet Mask	Comment	Select
1	0.0.0.0	0.0.0.0	All	○

Existing IP Address Entries

S.No.	IP Address	Subnet Mask	Comment	Delete

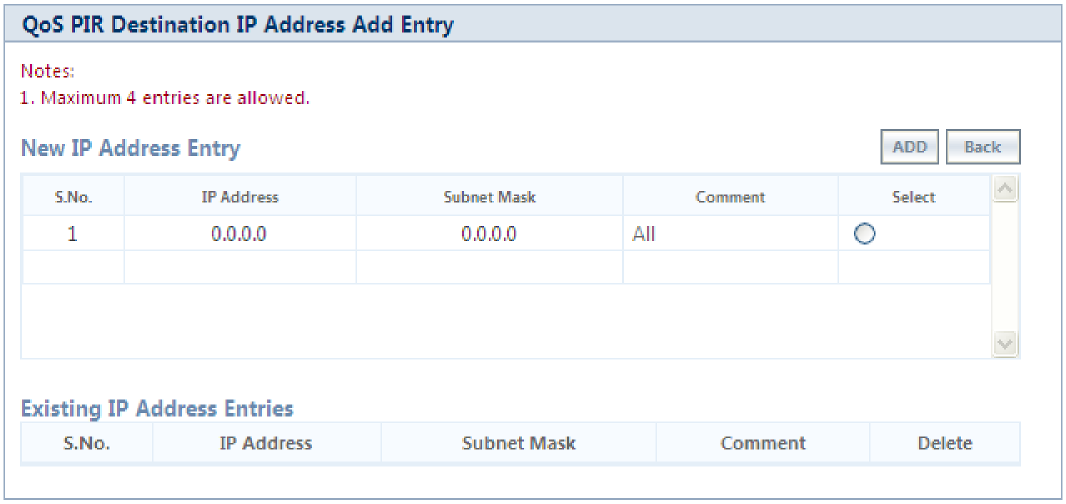
Figure 5-78 QoS PIR Source IP Address Add Entry

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

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

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



QoS PIR Destination IP Address Add Entry

Notes:
1. Maximum 4 entries are allowed.

New IP Address Entry

S.No.	IP Address	Subnet Mask	Comment	Select
1	0.0.0.0	0.0.0.0	All	○

Existing IP Address Entries

S.No.	IP Address	Subnet Mask	Comment	Delete

Figure 5-79 QoS PIR Destination IP Address Add Entry

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

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.

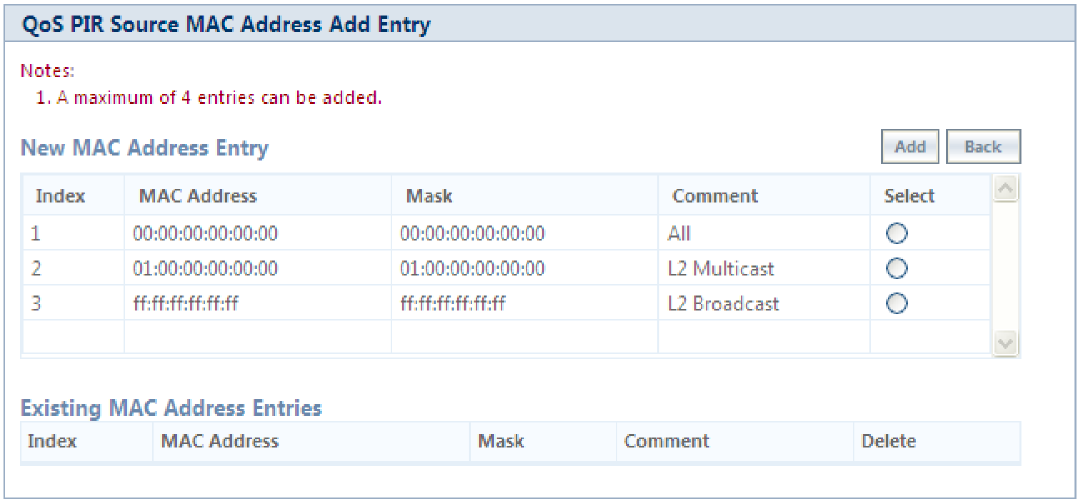
6. **Creating Matching Profile for range of Multicast IP Address (224.0.0.0 to 224.0.0.255)**

   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

Index	MAC Address	Mask	Comment	Select
1	00:00:00:00:00:00	00:00:00:00:00:00	All	○
2	01:00:00:00:00:00	01:00:00:00:00:00	L2 Multicast	○
3	ff:ff:ff:ff:ff:ff	ff:ff:ff:ff:ff:ff	L2 Broadcast	○

Existing MAC Address Entries

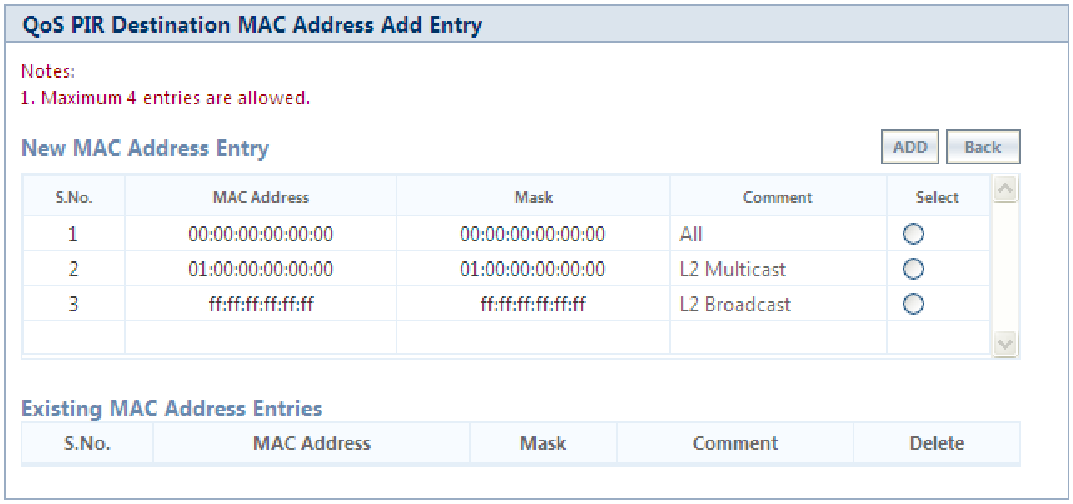
Index	MAC Address	Mask	Comment	Delete

Figure 5-80 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

S.No.	MAC Address	Mask	Comment	Select
1	00:00:00:00:00:00	00:00:00:00:00:00	All	○
2	01:00:00:00:00:00	01:00:00:00:00:00	L2 Multicast	○
3	ff:ff:ff:ff:ff:ff	ff:ff:ff:ff:ff:ff	L2 Broadcast	○

Existing MAC Address Entries

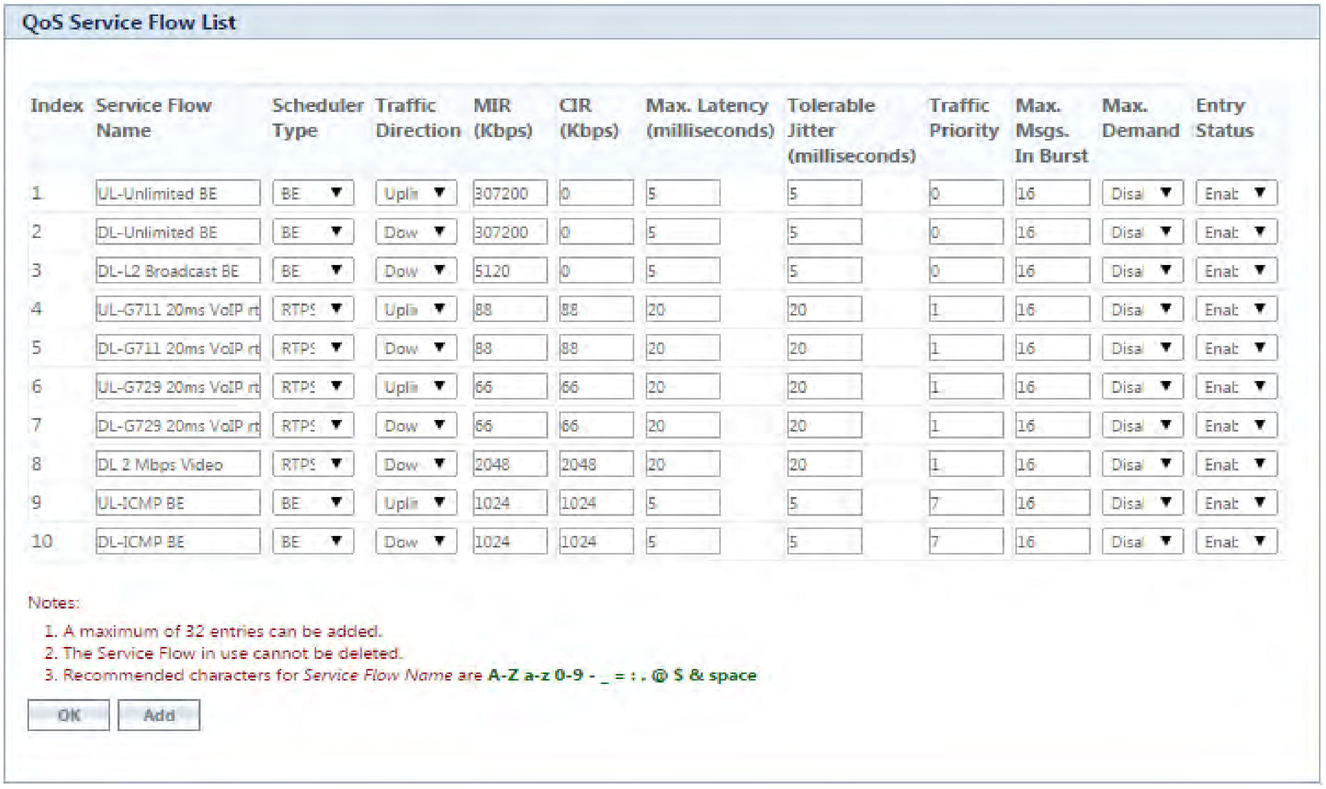
S.No.	MAC Address	Mask	Comment	Delete

Figure 5-81 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**. Ten 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

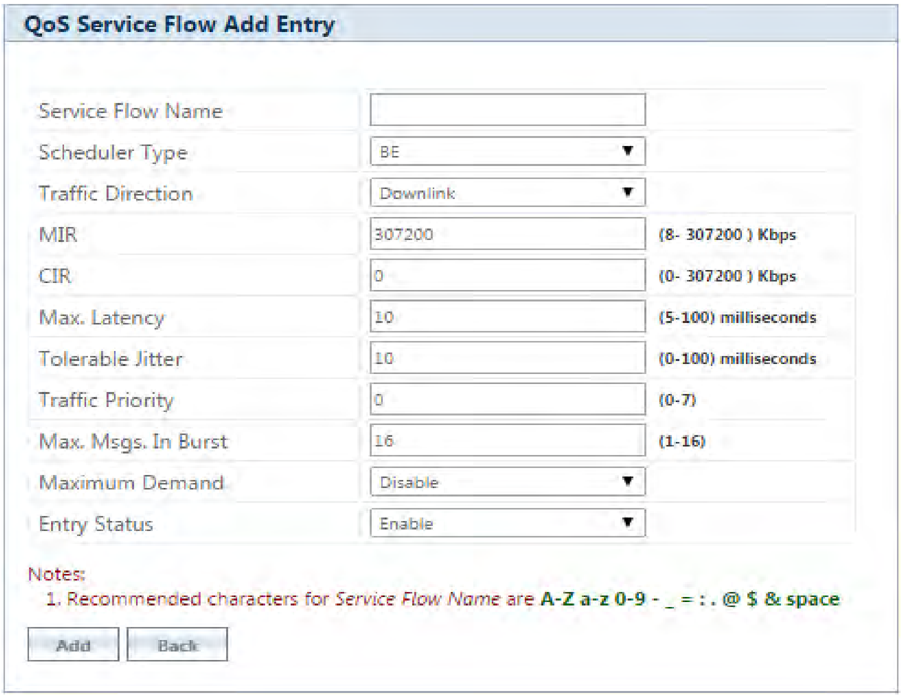
Index	Service Flow Name	Scheduler Type	Traffic Direction	MIR (Kbps)	CIR (Kbps)	Max. Latency (milliseconds)	Tolerable Jitter (milliseconds)	Traffic Priority	Max. Msgs. In Burst	Max. Demand	Entry Status
1	UL-Unlimited BE	BE ▼	Upli ▼	307200	0	5	5	0	16	Disa ▼	Enat ▼
2	DL-Unlimited BE	BE ▼	Dow ▼	307200	0	5	5	0	16	Disa ▼	Enat ▼
3	DL-L2 Broadcast BE	BE ▼	Dow ▼	5120	0	5	5	0	16	Disa ▼	Enat ▼
4	UL-G711 20ms VoIP rt	RTPS ▼	Upli ▼	88	88	20	20	1	16	Disa ▼	Enat ▼
5	DL-G711 20ms VoIP rt	RTPS ▼	Dow ▼	88	88	20	20	1	16	Disa ▼	Enat ▼
6	UL-G729 20ms VoIP rt	RTPS ▼	Upli ▼	66	66	20	20	1	16	Disa ▼	Enat ▼
7	DL-G729 20ms VoIP rt	RTPS ▼	Dow ▼	66	66	20	20	1	16	Disa ▼	Enat ▼
8	DL 2 Mbps Video	RTPS ▼	Dow ▼	2048	2048	20	20	1	16	Disa ▼	Enat ▼
9	UL-ICMP BE	BE ▼	Upli ▼	1024	1024	5	5	7	16	Disa ▼	Enat ▼
10	DL-ICMP BE	BE ▼	Dow ▼	1024	1024	5	5	7	16	Disa ▼	Enat ▼

Notes:

1. A maximum of 32 entries can be added.
2. The Service Flow in use cannot be deleted.
3. Recommended characters for *Service Flow Name* are **A-Z a-z 0-9 - _ = : . @ $ & space**

Figure 5-82 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		
Scheduler Type	BE ▼	
Traffic Direction	Downlink ▼	
MIR	307200	(8- 307200) Kbps
CIR	0	(0- 307200) Kbps
Max. Latency	10	(5-100) milliseconds
Tolerable Jitter	10	(0-100) milliseconds
Traffic Priority	0	(0-7)
Max. Msgs. In Burst	16	(1-16)
Maximum Demand	Disable ▼	
Entry Status	Enable ▼	

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

Figure 5-83 QoS Service Flow Add Entry

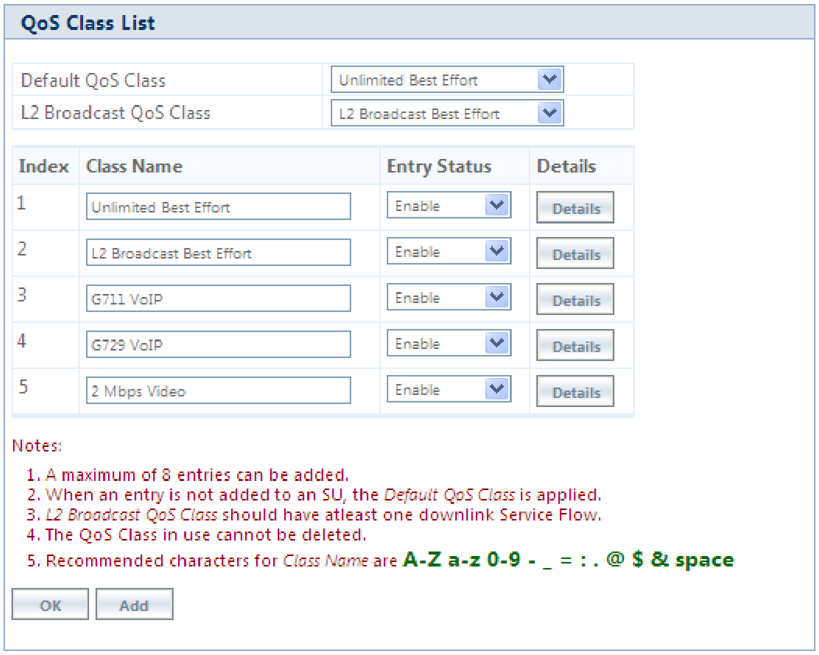
2. Specify details for the Service Flow Name, Scheduler Type, Traffic Direction, MIR, CIR, Max Latency, Tolerable Jitter, Traffic Priority, Max Messages in Burst and Entry Status.
3. Click **Add**.

Parameter	Description
Service Flow Name	Specifies the Name of the Service Flow. It can be of length 1-32 characters.
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.*
Maximum Demand	Enable- Specifies the demand(equal to Committed Information Rate CIR Mbps) is configured or set for a particular SFC, regardless of whether or not the demand exists. Disable- Specifies the demand is not configured for a particular SFC. *: Enabling the Maximum demand affects the latency & performance of the system.*
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	Unlimited Best Effort
L2 Broadcast QoS Class	L2 Broadcast Best Effort

Index	Class Name	Entry Status	Details
1	Unlimited Best Effort	Enable	Details
2	L2 Broadcast Best Effort	Enable	Details
3	G711 VoIP	Enable	Details
4	G729 VoIP	Enable	Details
5	2 Mbps Video	Enable	Details

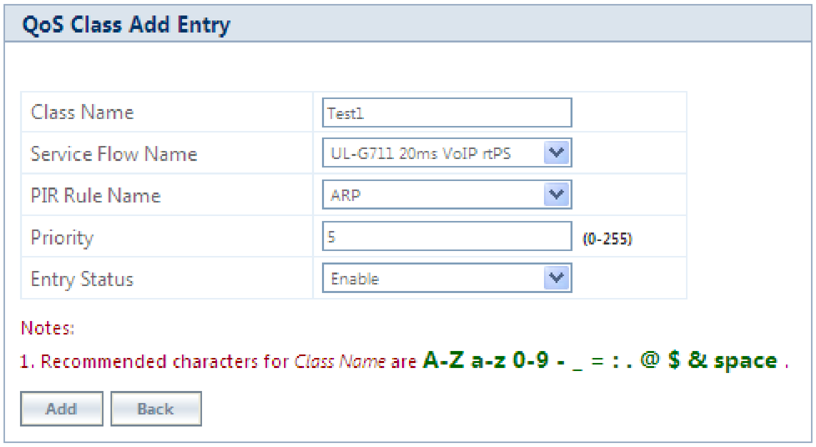
Notes:

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 5-84 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	Test1
Service Flow Name	UL-G711 20ms VoIP rtPS
PIR Rule Name	ARP
Priority	5 (0-255)
Entry Status	Enable

Notes:

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

Figure 5-85 QoS Class Add Entry

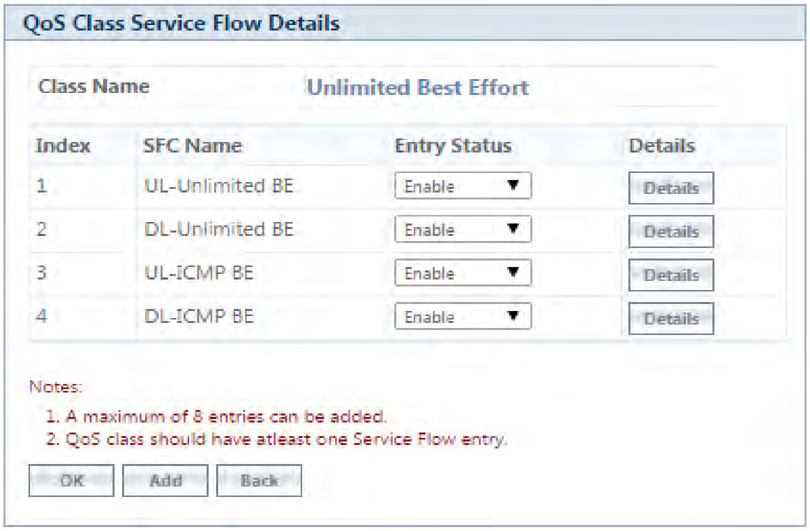
   b. Specify the QoS Class Name, Service Flow Name PIR Rule Name Priority and Entry Status and click **Add**.

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

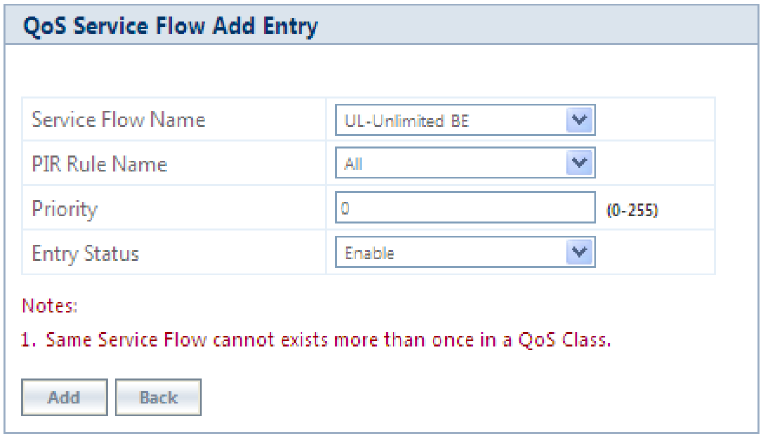
Index	SFC Name	Entry Status	Details
1	UL-Unlimited BE	Enable	Details
2	DL-Unlimited BE	Enable	Details
3	UL-ICMP BE	Enable	Details
4	DL-ICMP BE	Enable	Details

Notes:

1. A maximum of 8 entries can be added.
2. QoS class should have atleast one Service Flow entry.

Figure 5-86 QoS Class Service Flow Details

3. 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
PIR Rule Name	All
Priority	0 (0-255)
Entry Status	Enable

Notes:

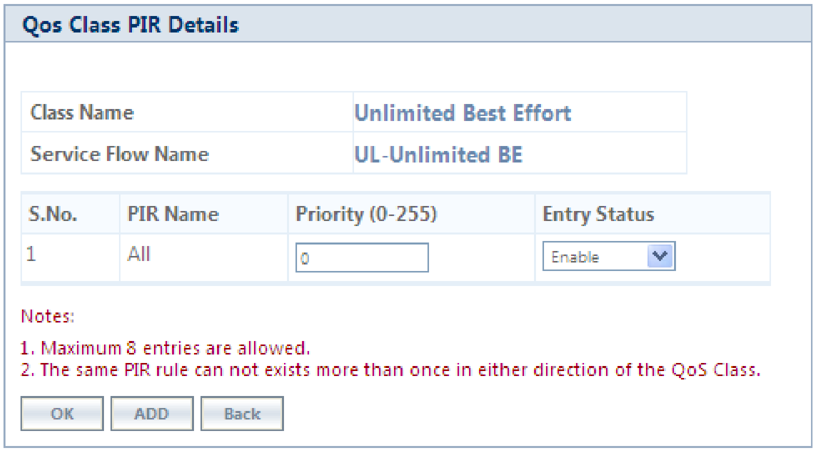
1. Same Service Flow cannot exists more than once in a QoS Class.

Figure 5-87 QoS Class Service Flow Add Entry

4. 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

1. 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.
2. Click **OK**.


Qos Class PIR Details

Class Name	Unlimited Best Effort
Service Flow Name	UL-Unlimited BE

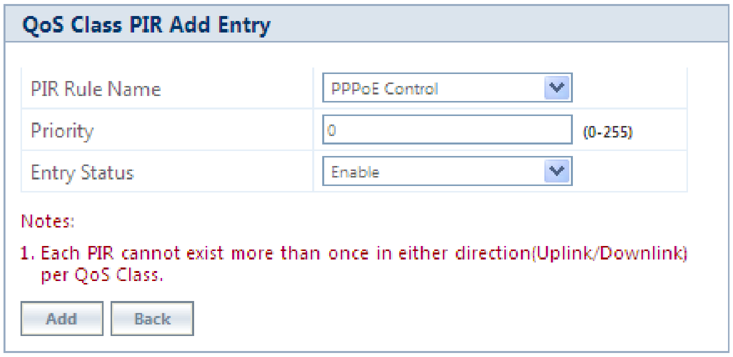
S.No.	PIR Name	Priority (0-255)	Entry Status
1	All	0	Enable

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.

Figure 5-88 QoS Class PIR Details

3. 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.

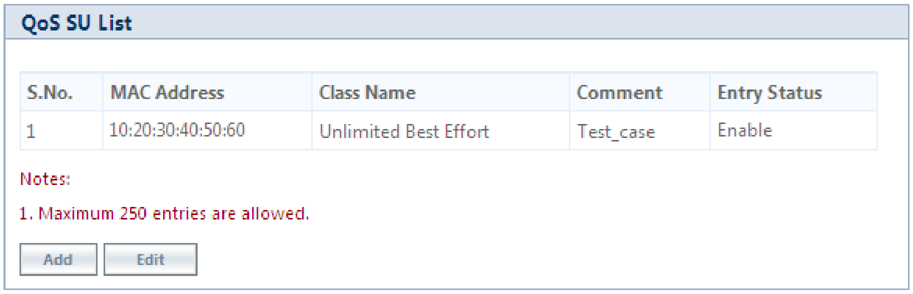
Figure 5-89 QoS Class PIR Add Entry

4. 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

1. 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:

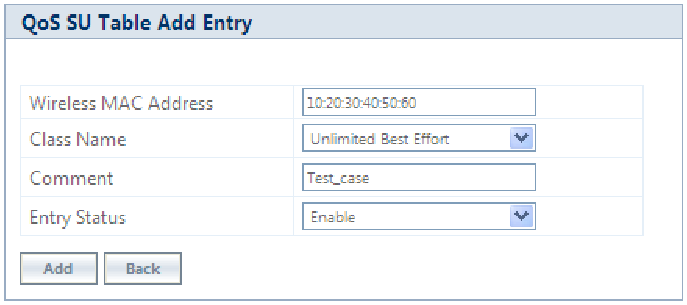
1. Maximum 250 entries are allowed.

Figure 5-90 QoS SU or End Point B List

2. 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

1. Navigate to **ADVANCED CONFIGURATION > QoS > SU or End Point B List**. The **QoS SU or End Point B Entries** screen appears.
2. 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	10:20:30:40:50:60
Class Name	Unlimited Best Effort
Comment	Test_case
Entry Status	Enable

Figure 5-91 QoS SU or End Point B Table Add Entry

3. 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 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
   f. Return to the Class List and add the UL-Management Service Flow in this class.
   g. 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

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.

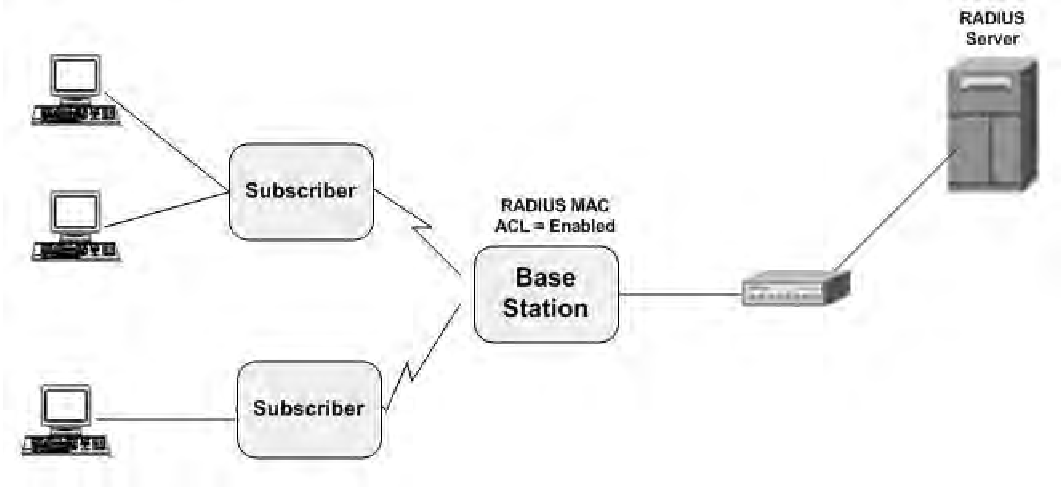


Figure 5-92 RADIUS Based QoS Configuration

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:

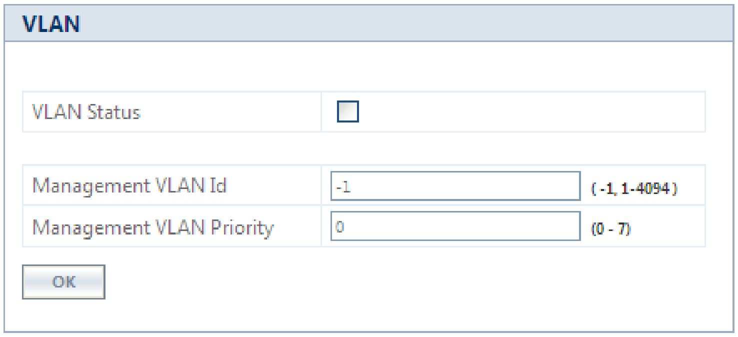
- Define groups
- Limits the broadcast and multicast traffic to a specific VLAN group
  – Improve network performance and reduce latency
- Increase security
  – Secure network restricts members to resources on their own VLAN

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

5.8.1 System-Level VLAN Configuration

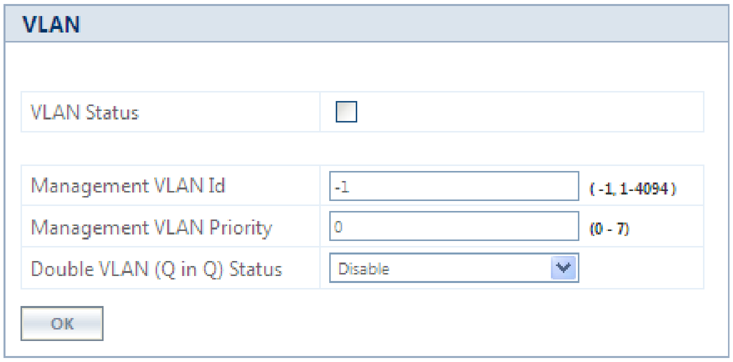
To configure system-level VLAN parameters, navigate to **ADVANCED CONFIGURATION > VLAN**. The **VLAN** configuration screen appears.



VLAN

VLAN Status	☐	
Management VLAN Id	-1	(-1, 1-4094)
Management VLAN Priority	0	(0 - 7)

Figure 5-93 System-Level VLAN Configuration (BSU)



VLAN

VLAN Status	☐	
Management VLAN Id	-1	(-1, 1-4094)
Management VLAN Priority	0	(0 - 7)
Double VLAN (Q in Q) Status	Disable	

Figure 5-94 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. The user can configure Service VLAN TPID as either 0x8100, 0x9100, or 0x88a8. By default the Service VLAN TPID is set to 0x8100.
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

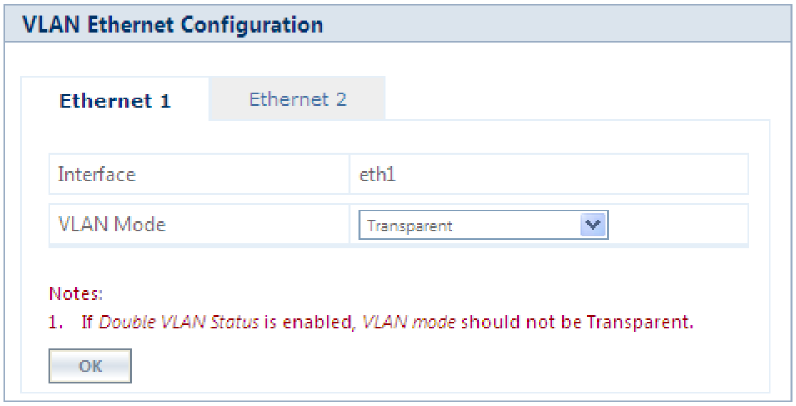
You can configure VLAN on the Ethernet interface(s) by using any one of the following VLAN Modes:

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:



VLAN Ethernet Configuration

Interface	eth1
VLAN Mode	Transparent

Notes:

1. If *Double VLAN Status* is enabled, *VLAN mode* should not be Transparent.

Figure 5-95 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**.

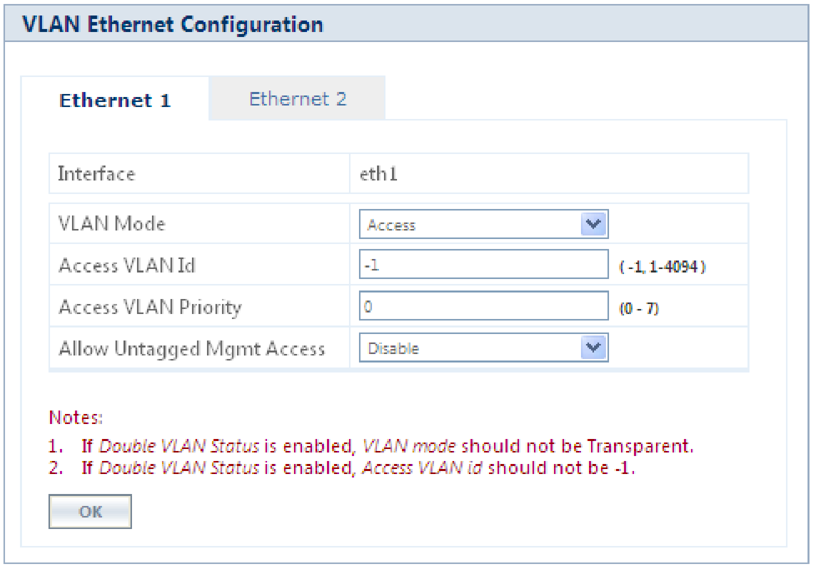
: *Wireless Interface of the device will always be in transparent mode. There is no support provided to edit the VLAN parameters of the wireless interface.*

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:



VLAN Ethernet Configuration

Interface	eth1	
VLAN Mode	Access	
Access VLAN Id	-1	(-1, 1-4094)
Access VLAN Priority	0	(0 - 7)
Allow Untagged Mgmt Access	Disable	

Notes:

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

Figure 5-96 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.*
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.

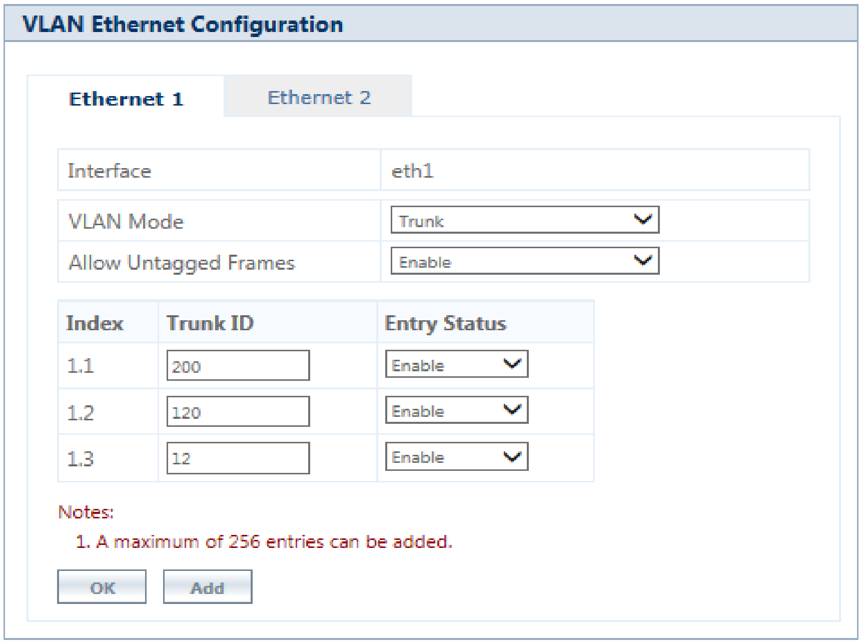
If the device receives untagged frames and the **Allow Untagged Frames** functionality is disabled, then the untagged packets are dropped.

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

Interface	eth1
VLAN Mode	Trunk
Allow Untagged Frames	Enable

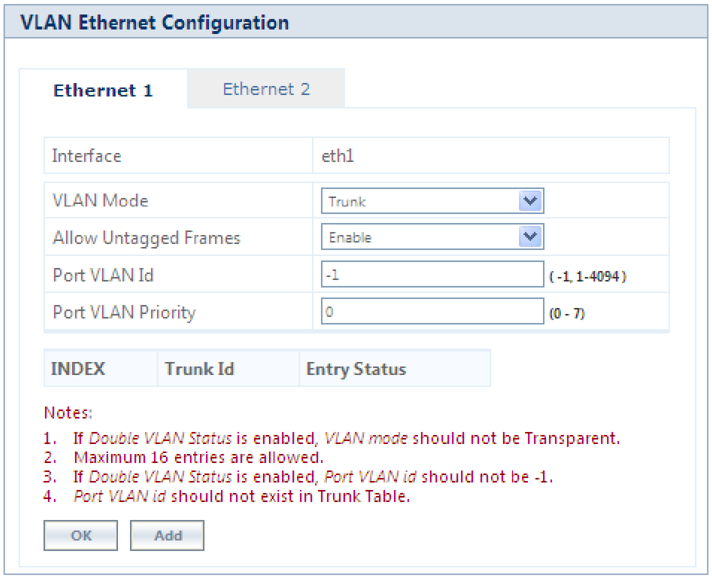
Index	Trunk ID	Entry Status
1.1	200	Enable
1.2	120	Enable
1.3	12	Enable

Notes:

1. A maximum of 256 entries can be added.

Figure 5-97 Trunk Mode (BSU)

: Ensure to configure an entry in Ethernet Trunk table, with a Trunk ID identical to Roaming VLAN ID.



VLAN Ethernet Configuration

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 *Double VLAN Status* is enabled, *VLAN mode* should not be Transparent.
2. Maximum 16 entries are allowed.
3. If *Double VLAN Status* is enabled, *Port VLAN id* should not be -1.
4. *Port VLAN id* should not exist in Trunk Table.

Figure 5-98 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:

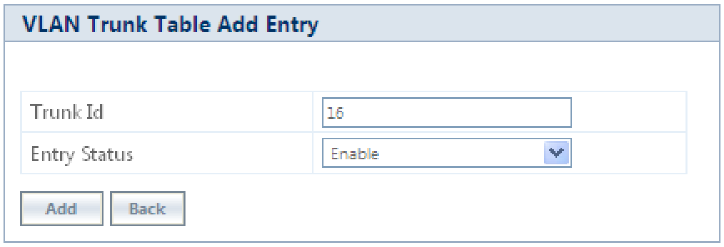
Parameter	Description
Interface	Displays the name of the Ethernet interface.
VLAN Mode	Select the **VLAN Mode** as **Trunk**.
Allow Untagged Frames	Select **Enable** or **Disable**. By default, it is disabled. • **Disable**: If this option is selected, the Ethernet interface forwards only tagged frames whose VLAN Id matches with a VLAN ID present in trunk table. • **Enable**: – 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**.
Port VLAN ID	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. 📝: • *Applicable only on an SU, End Point A and End Point B.* • *When Double VLAN is enabled on the device, the Port VLAN ID should not be set to -1.* • *The configured Port VLAN Id should not exist in the Trunk table.*
Port 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 Port VLAN priority, enter a value ranging from 0 to 7. 📝*: Applicable only to SU and End Point devices.*

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.



VLAN Trunk Table Add Entry

Trunk Id	16
Entry Status	Enable

Figure 5-99 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.

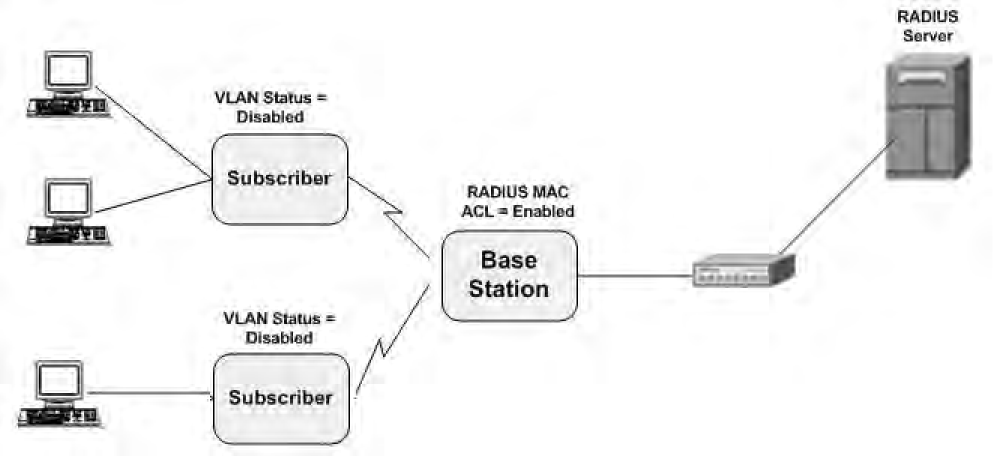


Figure 5-100 RADIUS Based VLAN Configuration

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

Name of the attribute	Vendor Assigned Attribute Number	Attribute Format	Attribute Value
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
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.11devices)	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.*

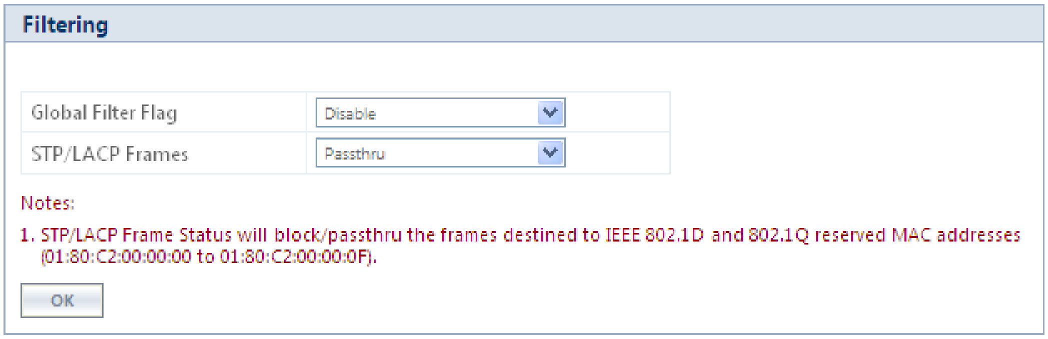
5.10 Filtering (Bridge Only)

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
- WORP 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.



Filtering

Global Filter Flag	Disable
STP/LACP Frames	Passthru

Notes:

1. STP/LACP Frame Status will block/passthru the frames destined to IEEE 802.1D and 802.1Q reserved MAC addresses (01:80:C2:00:00:00 to 01:80:C2:00:00:0F).

Figure 5-101 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.

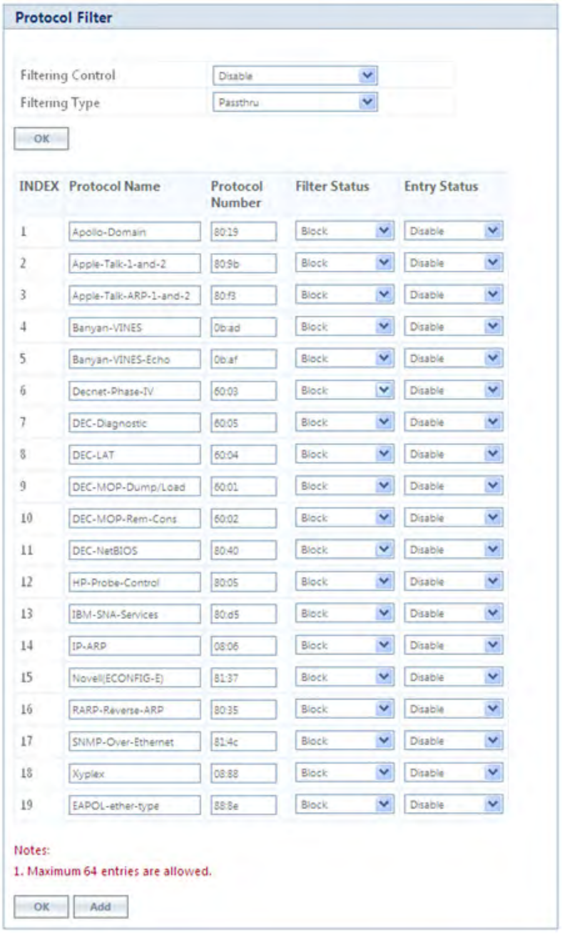
Parameter	Description
STP/LACP Frames	This parameter allows you to either **Block** or **Passthru** STP/LACP frames on the network. • **Passthru**: By allowing the STP/LACP frames, any loops that occurs within a network can be avoided. If configured to Passthru, the STP/LACP frames in the system are bridged. • **Block**: When blocked, the STP/LACP frames encountered on a network are terminated at bridge. By default, STP/LACP frames are allowed on the network. *: 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).*

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: Disable

Filtering Type: Passthru

INDEX	Protocol Name	Protocol Number	Filter Status	Entry Status
1	Apollo-Domain	80:19	Block	Disable
2	Apple-Talk-1-and-2	80:9b	Block	Disable
3	Apple-Talk-ARP-1-and-2	80:f3	Block	Disable
4	Banyan-VINES	0b:ad	Block	Disable
5	Banyan-VINES-Echo	0b:af	Block	Disable
6	Decnet-Phase-IV	60:03	Block	Disable
7	DEC-Diagnostic	60:05	Block	Disable
8	DEC-LAT	60:04	Block	Disable
9	DEC-MOP-Dump/Load	60:01	Block	Disable
10	DEC-MOP-Rem-Cons	60:02	Block	Disable
11	DEC-NetBIOS	80:40	Block	Disable
12	HP-Probe-Control	80:05	Block	Disable
13	IBM-SNA-Services	80:d5	Block	Disable
14	IP-ARP	08:06	Block	Disable
15	Novell(ECONFIG-E)	81:37	Block	Disable
16	RARP-Reverse-ARP	80:35	Block	Disable
17	SNMP-Over-Ethernet	81:4c	Block	Disable
18	Xyplex	08:88	Block	Disable
19	EAPOL-ether-type	88:8e	Block	Disable

Notes:
1. Maximum 64 entries are allowed.

Figure 5-102 Protocol Filter

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

Parameter	Description
Filtering Control	This parameter is used to apply filters on the device’s interface. The filtering can be applied on any of the following interfaces: • **Ethernet**: Packets are examined at the Ethernet interface. • **Wireless**: Packets are examined at the Wireless interface. • **All Interfaces**: Packets are examined at both Ethernet and Wireless interface. By default, the Filtering Control is set to **Disable**, meaning which Protocol Filters are disabled on all the interfaces. : *In addition to enabling **Filtering Control**, the **Global Filter Flag** should also be enabled to apply filters.*
Filtering Type	This parameter specifies the action to be performed on the data packets whose protocol type is not defined in the protocol filter table (this table contains a list of default protocols supported by the device and the protocols defined by the user), or whose Entry Status is in Disable state. The available filtering types are: • **Block**: The protocols with entry status Disable or the protocols which do not exist in the protocol filtering table are blocked. • **Passthru**: The protocols with entry status Disable or the protocols which do not exist in the protocol filtering table are allowed through the configured interface.

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

5.10.1.1 Protocol Filter Table

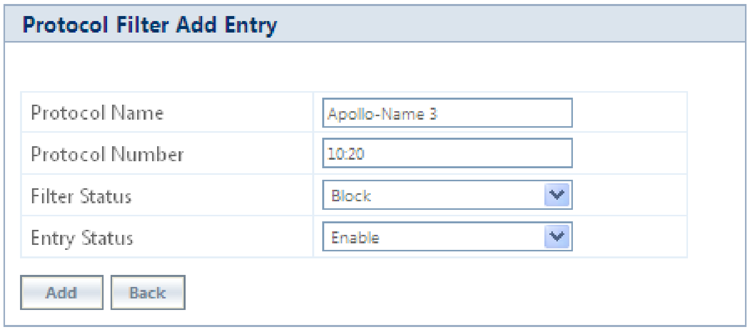
The Protocol Filter table displays a list of default protocols supported by the device and the protocols created by the user. By default, the system generates 19 protocols entries. Each of the Protocol contains the following information:

Parameter	Description
Protocol Name	Represents the Protocol name. The system throws an error when you try to edit the name of a default protocol.
Protocol Number	Represents the Protocol number. The value is of 4 digit hexadecimal format. The system throws an error when you try to edit the Protocol number of a default protocol.
Filter Status	The supported filter status are, • **Passthru**: When the filter status is set to **Passthru** and entry status is **Enable**, all packets whose protocol matches with the given protocol number are forwarded on the configured interface. • **Block**: When the filter status is set to **Block** and entry status is Enable, all packets whose protocol matches with the given protocol number are dropped on the configured interface. By default, the status is set to Block.
Entry Status	Set the entry status as either Enable, Disable or Delete. • **Enable**: Enables filter status on a protocol. • **Disable**: Disables filter status on a protocol. • **Delete**: Deletes a protocol entry from the Protocol Filter Table.

: System-defined default protocols cannot be deleted.

5.10.1.2 Add User-defined Protocols to the Filter Table

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



Protocol Filter Add Entry

Protocol Name	Apollo-Name 3
Protocol Number	10:20
Filter Status	Block
Entry Status	Enable

Figure 5-103 Add User-defined Protocols

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

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

5.10.2 Static MAC Address Filter

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

Each MAC Address or Mask is comprised of 12 hexadecimal digits (0-9, A-F) that correspond to a 48-bit identifier. (Each hexadecimal digit represents 4 bits (0 or 1)).

Taken together, a MAC Address/Mask pair specifies an address or a range of MAC addresses that the device will look for when examining packets. The device uses Boolean logic to perform an “AND” operation between the MAC Address and the Mask at the bit level. A Mask of 00:00:00:00:00:00 corresponds to all MAC addresses, and a Mask of FF:FF:FF:FF:FF:FF applies only to the specified MAC Address.

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

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

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

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

Static MAC Filter Examples

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

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

5.10.2.0.1 Prevent two specific PCs from communicating

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

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

Result: Traffic between the wired PC and wireless PC1 is blocked. wireless PC2 and PC3 can still communicate with the wired PC.

5.10.2.0.2 Prevent multiple Wireless PCs from communicating with a single wired PC

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

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

Result: When a logical “AND” is performed on the Wireless MAC Address and Wireless Mask, the result corresponds to any MAC address beginning with the 00:20:2D prefix. Since wireless PC1 and wireless PC2 share the same prefix (00:02:2D), traffic between the wired Server and wireless PC1 and PC2 is blocked. Wireless PC3 can still communicate with the wired PC since it has a different prefix (00:20:A6).

5.10.2.0.3 Prevent all wireless PCs from communicating with a single wired PC

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

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

Result: The device blocks all traffic between the wired PC and all wireless PCs.

5.10.2.0.4 Prevent a wireless PC from communicating with the wired network

Configure the following settings to prevent wireless PC3 from communicating with any device on the Ethernet:

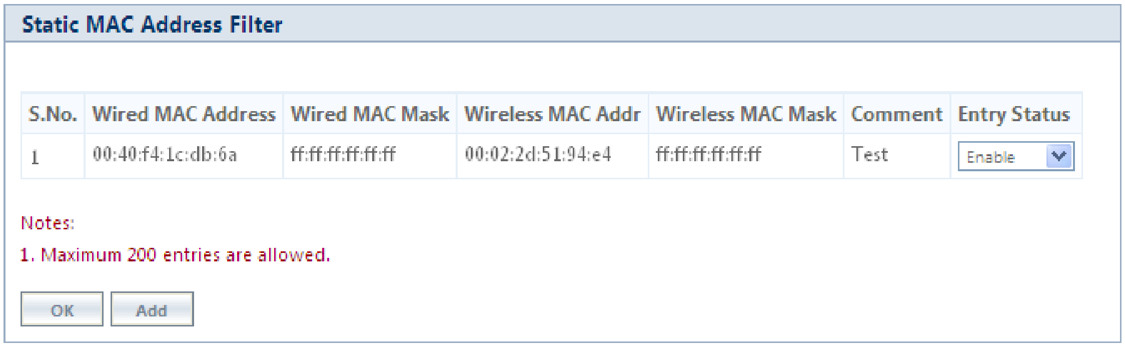
- **Wired MAC Address:** 00:00:00:00:00:00
- **Wired Mask:** 00:00:00:00:00:00

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

Result: The device blocks all traffic between wireless PC3 and the Ethernet network.

5.10.2.1 Static MAC Address Filter Configuration

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



Static MAC Address Filter

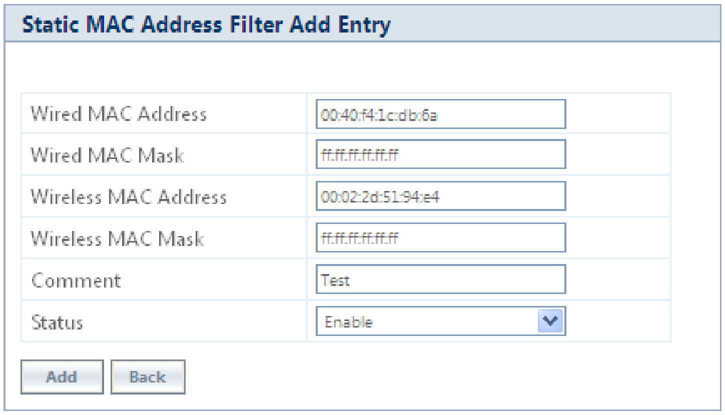
S.No.	Wired MAC Address	Wired MAC Mask	Wireless MAC Addr	Wireless MAC Mask	Comment	Entry Status
1	00:40:f4:1c:db:6a	ff:ff:ff:ff:ff:ff	00:02:2d:51:94:e4	ff:ff:ff:ff:ff:ff	Test	Enable

Notes:

1. Maximum 200 entries are allowed.

Figure 5-104 Static MAC Address Filter

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



Static MAC Address Filter Add Entry

Wired MAC Address	00:40:f4:1c:db:6a
Wired MAC Mask	ff:ff:ff:ff:ff:ff
Wireless MAC Address	00:02:2d:51:94:e4
Wireless MAC Mask	ff:ff:ff:ff:ff:ff
Comment	Test
Status	Enable

Figure 5-105 Static MAC Address Filter Add Entry

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

Parameter	Description
Wired MAC Address	Specifies the MAC address of the device on the wired network that is restricted from communicating with a device on the wireless network.
Wired MAC Mask	Specifies the range of MAC address to which this filter is to be applied.
Wireless MAC address	Specifies the MAC address of the device on the wireless network that is restricted from communicating with a device on the wired network.
Wireless MAC Mask	Specifies the range of MAC address to which this filter is to be applied.

Parameter	Description
Comment	Specifies the comment associated with **Static MAC Filter** table entry.
Status	Specifies the status of the newly created filter.

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

:

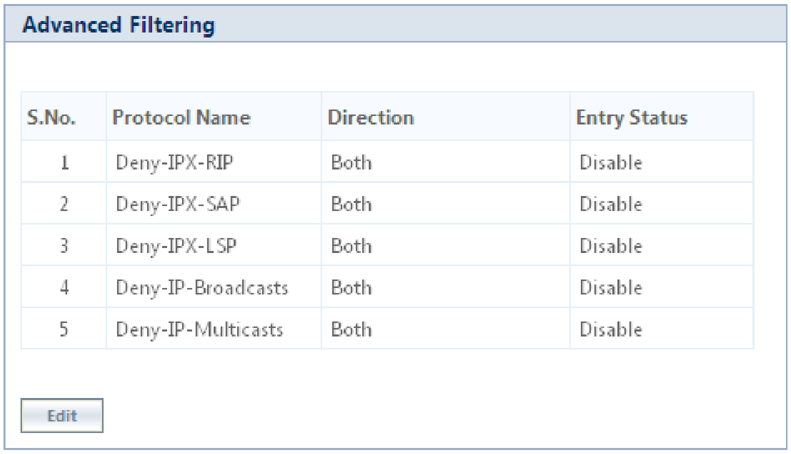
- *You can configure a maximum of 200 MAC address filters.*
- *The Wired MAC address and the Wireless MAC address should be a unicast MAC address.*
- *The MAC Address or Mask includes 12 hexadecimal digits (each hexadecimal equals to 4 bits containing 0 or 1) which is equivalent to 48 bit identifier.*

5.10.3 Advanced Filtering

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

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

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



Advanced Filtering

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

Figure 5-106 Advanced Filtering

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

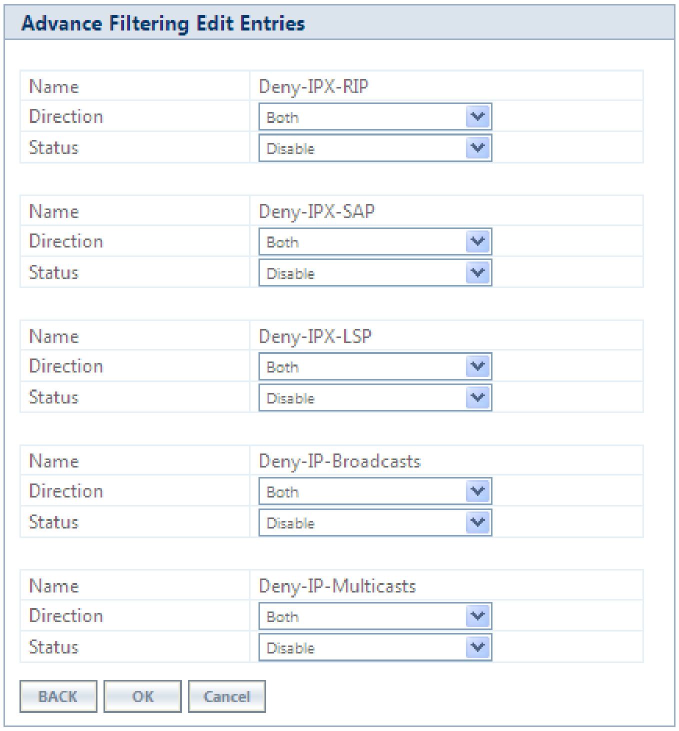
Parameter	Description
Protocol Name	Represents the protocol name. By default, Advanced Filtering is supported on the following 5 default protocols: • Deny IPX RIP • Deny IPX SAP • Deny IPX LSP • Deny IP Broadcasts • Deny IP Multicasts
Direction	Represents the direction of an IP Protocol traffic that needs to be filtered. The directions that can be filtered are, • Ethernet to wireless • Wireless to ethernet • Both
Entry Status	The filters are applied on the IP protocol only when Entry Status is enabled.

:

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

5.10.3.1 Edit Advanced Filtering Table Entries

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



Advance Filtering Edit Entries

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

Figure 5-107 Advance Filtering- Edit Entries

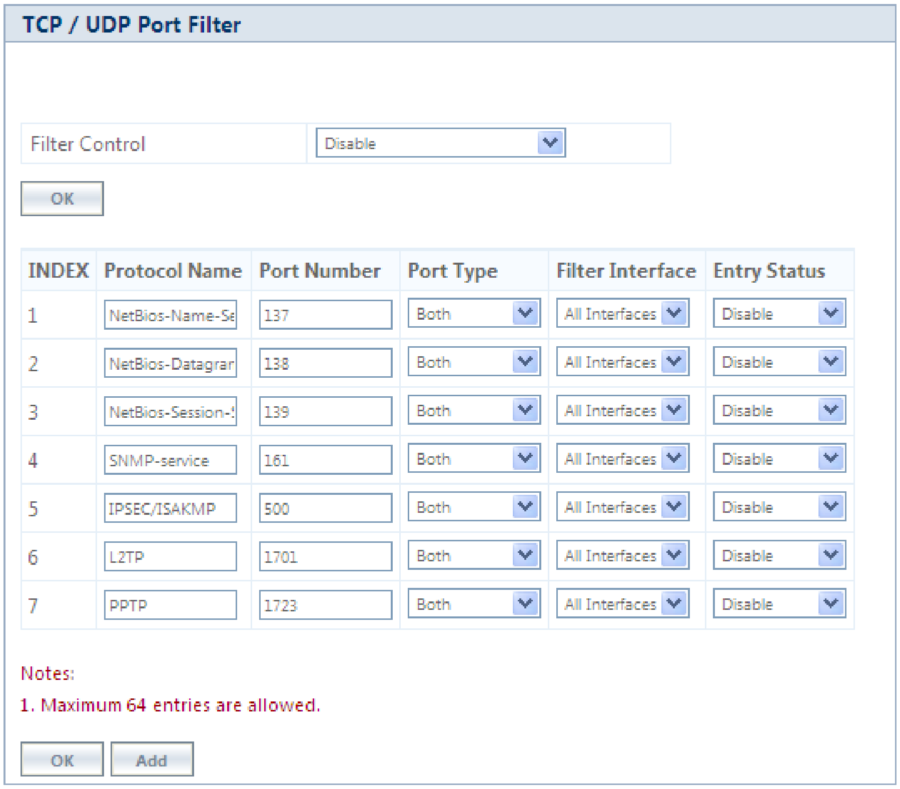
Modify the IP protocol traffic direction that needs to be filtered, and the filtering status for the desired IP Protocol.

Next click **OK** and then **COMMIT**.

5.10.4 TCP/UDP Port Filter

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

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



TCP / UDP Port Filter

Filter Control	Disable

INDEX	Protocol Name	Port Number	Port Type	Filter Interface	Entry Status
1	NetBios-Name-Se	137	Both	All Interfaces	Disable
2	NetBios-Datagrar	138	Both	All Interfaces	Disable
3	NetBios-Session-!	139	Both	All Interfaces	Disable
4	SNMP-service	161	Both	All Interfaces	Disable
5	IPSEC/ISAKMP	500	Both	All Interfaces	Disable
6	L2TP	1701	Both	All Interfaces	Disable
7	PPTP	1723	Both	All Interfaces	Disable

Notes:

1. Maximum 64 entries are allowed.

Figure 5-108 TCP/UDP Port Filter

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

5.10.4.1 TCP/UDP Port Filter Table

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

Parameter	Description
Protocol Name	Represents the name of the service/protocol. Please note that the system throws an error when an attempt is made to edit the default service/protocol name.

Parameter	Description
Port Number	Represents the destination port number. Please note that the system throws an error when an attempt is made to edit the port number.
Port Type	Represents the port type (TCP, UDP, Both).
Filter Interface	Represents the interface on which the filter is applied. The supported interfaces are, • Only Ethernet • Only Wireless • All Interfaces
Entry Status	Set the entry status as either Enable, Disable or Delete. • **Enable**: Filter is applied and filters the packet based on the Port number and port type. • **Disable**: No filter is applied. • **Delete**: Allows to delete only user-defined TCP/UDP port filter entry. When you attempt to delete default entries, the device throws an error.

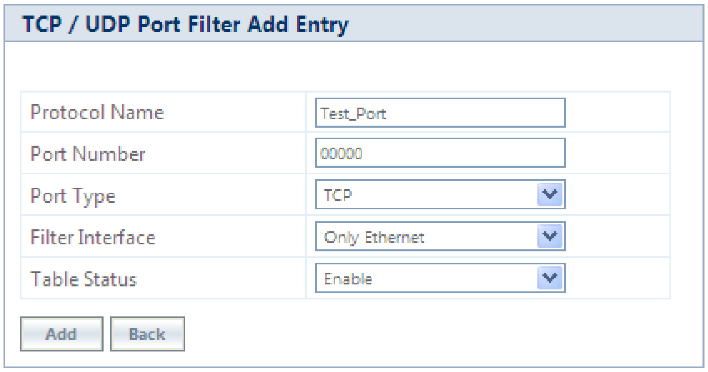
If you have configured any user-defined protocols then click **OK** and then **COMMIT**.

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

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

5.10.4.2 Adding User-defined TCP/UDP Port Filter Entries

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



TCP / UDP Port Filter Add Entry

Protocol Name	Test_Port
Port Number	00000
Port Type	TCP
Filter Interface	Only Ethernet
Table Status	Enable

Figure 5-109 Add User-defined TCP/UDP Protocols

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

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

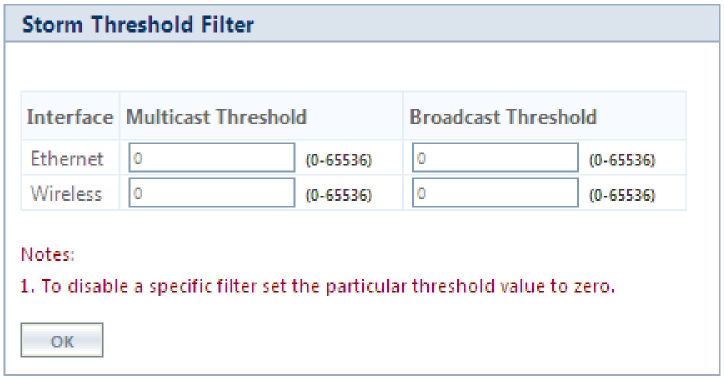
:

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

5.10.5 Storm Threshold Filter

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

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



Storm Threshold Filter

Interface	Multicast Threshold		Broadcast Threshold	
Ethernet	0	(0-65536)	0	(0-65536)
Wireless	0	(0-65536)	0	(0-65536)

Notes:

1. To disable a specific filter set the particular threshold value to zero.

Figure 5-110 Storm Threshold Filter

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

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

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

5.10.6 WORP Intra Cell Blocking

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

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

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

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

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

The following rules apply to Intra Cell Blocking Groups:

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

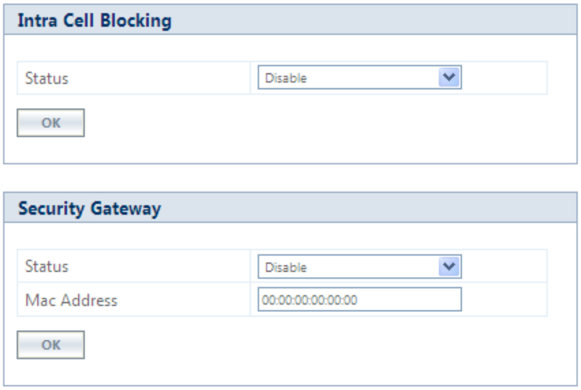
5.10.6.0.1 Example of Intra-Cell Blocking Groups

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

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

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

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



Intra Cell Blocking

Status: Disable

Security Gateway

Status: Disable

Mac Address: 00:00:00:00:00:00

Figure 5-111 Intra Cell Blocking

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

Parameter	Description
Intra Cell Blocking	
Status	By default, Intra Cell Blocking is disabled on a BSU. Select **Enable** to enable the feature and then Click **OK** and then **COMMIT**.
Security Gateway	
Status	By default, Security Gateway is disabled on a BSU. Select **Enable** to enable the feature.
MAC Address	Represents the MAC address of the security gateway. This gateway routes the packets transmitted by the SU to the different BSUs to which it belongs.
After configuring the required parameters, click **OK** and then **COMMIT**.	

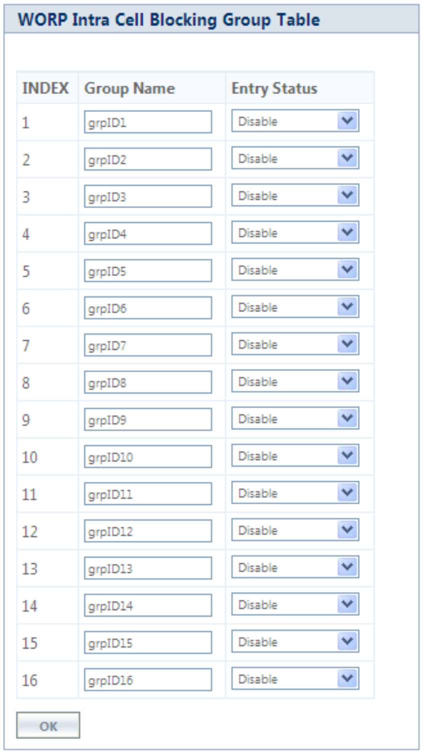
*: Intra Cell Blocking is configurable only in Bridge mode. When you change the device from **Bridge** to **Routing** mode or vice-versa, Intra-Cell Blocking stops or starts working only after device reboot.*

5.10.6.1 WORP Intra Cell Blocking Group Table

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

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

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



WORP Intra Cell Blocking Group Table

INDEX	Group Name	Entry Status
1	grpID1	Disable
2	grpID2	Disable
3	grpID3	Disable
4	grpID4	Disable
5	grpID5	Disable
6	grpID6	Disable
7	grpID7	Disable
8	grpID8	Disable
9	grpID9	Disable
10	grpID10	Disable
11	grpID11	Disable
12	grpID12	Disable
13	grpID13	Disable
14	grpID14	Disable
15	grpID15	Disable
16	grpID16	Disable

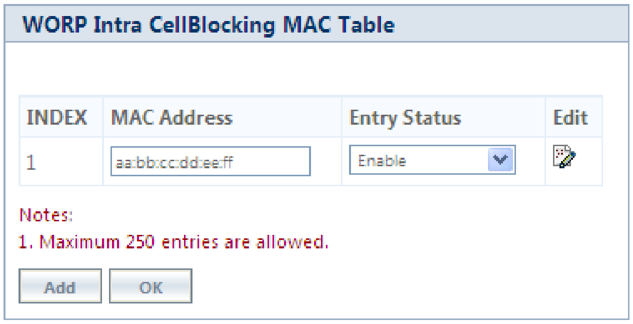
Figure 5-112 WORP Intra Cell Blocking Group Table

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

5.10.6.2 WORP Intra Cell Blocking MAC Table

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

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



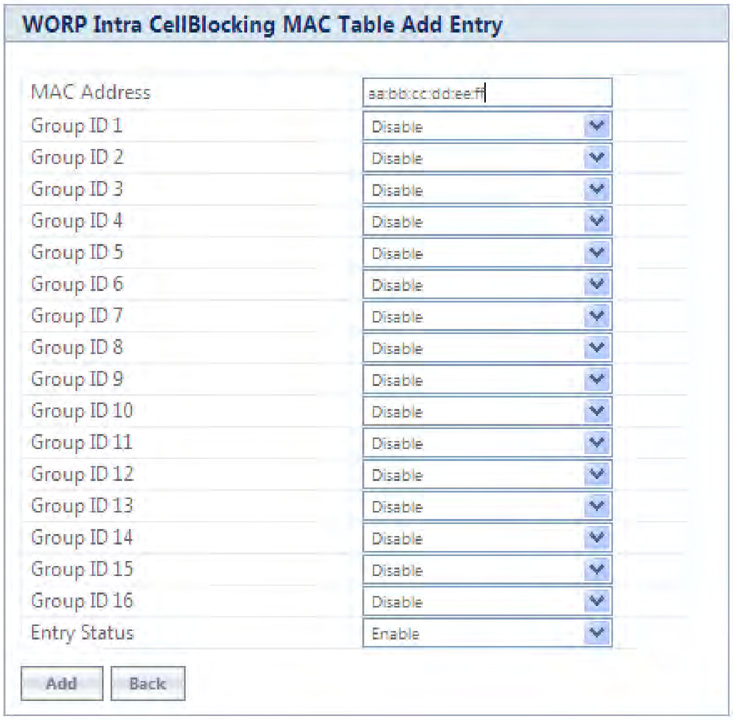
WORP Intra CellBlocking MAC Table

INDEX	MAC Address	Entry Status	Edit
1	aa:bb:cc:dd:ee:ff	Enable	✎

Notes:
1. Maximum 250 entries are allowed.

Figure 5-113 WORP Intra Cell Blocking MAC Table

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



WORP Intra CellBlocking MAC Table Add Entry

MAC Address	aa:bb:cc:dd:ee:ff
Group ID 1	Disable
Group ID 2	Disable
Group ID 3	Disable
Group ID 4	Disable
Group ID 5	Disable
Group ID 6	Disable
Group ID 7	Disable
Group ID 8	Disable
Group ID 9	Disable
Group ID 10	Disable
Group ID 11	Disable
Group ID 12	Disable
Group ID 13	Disable
Group ID 14	Disable
Group ID 15	Disable
Group ID 16	Disable
Entry Status	Enable

Figure 5-114 WORP Intra Cell Blocking MAC Table Add Entry

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

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

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

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

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

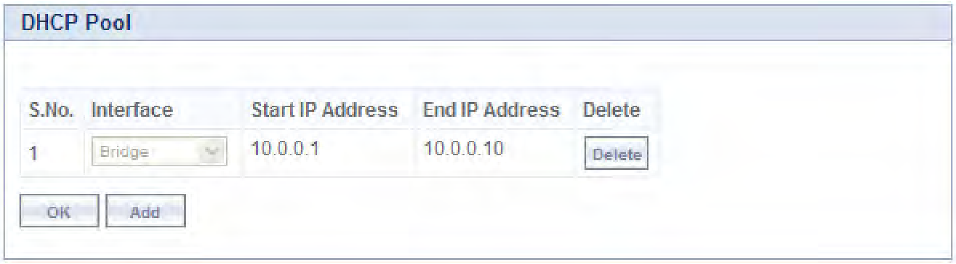
5.11 DHCP

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

5.11.1 DHCP Pool

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

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


DHCP Pool

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

Figure 5-115 DHCP Pool

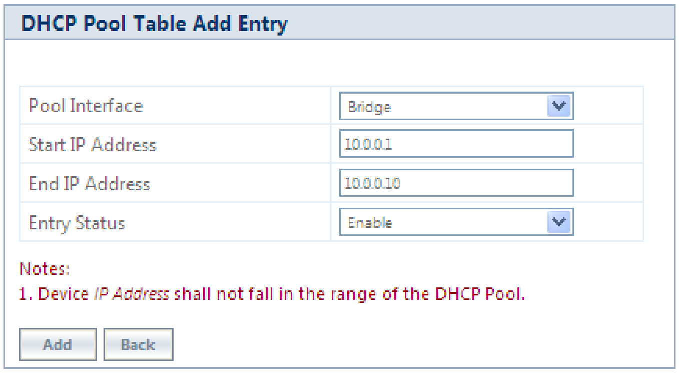
Each pool entry comprises the following tabulated information:

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

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

5.11.1.1 Adding a New Pool Entry

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



DHCP Pool Table Add Entry

Pool Interface	Bridge
Start IP Address	10.0.0.1
End IP Address	10.0.0.10
Entry Status	Enable

Notes:
1. Device *IP Address* shall not fall in the range of the DHCP Pool.

Figure 5-116 DHCP Pool Table Add Entry

Enter the pool details and click **Add**. The entry will be updated in the DHCP pool table.

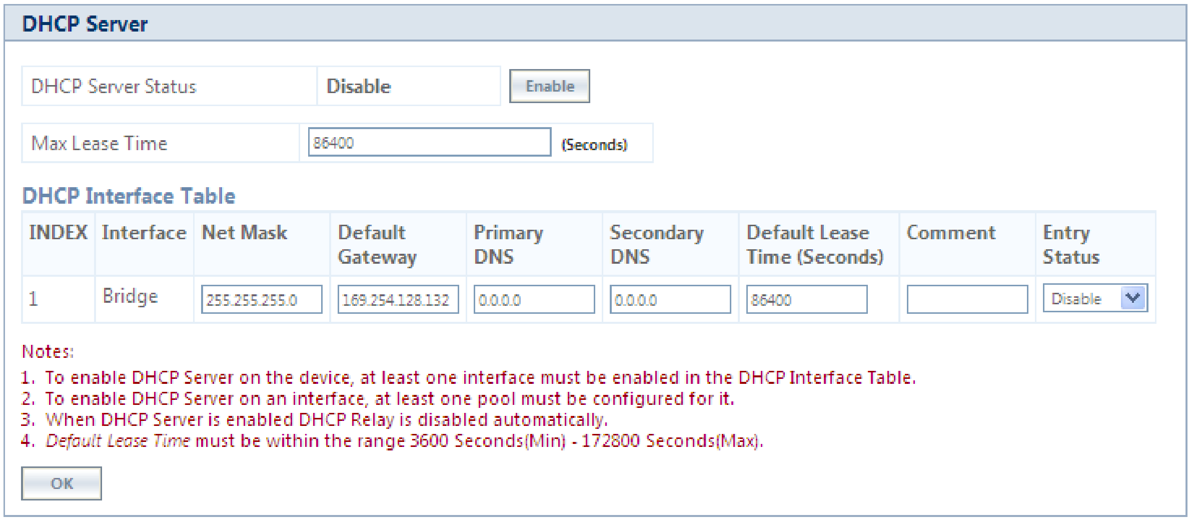
To apply the configured changes, click **COMMIT**.

5.11.2 DHCP Server

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

DHCP Server feature is applicable to both **Bridge** and **Routing** Mode. In Routing mode, DHCP Server can be configured for each interface (Ethernet and Wireless) separately. Unless the DHCP Server functionality is enabled for an interface, the DHCP Server does not respond to the DHCP requests received on that interface.

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



DHCP Server

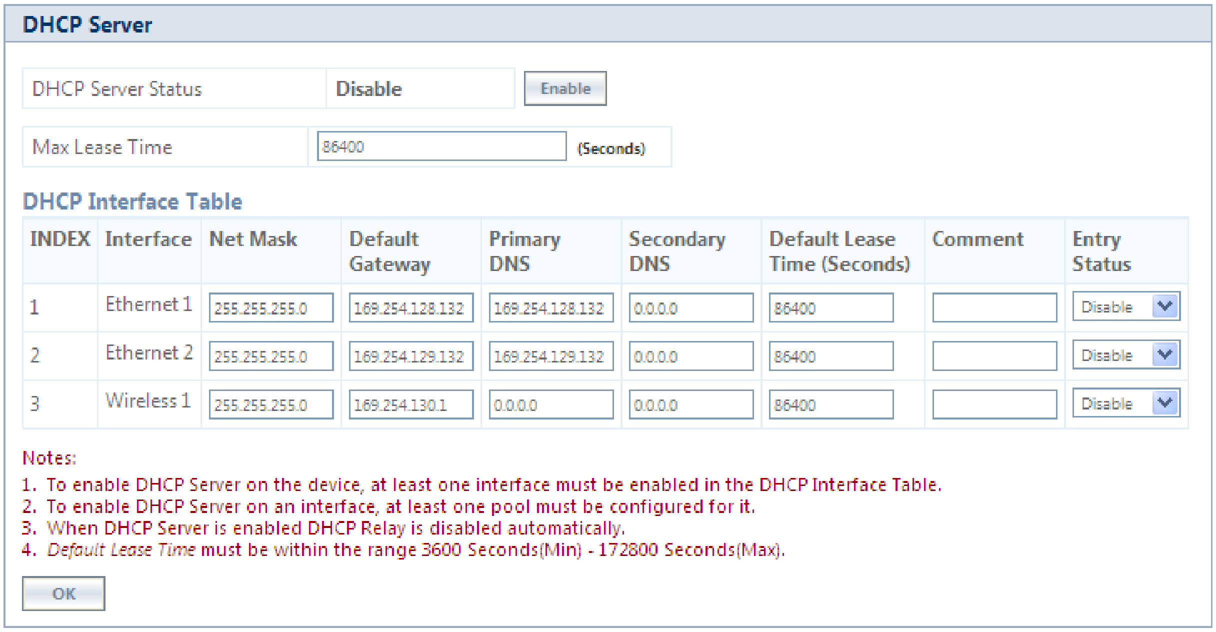
DHCP Server Status	Disable	Enable
Max Lease Time	86400	(Seconds)

DHCP Interface Table

INDEX	Interface	Net Mask	Default Gateway	Primary DNS	Secondary DNS	Default Lease Time (Seconds)	Comment	Entry Status
1	Bridge	255.255.255.0	169.254.128.132	0.0.0.0	0.0.0.0	86400		Disable

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

Figure 5-117 DHCP Server (Bridge Mode)



DHCP Server

DHCP Server Status	Disable	Enable
Max Lease Time	86400	(Seconds)

DHCP Interface Table

INDEX	Interface	Net Mask	Default Gateway	Primary DNS	Secondary DNS	Default Lease Time (Seconds)	Comment	Entry Status
1	Ethernet 1	255.255.255.0	169.254.128.132	169.254.128.132	0.0.0.0	86400		Disable
2	Ethernet 2	255.255.255.0	169.254.129.132	169.254.129.132	0.0.0.0	86400		Disable
3	Wireless 1	255.255.255.0	169.254.130.1	0.0.0.0	0.0.0.0	86400		Disable

Notes:

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

Figure 5-118 DHCP Server (Routing Mode)

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

Parameter	Description
DHCP Server Status	By default, DHCP Server is disabled on a device. To enable DHCP Server, select **Enable**. A DHCP Server can be enabled only when the following two conditions are satisfied: 1. Before enabling, atleast one interface should be enabled on which the DHCP Server has to run. 2. The DHCP pool table should have atleast one pool configured for that interface.
Max Lease Time	Specifies the maximum lease time for which the DHCP client can use the IP address provided by the DHCP Server. The value ranges from 3600 - 172800 seconds.
DHCP Interface Table	
Interface Type	Specifies the interface for which the DHCP Server functionality shall be configured. That is Bridge or Ethernet/Wireless in case of Routing mode.
Net Mask	Specifies the subnet mask to be sent to the DHCP client along with the assigned IP address. The netmask configured here should be greater than or equal to the netmask configured on the interface.
Default Gateway	Specifies the default gateway to be sent to the DHCP client along with the assigned IP Address. Default Gateway is a node that serves as an accessing point to another network.
Primary DNS	Specifies the primary DNS (Domain Name Server) IP address to be sent to the DHCP client.
Secondary DNS	Specifies the secondary DNS IP address to be sent to the DHCP client.

Parameter	Description
Default Lease Time	DHCP Server uses this option to specify the lease time it is willing to offer to the DHCP client over that interface. Once the lease time expires, the DHCP Server allocates a new IP address to the device. The **Default Lease Time** should be less than or equal to the configured **Max Lease Time**.
Comment	Specifies a note for the device administrator.
Entry Status	Used to **Enable** or **Disable** the DHCP Server functionality over the interface.

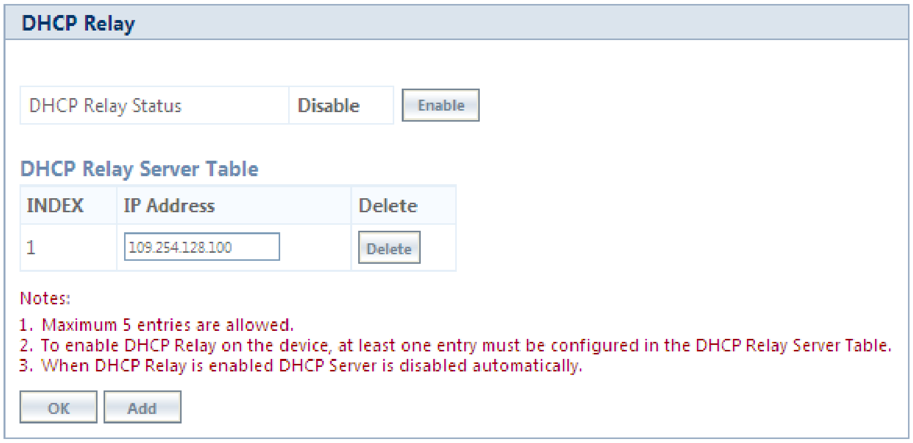
After configuring the required parameters, click **OK** and then **COMMIT**.

5.11.3 DHCP Relay (Routing Mode only)

The DHCP relay agent relays DHCP messages between the DHCP Clients and the configured DHCP Servers on different IP networks. You can configure a maximum of five DHCP Servers. There must be at least one DHCP Server configured in order to relay DHCP request.

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

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



DHCP Relay

DHCP Relay Status	Disable	Enable

DHCP Relay Server Table

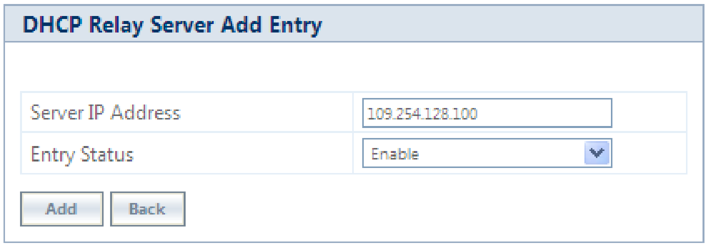
INDEX	IP Address	Delete
1	109.254.128.100	Delete

Notes:
1. Maximum 5 entries are allowed.
2. To enable DHCP Relay on the device, at least one entry must be configured in the DHCP Relay Server Table.
3. When DHCP Relay is enabled DHCP Server is disabled automatically.

Figure 5-119 DHCP Relay

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

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



DHCP Relay Server Add Entry

Server IP Address	109.254.128.100
Entry Status	Enable

Figure 5-120 DHCP Relay Server Add Entry

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

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

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

5.12 IGMP Snooping

: IGMP Snooping is applicable only in Bridge Mode.

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

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

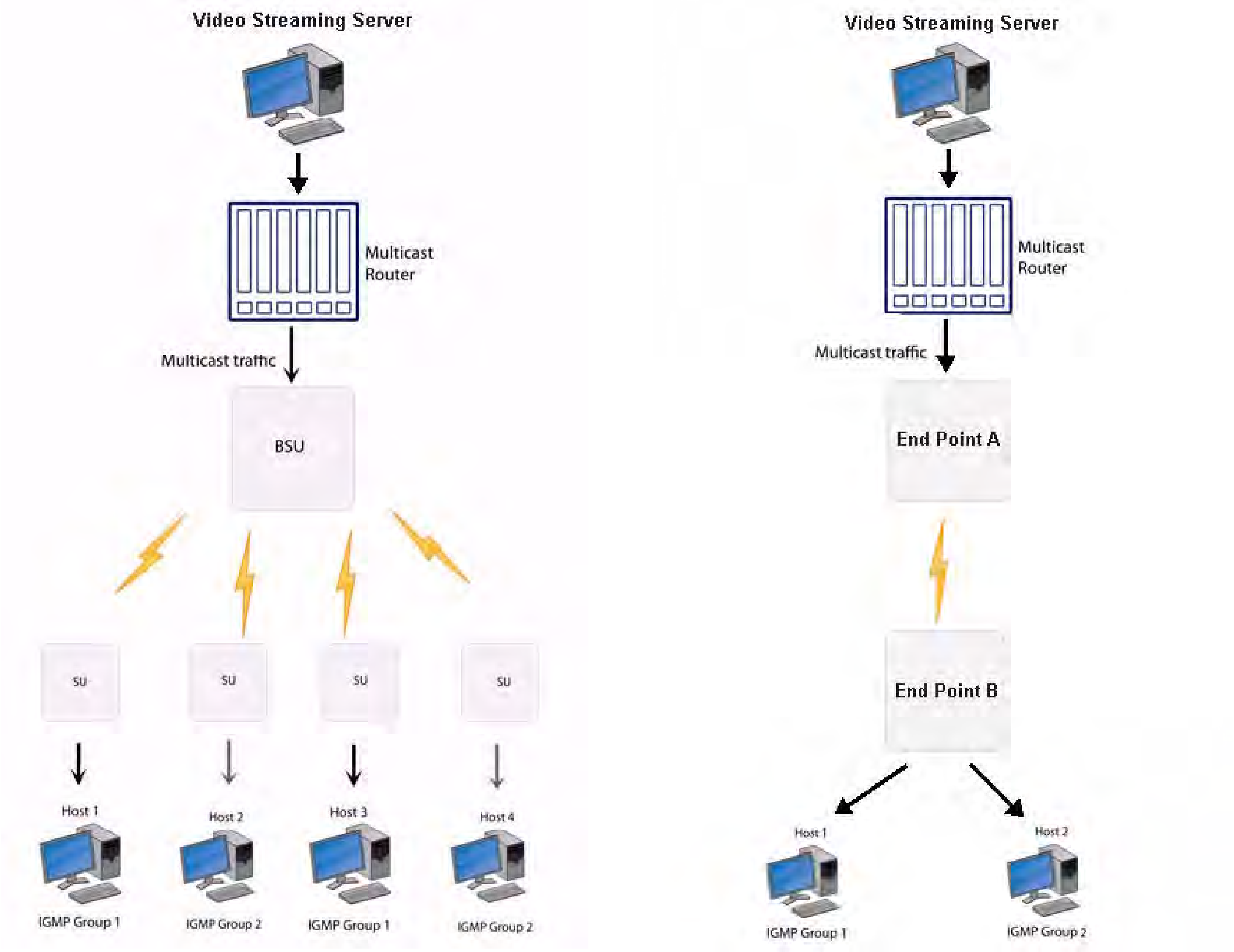


Figure 5-121 IGMP Snooping Process

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

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

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

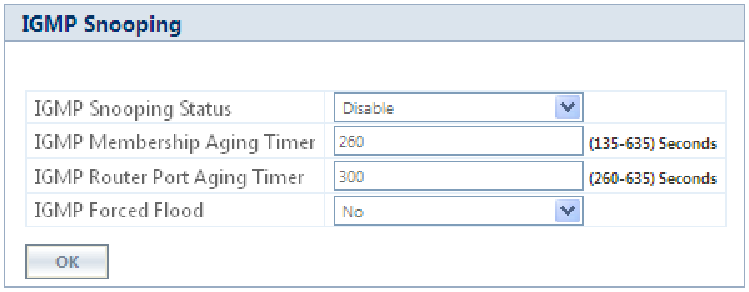
IGMP Snooping is of 2 kinds:

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

:

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

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



IGMP Snooping

IGMP Snooping Status	Disable	
IGMP Membership Aging Timer	260	(135-635) Seconds
IGMP Router Port Aging Timer	300	(260-635) Seconds
IGMP Forced Flood	No	

Figure 5-122 IGMP Snooping

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

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

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

Management

6

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

- System
- File Management
- Services
- Simple Network Time Protocol (SNTP)
- Access Control
- Reset to Factory
- Convert QB to MP
- Auto Config Recovery

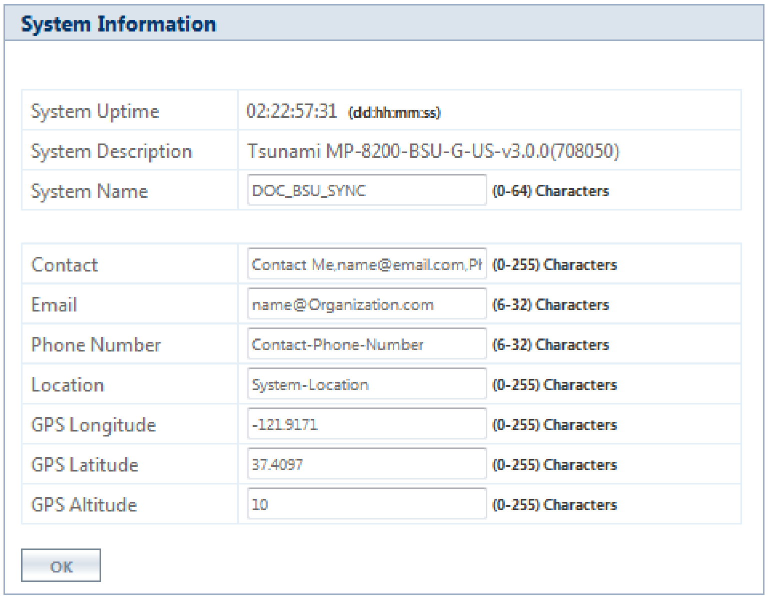
! ***: Recommended characters for the name field are A-Z a-z 0-9 - _ = : . @ $ & and space.***

6.1 System

6.1.1 System Information

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

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



System Information

System Uptime	02:22:57:31 (dd:hh:mm:ss)	
System Description	Tsunami MP-8200-BSU-G-US-v3.0.0(708050)	
System Name	DOC_BSU_SYNC	(0-64) Characters
Contact	Contact Me,name@email.com,Pł	(0-255) Characters
Email	name@Organization.com	(6-32) Characters
Phone Number	Contact-Phone-Number	(6-32) Characters
Location	System-Location	(0-255) Characters
GPS Longitude	-121.9171	(0-255) Characters
GPS Latitude	37.4097	(0-255) Characters
GPS Altitude	10	(0-255) Characters

Figure 6-1 System Information

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

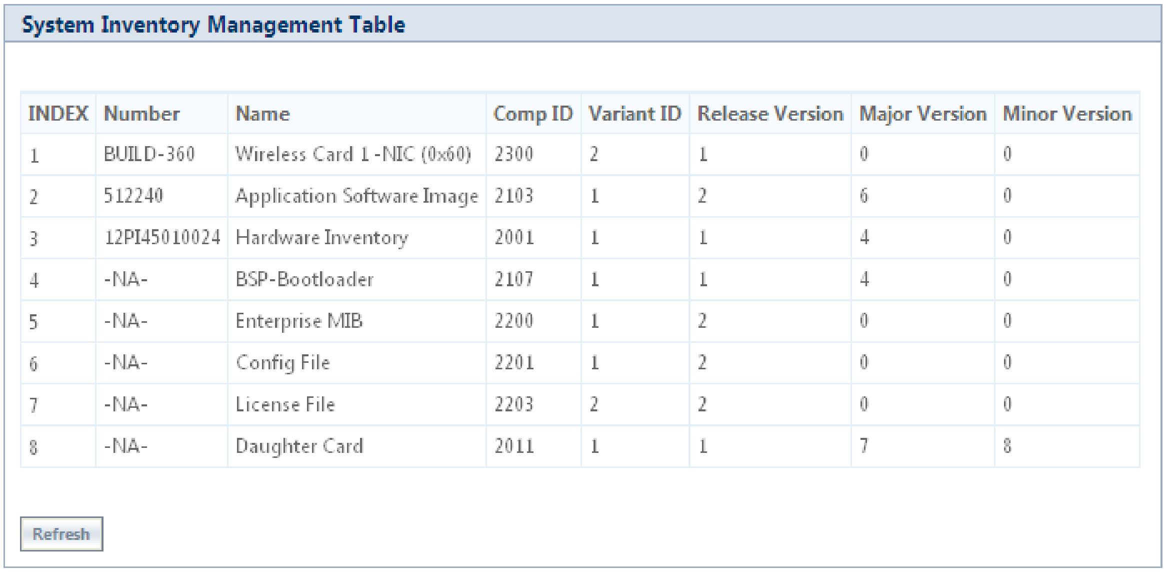
Parameter	Description
System Up-Time	This is a read-only parameter. It represents the operational time of the device since its last reboot.
System Description	This is a read-only parameter. It provides system description such as system name, firmware version and the latest firmware build supported. For example: MP-8200-BSU-G-US-v3.X.Y(Build No.)
System Name	Represents the name assigned to the device. You can enter a system name of maximum 64 characters and should be unique across all devices in WORP network.
Email	Represents the email address of the person administering the device. You can enter an email address of minimum 6 and maximum 32 characters.
Phone Number	Represents the phone number of the person administering the device. You can enter a phone number of minimum 6 and maximum 32 characters.
Location	Represents the location where the device is installed. You can enter the location name of minimum 0 and maximum 255 characters.
GPS Longitude	Represents the longitude at which the device is installed. You can enter a longitude value of minimum 0 and maximum 255 characters.
GPS Latitude	Represents the latitude at which the device is installed. You can enter a latitude value of minimum 0 and maximum 255 characters.
GPS Altitude	Represents the altitude at which the device is installed. You can enter a altitude value of minimum 0 and maximum 255 characters.

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

6.1.2 Inventory Management

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

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



System Inventory Management Table

INDEX	Number	Name	Comp ID	Variant ID	Release Version	Major Version	Minor Version
1	BUILD-360	Wireless Card 1 -NIC (0x60)	2300	2	1	0	0
2	512240	Application Software Image	2103	1	2	6	0
3	12PI45010024	Hardware Inventory	2001	1	1	4	0
4	-NA-	BSP-Bootloader	2107	1	1	4	0
5	-NA-	Enterprise MIB	2200	1	2	0	0
6	-NA-	Config File	2201	1	2	0	0
7	-NA-	License File	2203	2	2	0	0
8	-NA-	Daughter Card	2011	1	1	7	8

Figure 6-2 An Example - Inventory Management

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

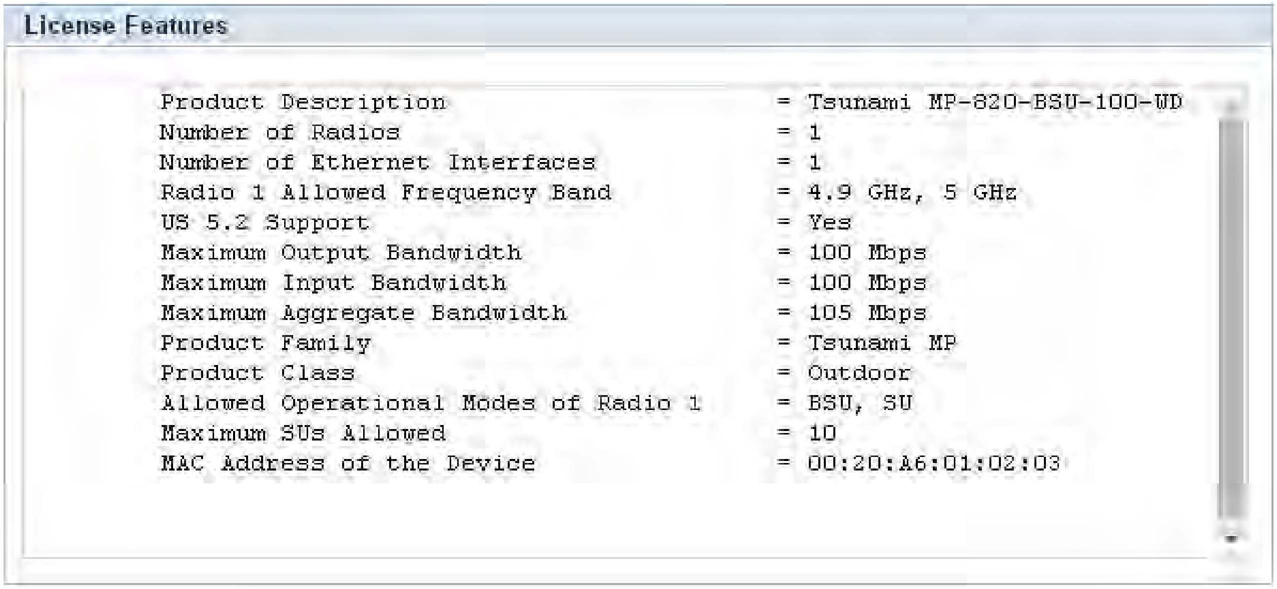
Click **Refresh**, to view the updated system inventory management information.

6.1.3 Licensed Features

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

Licensed Features are, by default, set by the company.

To view the licensed features set on the device, click **MANAGEMENT** > **System** > **Licensed Features**. The **Licensed Features** screen appears.



License Features

```
Product Description                        = Tsunami MP-820-BSU-100-WD
Number of Radios                           = 1
Number of Ethernet Interfaces              = 1
Radio 1 Allowed Frequency Band             = 4.9 GHz, 5 GHz
US 5.2 Support                             = Yes
Maximum Output Bandwidth                   = 100 Mbps
Maximum Input Bandwidth                    = 100 Mbps
Maximum Aggregate Bandwidth                = 105 Mbps
Product Family                             = Tsunami MP
Product Class                              = Outdoor
Allowed Operational Modes of Radio 1       = BSU, SU
Maximum SUs Allowed                        = 10
MAC Address of the Device                  = 00:20:A6:01:02:03
```

Figure 6-3 An Example - Licensed Features

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

Parameter	Description
Product Description	Description about the device.
Number of Radios	The number of radios the device supports.
Number of Ethernet Interfaces	The number of Ethernet interfaces supported by the device.
Radio 1 Allowed Frequency Band	The operational frequency band supported by the device radio.
US 5.2 Support	The US 5.2 frequency band is supported by the device if "**yes**".
Maximum Output Bandwidth	The maximum output bandwidth limit of the device. It is represented in mbps.
Maximum Input Bandwidth	The maximum input bandwidth limit of the device. It is represented in mbps. : *The Input and Output Bandwidth features are referred with respect to the wireless interface. Input bandwidth refers to the data received on the wireless interface and output bandwidth refers to the data sent out of the wireless interface.*
Maximum Aggregate Bandwidth	The maximum cumulative bandwidth of the device, which is the sum of configured output and input bandwidths.
Product Family	Represents the product family of the device.
Product Class	Represents the product class of the device, which is either indoor or outdoor.
Allowed Operational Modes of Radio1	Represents the operational mode of the device, that is, BSU/SU/End Point A/End Point B.
Maximum SUs Allowed	The maximum number of SUs that a BSU supports.
MAC address of the Device is	The MAC address of the device.

6.1.3.1 License Upgrade Procedure

In order to get additional bandwidth**/**US 5.2 G Hz frequency band **Upgrade the License** by following the procedure given below:

- Retrieve the license information (**License Info** file with **.lic** extension) from the device. For more details, refer Retrieve From Device section.

To purchase a license upgrade, please contact your Proxim Sales Representative; to generate a unique license file for your device, please refer to the Technical Note available on Proxim support site: https://my.proxim.com/article/3003 (for bandwidth), and https://my.proxim.com/article/3008 (for US 5.2 G Hz support).

- Upgrade the bandwidth using the license file(**.bin** extension) generated in the above step. For more details, refer Upgrade License section.

6.2 File Management

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

6.2.1 TFTP Server

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

While using TFTP server, ensure the following:

- The upload or download directory is correctly set (the default directory is **C:\TFTP-Root**).
- The required firmware file is present in the directory.
- The TFTP server is running during file upload and download. You can check the connectivity between the device and the TFTP server by pinging the device from the Personal Computer that hosts the TFTP server. The ping program should show replies from the device.
- The TFTP server should be configured to transmit and receive files (on the Security tab under **File > Configure**), with no automatic shutdown or time-out (on the **Auto-Close** tab).

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

6.2.2 Text Based Configuration (TBC) File Management

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

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

6.2.2.1 Generating TBC File

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

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

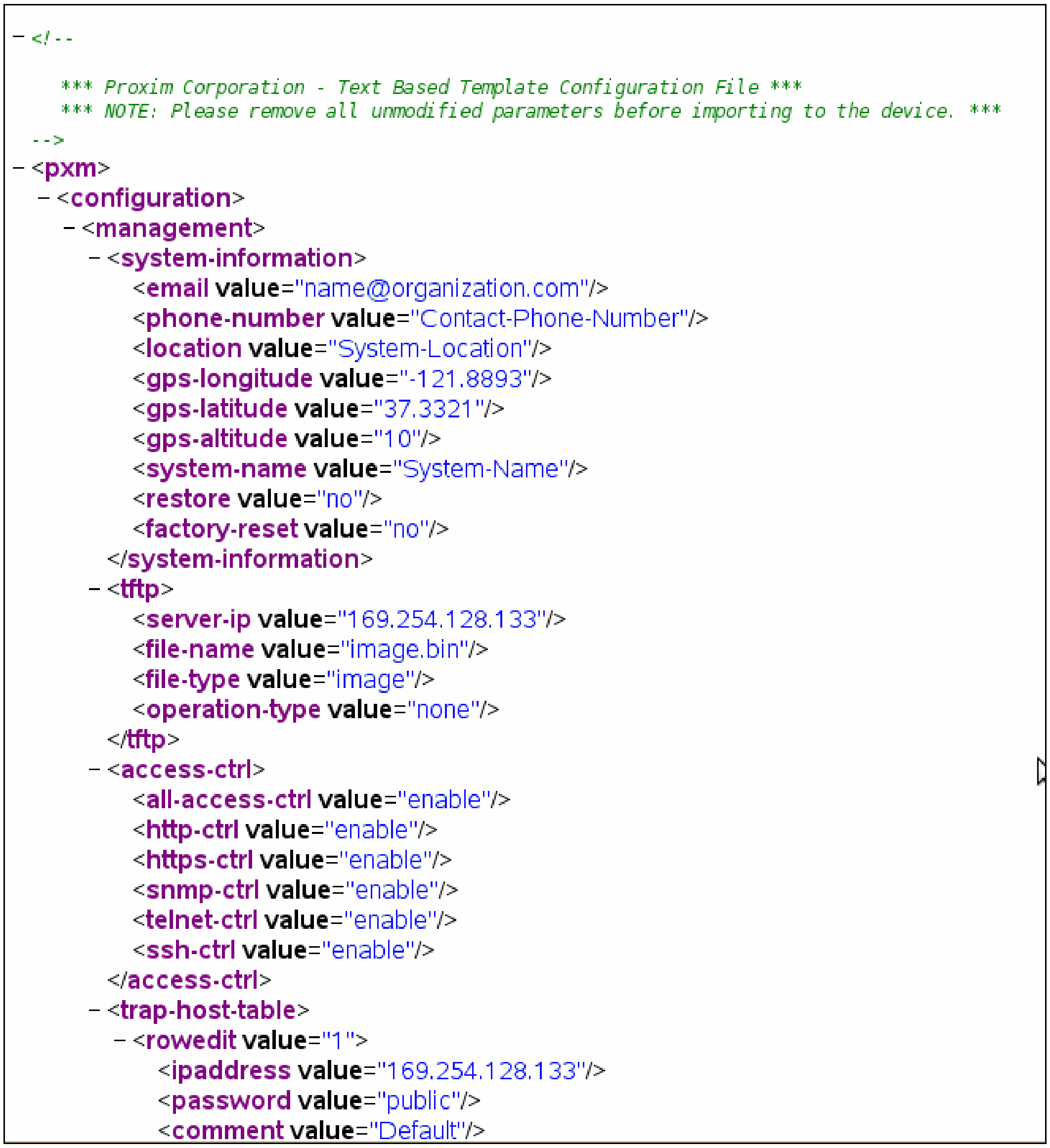
The commands used for the generation of TBC file are:

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

The generated TBC file contains,

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

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



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

Figure 6-4 TBC File in xml Format

6.2.2.2 Editing the TBC File

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

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

6.2.2.3 Loading the TBC file

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

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

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

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

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

:

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

6.2.3 Upgrade Firmware

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

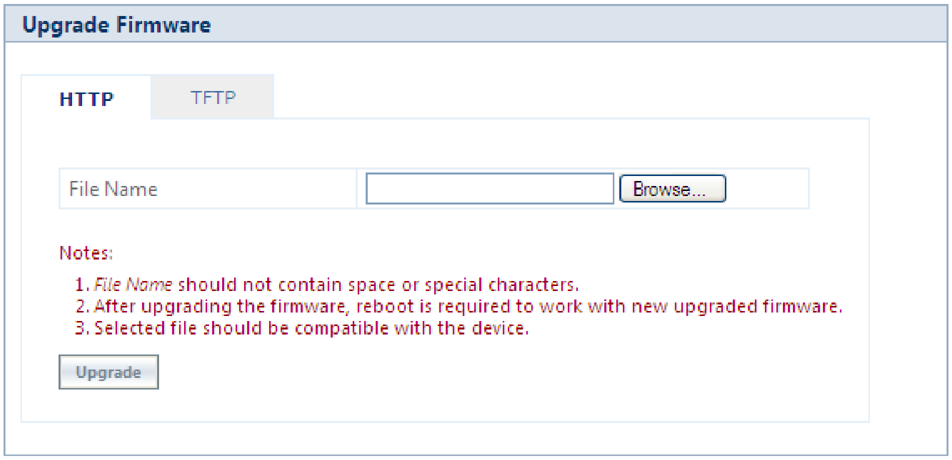
:

- *Make sure the firmware being loaded is compatible to the device being upgraded.*
- *In a point-to-multipoint network, it is recommended to upgrade the base station first and then the subscriber(s).*
- *In a point-to-point network, it is recommended to upgrade the End Point A first and then the End Point B.*

6.2.3.1 Upgrade Firmware via HTTP

To upgrade the firmware via HTTP, do the following:

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



Upgrade Firmware

File Name

Notes:

1. *File Name* should not contain space or special characters.
2. After upgrading the firmware, reboot is required to work with new upgraded firmware.
3. Selected file should be compatible with the device.

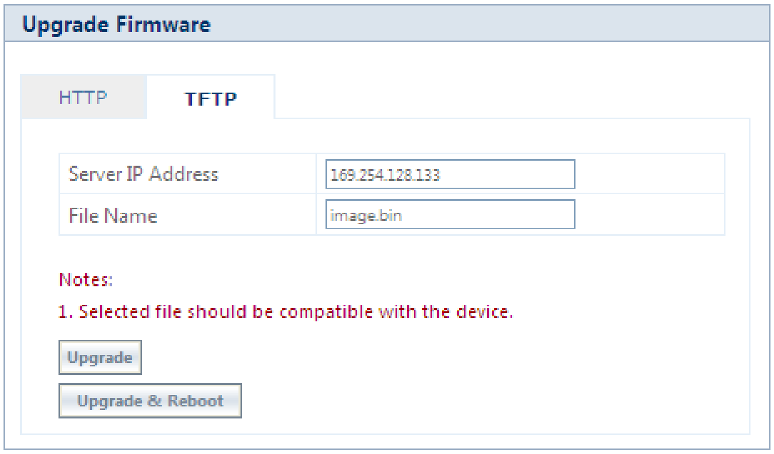
Figure 6-5 Upgrade Firmware - HTTP

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

6.2.3.2 Upgrade Firmware via TFTP

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

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



Upgrade Firmware

Server IP Address	169.254.128.133
File Name	image.bin

Notes:

1. Selected file should be compatible with the device.

Figure 6-6 Upgrade Firmware - TFTP

2. Based on the IP mode configure either IPv4 or IPv6 address as TFTP Server address.
3. Enter the name of the latest firmware file (including the file extension) that has to be loaded onto the device in the **File Name** box.
4. To upgrade the device with new firmware click **Upgrade** and then reboot the device, or click **Upgrade & Reboot**.

:

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

- *If the device configuration is upgraded from the version 2.6.x to 3.0.x, with the channel bandwidth 5MHz, then the device boots up in the* ***custom*** *compatibility mode with* ***10ms*** *timeframe.*

6.2.4 Upgrade Configuration

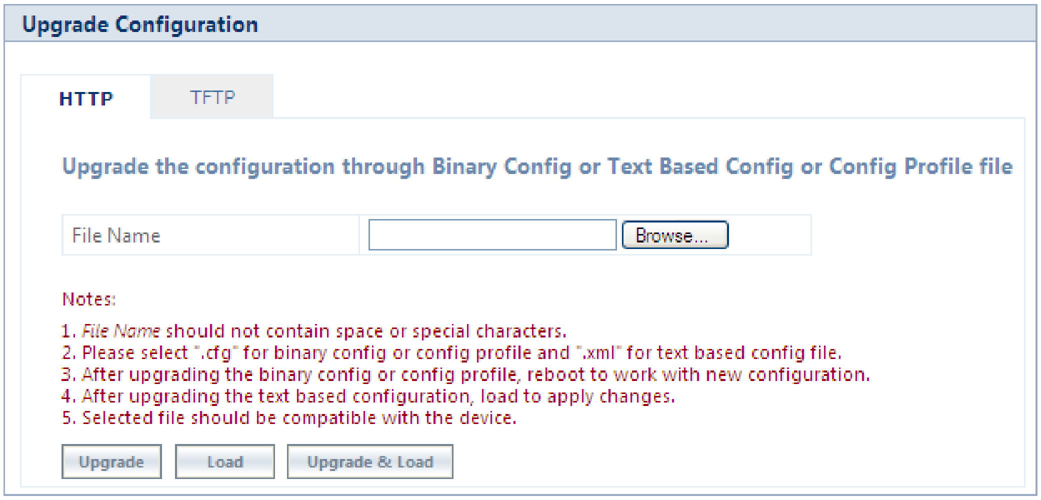
You can upgrade the device with the latest configuration files either through HTTP or TFTP.

: Make sure the configuration file being loaded into the device is compatible. That is, the configuration file being loaded should have been retrieved from a device of the same SKU.

6.2.4.1 Upgrade Configuration via HTTP

To upgrade the configuration files by using HTTP, do the following:

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


Upgrade Configuration
HTTP
TFTP
Upgrade the configuration through Binary Config or Text Based Config or Config Profile file
File Name
Browse...
Upgrade
Load
Upgrade & Load

Notes:

1. *File Name* should not contain space or special characters.
2. Please select ".cfg" for binary config or config profile and ".xml" for text based config file.
3. After upgrading the binary config or config profile, reboot to work with new configuration.
4. After upgrading the text based configuration, load to apply changes.
5. Selected file should be compatible with the device.

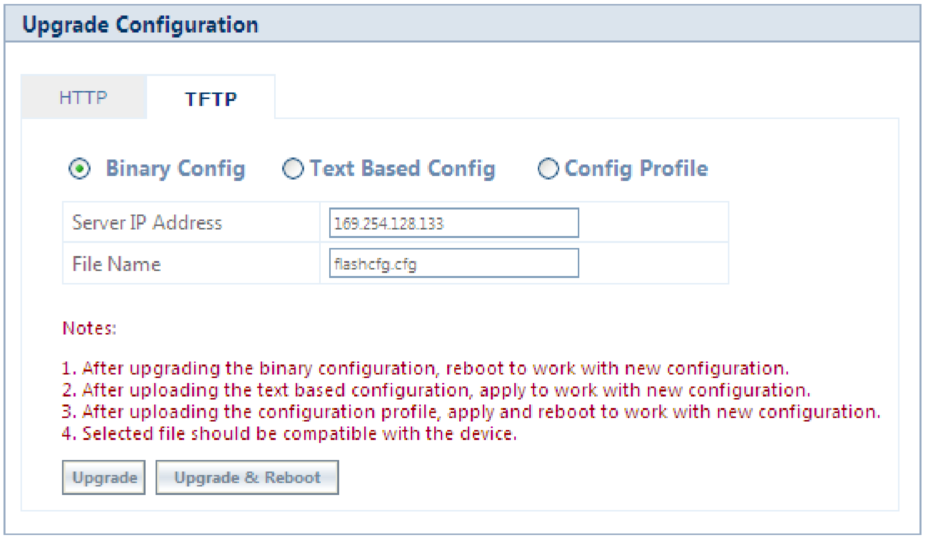
Figure 6-7 Upgrade Configuration - HTTP

2. In the HTTP screen, click **Browse** to locate the configuration file. Select a Binary Configuration file or a Config Profile file, or a **PXM-TBC.xml** for Text Based Configuration file. Make sure that the file name does not contain any space or special characters.
3. If you are upgrading the device with Binary Configuration file then click **Upgrade** and then reboot the device.
4. If you are upgrading the device with Config Profile file then click **Upgrade** and then reboot the device. On upgrade, the device shall come up with the loaded profile. If the configuration profile is not compatible, then on reboot, the device will rollback to its old configuration.
5. If you are upgrading the device with Text Based Configuration file then click **Upgrade** to upgrade the device with the config file and then click **Load** for loading the config file onto the device. Alternatively, you can perform both upgrade and load operation in one single step, by clicking **Upgrade & Load**.

6.2.4.2 Upgrade Configuration via TFTP

To upgrade the configuration files by using TFTP Server, do the following:

1. Navigate to **MANAGEMENT** > **File Management** > **Update Configuration > TFTP**.



Upgrade Configuration

● Binary Config ○ Text Based Config ○ Config Profile

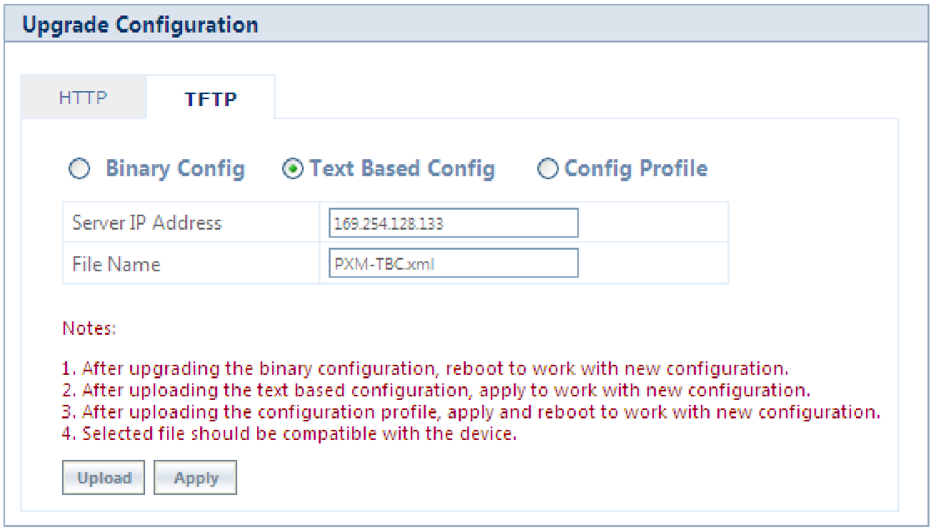
Server IP Address	169.254.128.133
File Name	flashcfg.cfg

Notes:

1. After upgrading the binary configuration, reboot to work with new configuration.
2. After uploading the text based configuration, apply to work with new configuration.
3. After uploading the configuration profile, apply and reboot to work with new configuration.
4. Selected file should be compatible with the device.

Figure 6-8 Upgrade Binary Configuration via TFTP

2. You can update the device with three types of configuration files: Binary, Text Based and Config Profile. To update the device with Binary Configuration file, select **Binary Config**.
   - Based on the IP mode configure either IPv4 or IPv6 address as TFTP Server address.
   - Enter the name of the Binary file (including the file extension) that has to be downloaded onto the device in the **File Name** box.
3. To update the device with Text Based Configuration files, select **Text Based Config**.
   - Based on the IP mode configure either IPv4 or IPv6 address as TFTP Server address.
   - Enter the name of the Text Based file (including the file extension) that has to be downloaded onto the device in the **File Name** box.



Upgrade Configuration

○ Binary Config ● Text Based Config ○ Config Profile

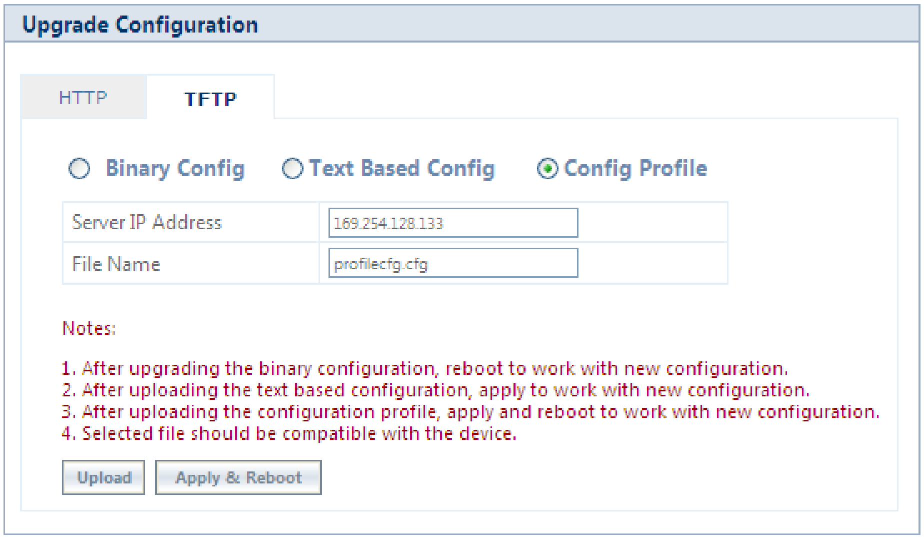
Server IP Address	169.254.128.133
File Name	PXM-TBC.xml

Notes:

1. After upgrading the binary configuration, reboot to work with new configuration.
2. After uploading the text based configuration, apply to work with new configuration.
3. After uploading the configuration profile, apply and reboot to work with new configuration.
4. Selected file should be compatible with the device.

Figure 6-9 Upgrade Text Based Configuration via TFTP

4. To update the device with Configuration Profile files, select **Config Profile**.
   - Based on the IP mode, configure either IPv4 or IPv6 address as TFTP Server address.
   - Enter the name of the Config Profile file (including the file extension) that has to be downloaded onto the device in the **File Name** box.


Upgrade Configuration

○ Binary Config ○ Text Based Config ● Config Profile

Server IP Address	169.254.128.133
File Name	profilecfg.cfg

Notes:

1. After upgrading the binary configuration, reboot to work with new configuration.
2. After uploading the text based configuration, apply to work with new configuration.
3. After uploading the configuration profile, apply and reboot to work with new configuration.
4. Selected file should be compatible with the device.

Figure 6-10 Upgrade Configuration Profile via TFTP

5. If you are upgrading the device with Binary Configuration file then click **Upgrade** and then reboot the device, or click **Upgrade & Reboot**.
6. If you are upgrading the device with Text Based Configuration file, click **Upload** and then click **Apply**.
7. If you are upgrading the device with Config profile file then click **Upload** and then reboot the device, or click **Apply & Reboot**.

: It is recommended not to navigate away from the upgrade screen, while the upgrade is in progress.

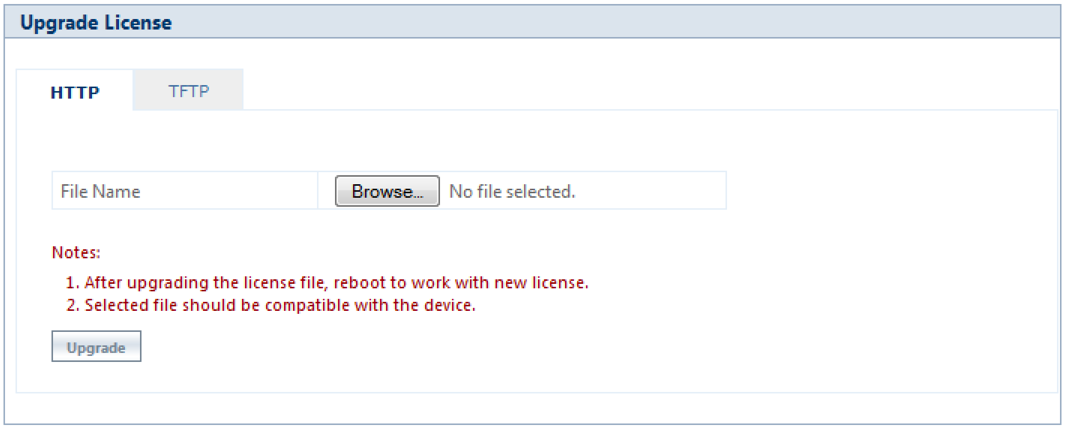
6.2.5 Upgrade License

You can upgrade the license file on the device either through HTTP or TFTP. Refer License Upgrade Procedure section for more details.

6.2.5.1 Upgrade License via HTTP

To upgrade the license using HTTP, do the following:

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


Upgrade License

File Name	Browse... No file selected.

Notes:

1. After upgrading the license file, reboot to work with new license.
2. Selected file should be compatible with the device.

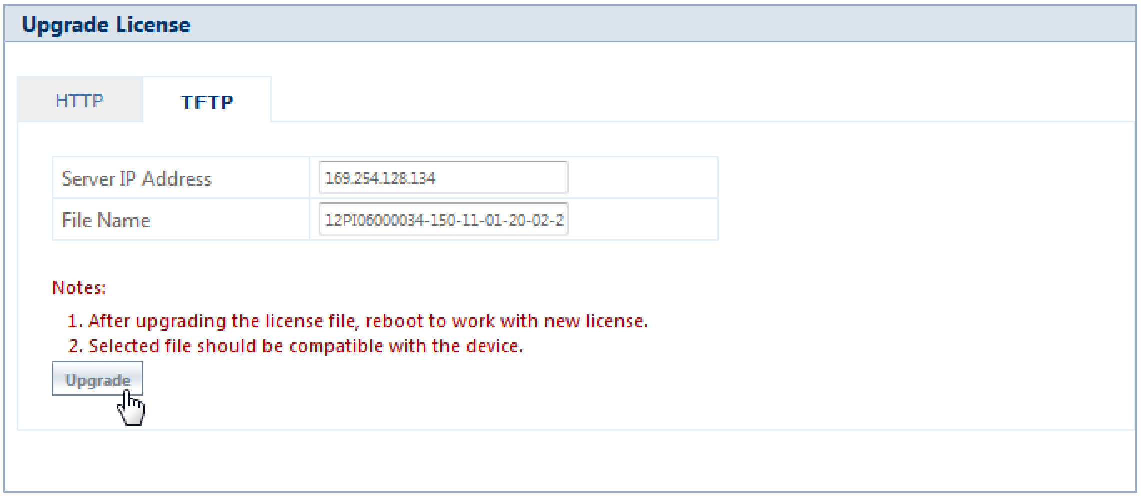
Figure 6-11 Upgrade License via HTTP

2. In the HTTP screen, click **Browse** to locate the license upgrade(**.bin**) file to be loaded on the device.
3. Click **Upgrade** button to upgrade the license on the device and then reboot the device.

6.2.5.2 Upgrade License via TFTP

To upgrade the license file using TFTP Server, do the following:

1. Navigate to **MANAGEMENT** > **File Management** > **Update License > TFTP**.



Server IP Address	169.254.128.134
File Name	12PI06000034-150-11-01-20-02-2

Notes:

1. After upgrading the license file, reboot to work with new license.
2. Selected file should be compatible with the device.

Figure 6-12 Upgrade License via TFTP

2. Based on the IP mode, configure either IPv4 or IPv6 address as TFTP Server address.
3. Enter the name of the file (including the file extension) that has to be loaded on the device, in the **File Name** box.
4. Click **Upgrade** button to upgrade the license on the device and then reboot the device.

- *Upgrade license can be done through CLI/Web Interface/SNMP.*
- *License Upgrade for **Bandwidth**:*
  - *It is applicable only to MP-820-SUA-50⁺ and MP-825-SUR-50⁺ devices.*
  - *Please refer to https://my.proxim.com/article/3003 to obtain license.*
  - *After license upgrade and device reboot, please reconfigure the WORP input and output bandwidth limits as per the new licensed values; for more information, refer Input Bandwidth Limit and Output Bandwidth Limit.*
- *License Upgrade for **WORP Sync** Functionality:*
  - For **82xx-G** and **82x Series** MP and QB devices,
    - *WORP sync is enabled on units produced till the end of 2014. After this time period, license has to be obtained to enable this functionality. Please contact customer support/SE for more details on how to obtain the license.*

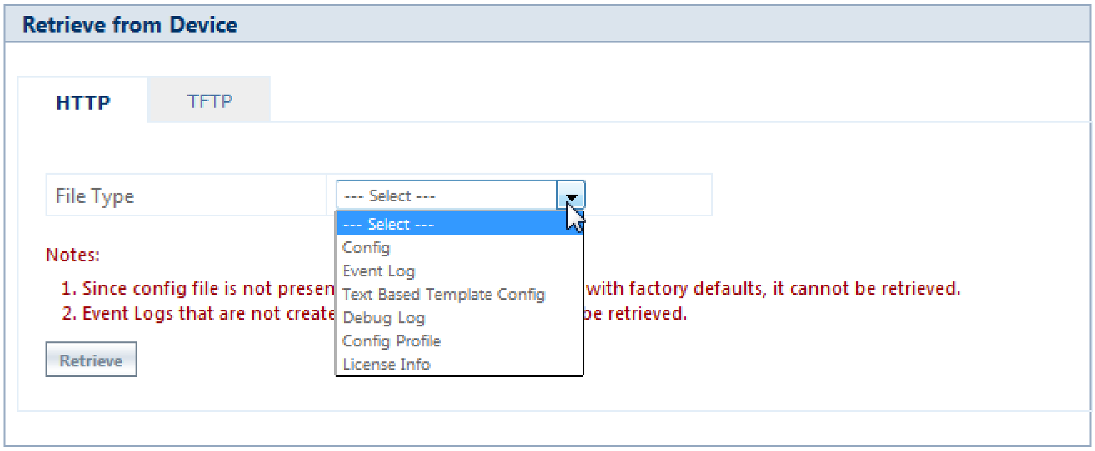
6.2.6 Retrieve From Device

The **Retrieve From Device** tab allows you to retrieve logs, config files, and license info from the device either through HTTP or TFTP.

6.2.6.1 Retrieve from Device via HTTP

To retrieve files from the device by using HTTP, do the following:

1. Navigate to **MANAGEMENT** > **File Management** > **Retrieve from Device > HTTP**.



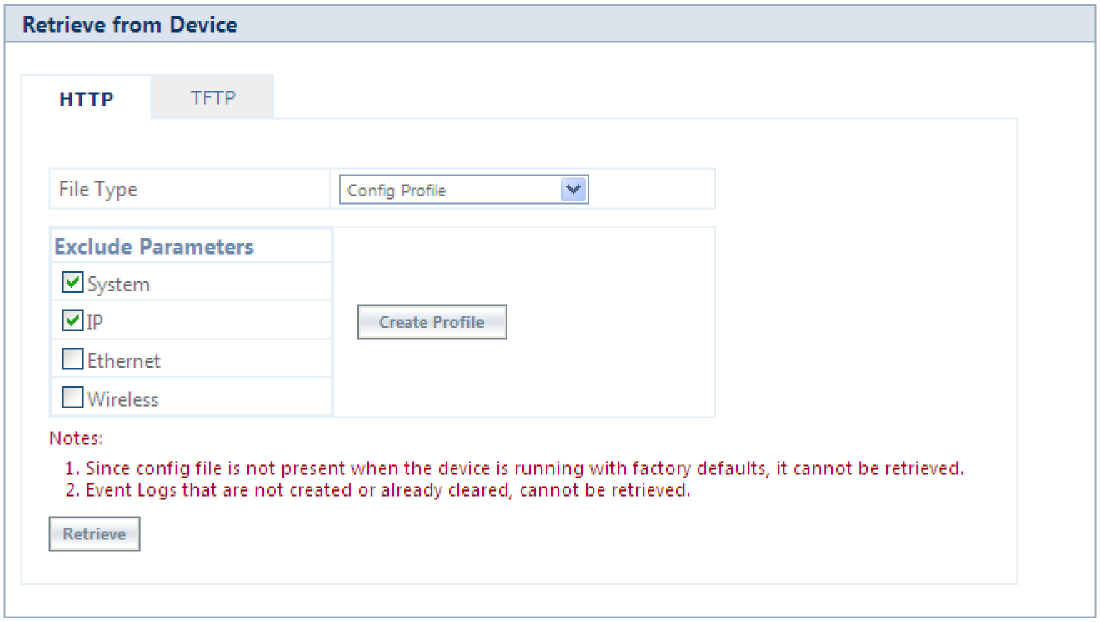
Notes:

1. Since config file is not presen with factory defaults, it cannot be retrieved.
2. Event Logs that are not create be retrieved.

Figure 6-13 Retrieve Files via HTTP

2. Select the type of file that you want to retrieve from the device from the **File Type** drop down box. The files may vary depending on your device. The **File Types** are:
   a. Config
   b. Event Log
   c. Temperature Log
   d. Text Based Template Config
   e. Debug Log
   f. Config Profile
   g. License Info

   The Config Profile is used for replicating the configuration of a master device on to other similar devices by excluding the unique parameters like System information, IP configuration, Ethernet configuration, Wireless configuration based on the selection. By default, System Information and IP Configuration parameters are excluded. On selecting config profile type the following screen appears:



File Type: Config Profile

Exclude Parameters

- ☑ System
- ☑ IP
- □ Ethernet
- □ Wireless

Notes:

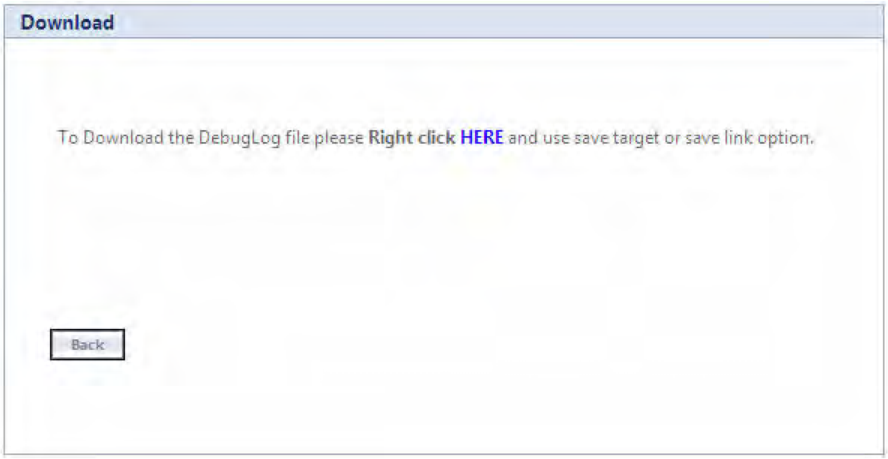
1. Since config file is not present when the device is running with factory defaults, it cannot be retrieved.
2. Event Logs that are not created or already cleared, cannot be retrieved.

Figure 6-14 Retrieve Config Profile File via HTTP

After excluding the unique parameters, click **Create Profile** for creating the profile and then click **Retrieve**. When the retrieved configuration profile file is loaded on target devices, the target devices will come up with configuration of the master device except the excluded parameters. The excluded parameters are retained as configured on the target device.

Config Profile is applicable only to the compatible devices.

3. Click **Retrieve.** Based on the selected file, the following **Download** screen appears.



Download

To Download the DebugLog file please **Right click HERE** and use save target or save link option.

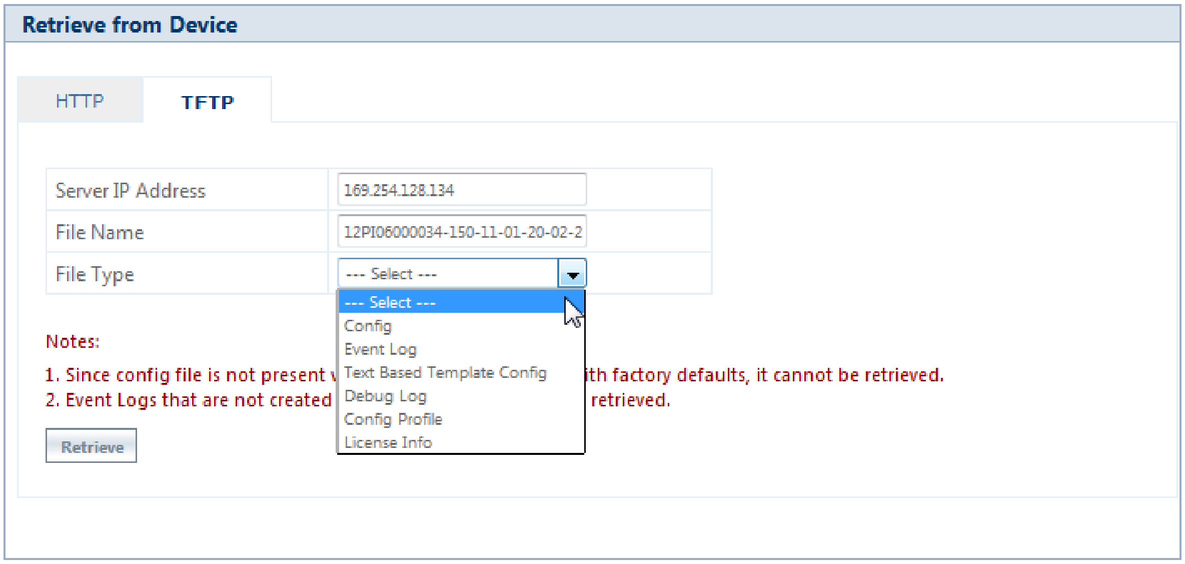
Figure 6-15 Download Screen

4. Right-click the **Download** link and select **Save Target As** or **Save Link As** to save the file to the desired location.

6.2.6.2 TFTP Retrieve

To retrieve files from the device by using TFTP, do the following:

1. Navigate to **MANAGEMENT** > **File Management** > **Retrieve from Device > TFTP**.



Retrieve from Device

Server IP Address	169.254.128.134
File Name	12PI06000034-150-11-01-20-02-2
File Type	--- Select ---

Notes:

1. Since config file is not present v ith factory defaults, it cannot be retrieved.
2. Event Logs that are not created retrieved.

Figure 6-16 Retrieve Files via TFTP

2. Based on the IP mode, configure either IPv4 or IPv6 address as TFTP Server address.
3. Enter the name of the file (including the file extension) that has to be retrieved from the device, in the **File Name** box.
4. Select the file type that you want to retrieve from the device, from the **File Type** drop down box. The file types are:

   a. Config

   b. Event Log

   c. Temperature Log

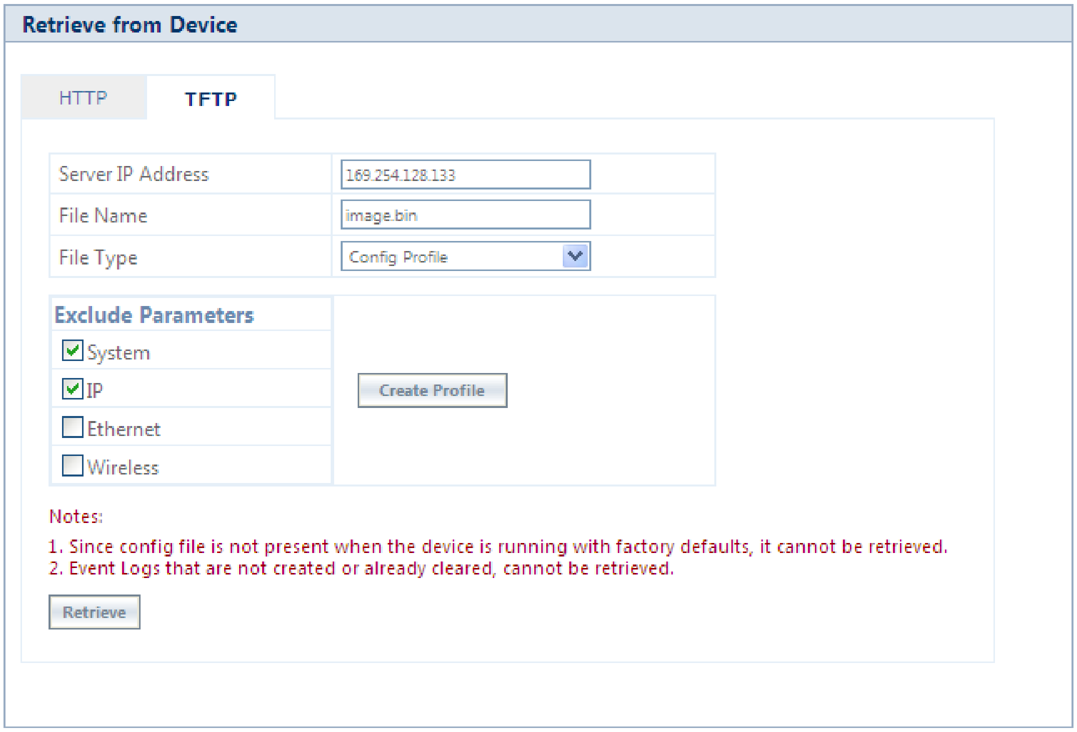
   d. Text Based Template Config

   e. Debug Log

   f. Config Profile

   g. License Info

   The Config Profile is used for replicating the configuration of a master device on to other similar devices by excluding the unique parameters like System information, IP configuration, Ethernet configuration, Wireless configuration based on the selection. By default, System Information and IP Configuration parameters are excluded. On selecting config profile type the following screen appears:



Retrieve from Device

Server IP Address	169.254.128.133
File Name	image.bin
File Type	Config Profile

Exclude Parameters

☑ System

☑ IP

□ Ethernet

□ Wireless

Notes:

1. Since config file is not present when the device is running with factory defaults, it cannot be retrieved.
2. Event Logs that are not created or already cleared, cannot be retrieved.

Figure 6-17 Retrieve Config Profile File via TFTP

After excluding the unique parameters, click **Create Profile** for creating the profile and then click **Retrieve**. When the retrieved configuration profile file is loaded on the target devices, the target devices will come up with configuration of the master device except the excluded parameters. The excluded parameters are retained as configured on the target device.

5. Click **Retrieve.** The retrieved file can be found in the TFTP Server folder.

:

- *Config Profile is applicable only to the compatible devices.*

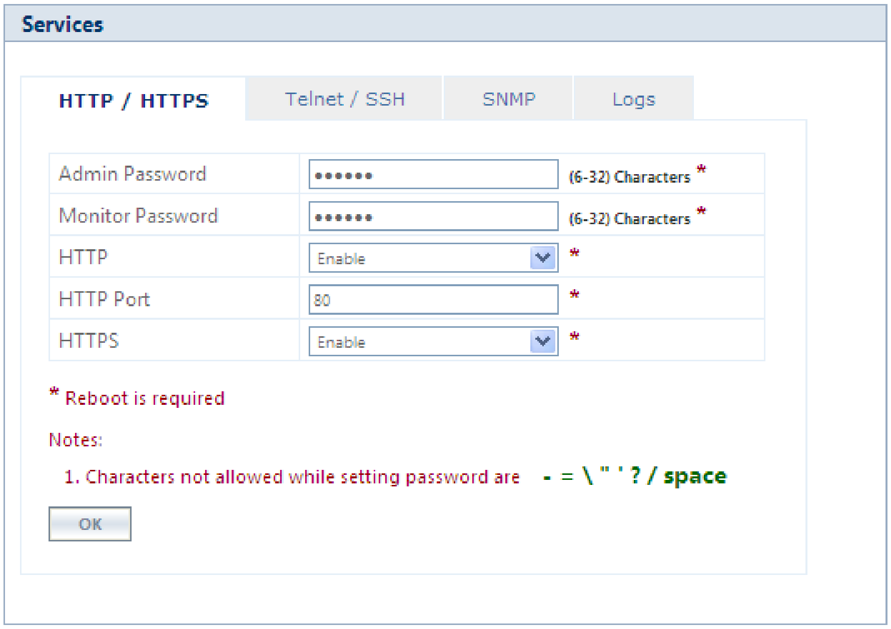
- *When the device is running with default factory settings, there is no Binary Configuration file present and hence it cannot be retrieved.*
- *Similarly, the Text Based Template Configuration file does not exist if it is not generated from the CLI.*
- *You can retrieve Event Logs only when they are generated by the device.*
- *For more information on license upgrade, refer* License Upgrade Procedure *and* Upgrade License *sections.*

6.3 Services

The **Services** tab lets you configure the HTTP/HTTPS, Telnet/SSH and SNMP interface parameters.

6.3.1 HTTP/HTTPS

To configure HTTP/HTTPS interface parameters, navigate to **MANAGEMENT** > **Services > HTTP / HTTPS**.



Admin Password	••••••	(6-32) Characters *
Monitor Password	••••••	(6-32) Characters *
HTTP	Enable	*
HTTP Port	80	*
HTTPS	Enable	*

* Reboot is required

Notes:

1. Characters not allowed while setting password are - = \ " ' ? / space

Figure 6-18 HTTP/HTTPS

Given below is the table which explains HTTP/HTTPS parameters and the method to configure the configurable parameter(s).

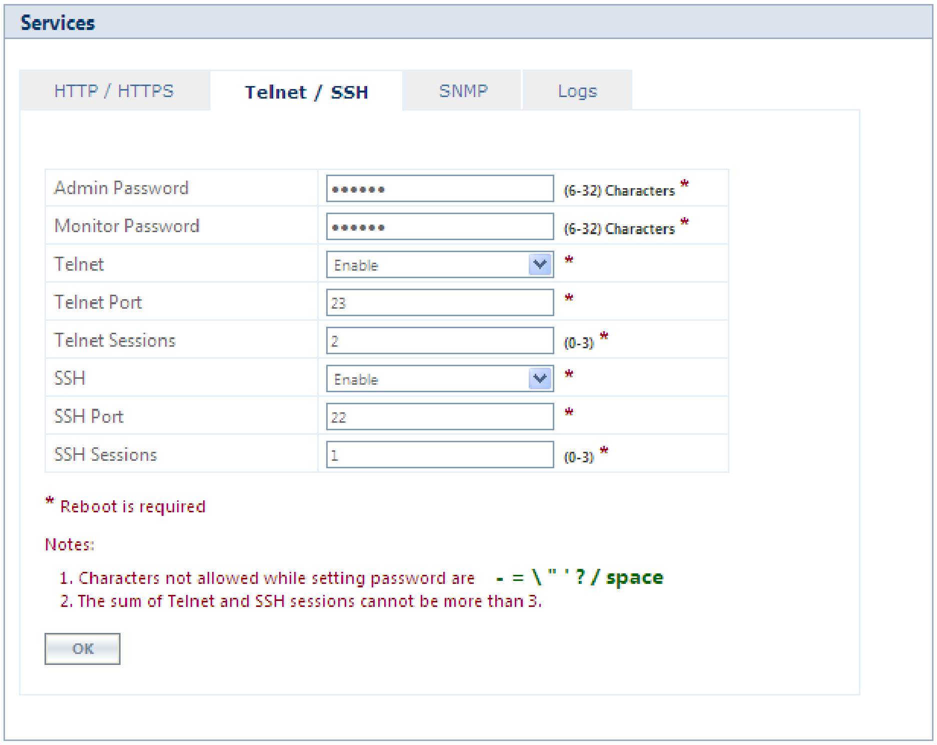
Parameter	Description
Admin Password	By default, the Administrator password to access HTTP/HTTPS interface is **public**. For security reasons, it is recommended to change the default password. The password should be alphanumeric with minimum of 6 and maximum of 32 characters. : *The following special characters are not allowed in the password:* ***- = \ " ' ? / space***

Parameter	Description
Monitor Password	The Administrator user has the privilege to change the Monitor user password. By default, the Monitor user password to access HTTP/HTTPS interface is **public**. For security reasons it is recommended to change the default password. The password should be alphanumeric with minimum of 6 and maximum of 32 characters. *: The following special characters are not allowed in the password:* **- = \ “ ‘ ? / space**
HTTP	By default, a user can manage the device through Web Interface. To prevent access to the device through Web Interface, select **Disable**.
HTTP Port	Represents the HTTP port to manage the device through Web Interface. By default, the HTTP port is **80**.
HTTPS	By default, a user can manage the device through Web Interface over secure socket Layer (HTTPS). To prevent access to the device through HTTPS, select **Disable**. : The password configuration for HTTPS is same as configured for HTTP.

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

6.3.2 Telnet/SSH

To configure Telnet/SSH interface parameters, navigate to **MANAGEMENT** > **Services > Telnet / SSH.**



Admin Password	••••••	(6-32) Characters *
Monitor Password	••••••	(6-32) Characters *
Telnet	Enable	*
Telnet Port	23	*
Telnet Sessions	2	(0-3) *
SSH	Enable	*
SSH Port	22	*
SSH Sessions	1	(0-3) *

* Reboot is required

Notes:

1. Characters not allowed while setting password are **- = \ " ' ? / space**
2. The sum of Telnet and SSH sessions cannot be more than 3.

Figure 6-19 Telnet/SSH

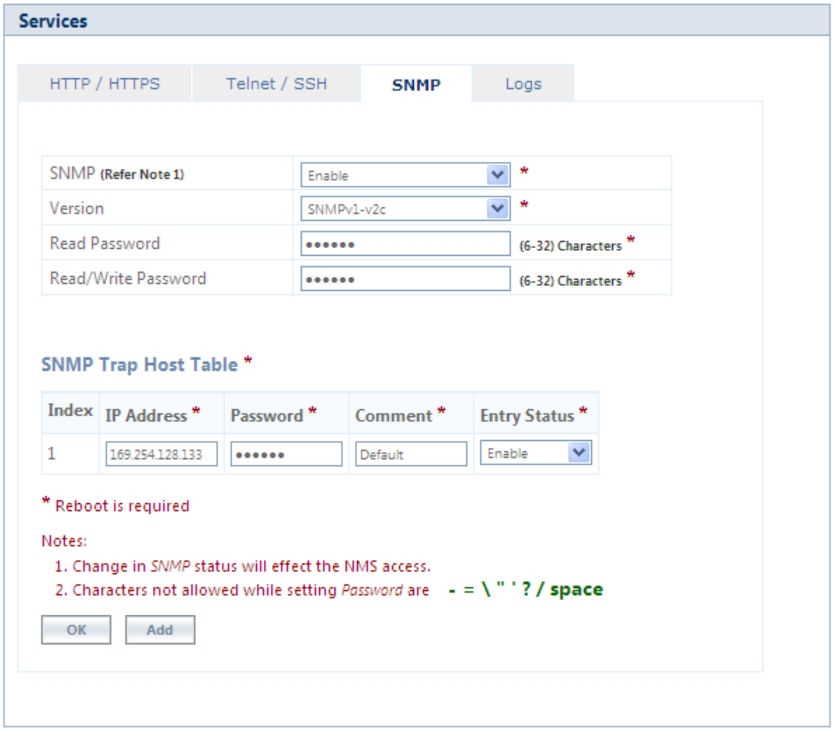
Given below is the table which explains Telnet/SSH parameters and the method to configure the configurable parameter(s):

Parameter	Description
Admin Password	By default, the Administrator password to access Telnet/SSH interface is **public**. For security reasons, it is recommended to change the default password. The password should be alphanumeric with minimum of 6 and maximum of 32 characters. *: The following special characters are not allowed in the password:* ***- = \ “ ‘ ? / space***
Monitor Password	The Administrator user has the privilege to change the Monitor user password. By default, the Monitor user password to access Telnet/SSH interface is **public**. For security reasons it is recommended to change the default password. The password should be alphanumeric with minimum of 6 and maximum of 32 characters. *: The following special characters are not allowed in the password:* **- = \ “ ‘ ? / space**
Telnet	By default, a user can manage the device through Telnet. To prevent access to the device through Telnet, select **Disable**.
Telnet Port	Represents the port to manage the device using Telnet. By default, the Telnet port is **23**.
Telnet Sessions	The number of Telnet sessions which controls the number of active Telnet connections. A user is restricted to configure a maximum of 3 Telnet sessions. By default, the number of Telnet sessions allowed is **2**.
SSH	By default, a user can manage the device through SSH. To prevent access to the device through SSH, select **Disable**.
SSH Port	Represents the port to manage the device using Secure Shell. By default, the Secure Shell port is **22**.
SSH Sessions	Represents the number of SSH sessions which controls the number of active SSH connections. A user is restricted to configure a maximum of 3 SSH sessions. By default, the number of SSH sessions allowed is **1**. *: The total number of CLI sessions allowed is 3, so the sum of Telnet and SSH sessions cannot be more than 3. For example, if you configure the number of Telnet sessions as 2, then the number of SSH sessions can only be a value 0 or 1.*

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

6.3.3 SNMP

To configure SNMP interface parameters, navigate to **MANAGEMENT** > **Services > SNMP.**



SNMP **(Refer Note 1)**	Enable	*
Version	SNMPv1-v2c	*
Read Password	••••••	(6-32) Characters *
Read/Write Password	••••••	(6-32) Characters *

SNMP Trap Host Table *

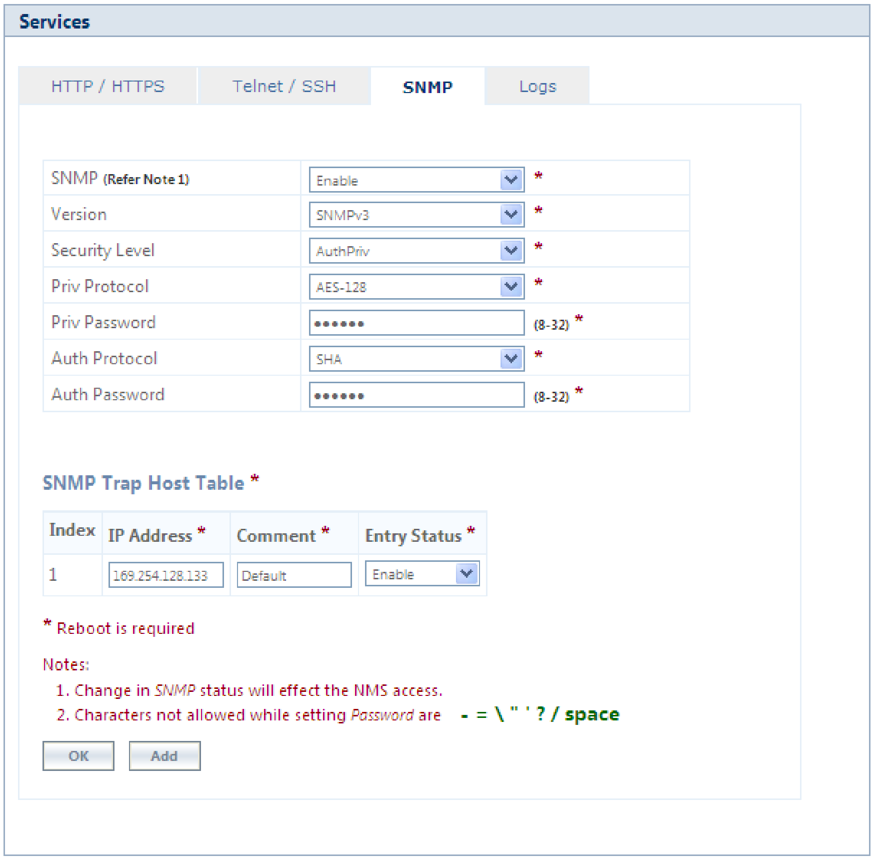
Index	IP Address *	Password *	Comment *	Entry Status *
1	169.254.128.133	••••••	Default	Enable

* Reboot is required

Notes:

1. Change in *SNMP* status will effect the NMS access.
2. Characters not allowed while setting *Password* are **- = \ " ' ? / space**

Figure 6-20 SNMPv1-v2c



SNMP **(Refer Note 1)**	Enable	*
Version	SNMPv3	*
Security Level	AuthPriv	*
Priv Protocol	AES-128	*
Priv Password	••••••	(8-32) *
Auth Protocol	SHA	*
Auth Password	••••••	(8-32) *

SNMP Trap Host Table *

Index	IP Address *	Comment *	Entry Status *
1	169.254.128.133	Default	Enable

* Reboot is required

Notes:

1. Change in *SNMP* status will effect the NMS access.
2. Characters not allowed while setting *Password* are **- = \ " ' ? / space**

Figure 6-21 SNMPv3

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

Parameter	Description
SNMP	By default, the user has the access to manage the device through SNMP Interface. To prevent access to the device through SNMP, select **Disable**. *: Any change in the SNMP status will affect the Network Management System access.*
Version	Allows you to configure the SNMP version. The supported SNMP versions are v1-v2c and v3. By default, the SNMP version is **v1-v2c**.
SNMP v1-v2c Specific Parameters	
Read Password	Represents the read only community string used in SNMP Protocol. It is sent along with each SNMP GET / WALK / GETNEXT / GETBULK request to allow or deny access to the device. This password should be same as read password set in the NMS or MIB browser. The default password is “public”. The password should be of minimum 6 and maximum 32 characters.
	: The following special characters are not allowed in the password: **- = \ “ ‘ ? / space**
Read/Write Password	Represents the read-write community string used in SNMP Protocol. It is sent along with each SNMP GET / WALK / GETNEXT / SET request to allow or deny access to the device. This password should be same as read-write password set in the NMS or MIB browser. The default password is “public”. The password should be of minimum 6 and maximum 32 characters. *: The following special characters are not allowed in the password:* **- = \ “ ‘ ? / space**
SNMP v3 Specific Parameters	
Security level	The supported security levels for the device are **AuthNoPriv** and **AuthPriv**. Select **AuthNoPriv** for Extensible Authentication or **AuthPriv** for both Authentication and Privacy (Encryption).
Priv Protocol	Applicable only when the Security Level is set to **AuthPriv**. Represents the type of privacy (or encryption) protocol. Select the encryption standard as either AES-128 (Advanced Encryption Standard) or DES (Data Encryption Standard). The default Priv Protocol is AES-128. *: The following special characters are not allowed in the password:* **- = \ “ ‘ ? / space**

Parameter	Description
Priv Password	Applicable only when the Security Level is set to **AuthPriv**. Represents the pass key for the selected Privacy protocol. The default password is **public123**. The password should be of minimum 8 and maximum 32 characters. *: The following special characters are not allowed in the password:* **- = \ " ' ? / space**
Auth Protocol	Represents the type of Authentication protocol. Select the encryption standard as either **SHA** (Secure Hash Algorithm) or **MD5** (Message-Digest algorithm). The default Auth Protocol is **SHA**.
Auth Password	Represents the pass key for the selected Authentication protocol. The default password is **public123**. The password should be of minimum 8 and maximum 32 characters.

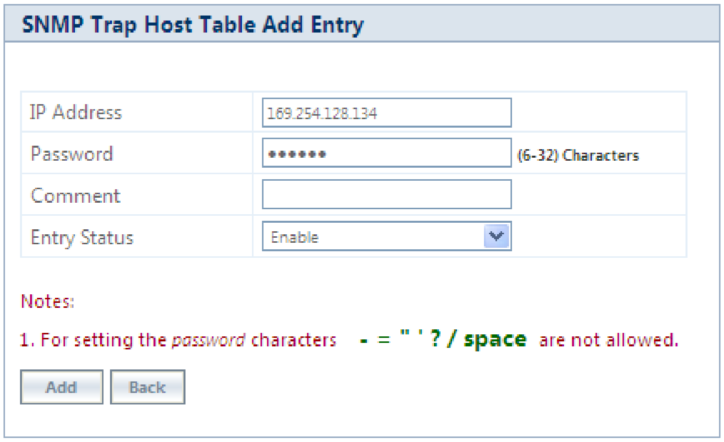
After configuring the required parameters, click **OK**, **COMMIT** and then **REBOOT.**

6.3.3.1 SNMP Trap Host Table

The SNMP Trap Host table allows you to add a maximum of 5 Trap server's IP address to which the SNMP traps will be delivered. By default, the SNMP traps are delivered to 169.254.128.133.

: The default SNMP Trap Host Table entry cannot be deleted.

To add entries to the Trap Host Table, click **Add** in the **Services** screen. The **SNMP Trap Host Table Add Row** screen appears:



SNMP Trap Host Table Add Entry

IP Address	169.254.128.134	
Password	••••••	(6-32) Characters
Comment		
Entry Status	Enable	

Notes:

1. For setting the *password* characters - = " ' ? / space are not allowed.

Figure 6-22 Add Entries to SNMP Host Table

Configure the following parameters:

- **IP Address**: Based on the IP mode, enter the IPv4 or IPv6 address of the Trap server to which SNMP traps will be delivered.

  : IPv6 address should be the global IP address and not the link local IP address.

- **Password**: Type the password to authenticate the Trap Server. The following special characters are not allowed in the password: **- = \ " ' ? /** ***space***

  : Applicable only to SNMP v1-v2c.

- **Comment**: Type comments, if any.
- **Entry Status**: Select the entry status as either Enable or Disable. If enabled, the device will send SNMP traps to the authenticated Trap Server.
- After configuring the required parameters, click **Add** and then **COMMIT**.

6.3.3.2 Edit SNMP Trap Host Table

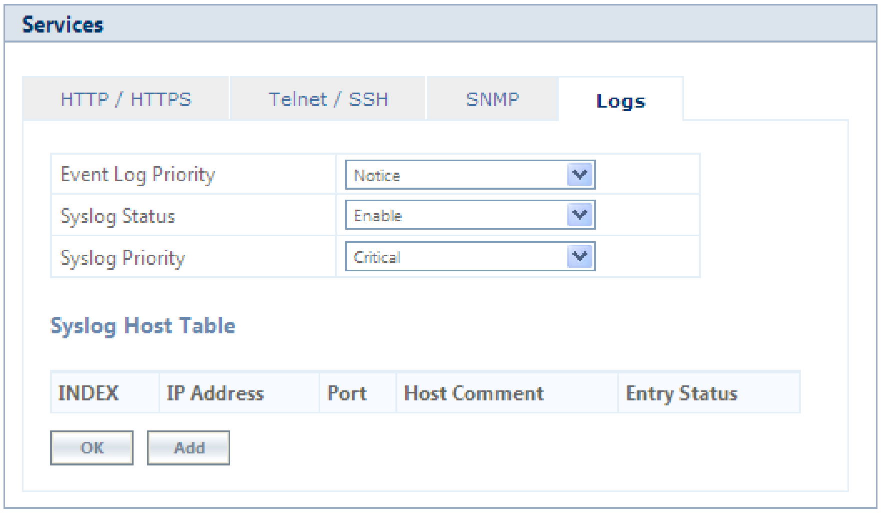
Edit the desired SNMP Trap Host Table entries and click **OK**, **COMMIT** and then **REBOOT**.

6.3.4 Logs

The device supports two types of log mechanisms:

1. **Event Log**: Based on the configured event log priority, all the log messages are logged and used for any analysis. This log messages remain until they are cleared by the user.
2. **Syslog**: They are similar to Event logs except that they are cleared on device reboot.

To configure Event log and Syslog priority, navigate to **MANAGEMENT** > **Services** > **Logs**. The following screen appears:



Event Log Priority	Notice
Syslog Status	Enable
Syslog Priority	Critical

Syslog Host Table

INDEX	IP Address	Port	Host Comment	Entry Status

Figure 6-23 Logs

- **Event Log Priority**: By default, the priority is set to Notice. You can configure the event log priority as one of the following:
  – Emergency
  – Alert
  – Critical
  – Error
  – Warning
  – Notice

  - Info
  - Debug

  Please note that the priorities are listed in the order of their severity, where **Emergency** takes the highest severity and **Debug** the lowest. When the log priority is configured as high, all the logs with low priority are also logged. For example, if **Event Log Priority** is set to **Notice**, then the device will log all logs with priorities Notice, Warning, Error, Critical, Alert and Emergency.

- **Syslog Status**: By default, **Syslog Status** is enabled and default priority is **Critical**. If desired, you can choose to disable.
- **Syslog Priority**: Configuration is same as Event Log Priority.
- After configuring the required parameters, click **OK** and then **COMMIT**.

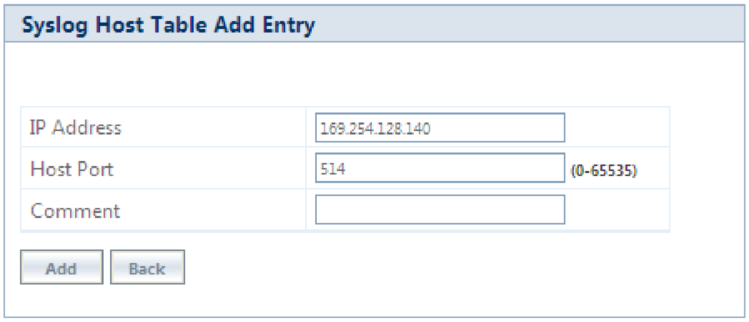
6.3.4.1 Configure a Remote Syslog host

Configure a syslog host (server) in order to forward syslog messages to it.

: You can configure only one syslog host.

Follow the following steps to configure a remote syslog host:

1. Click **Add** in the **Syslog Host Table** screen. The **Syslog Host Table Add Row** screen appears:



Syslog Host Table Add Entry

IP Address	169.254.128.140
Host Port	514 (0-65535)
Comment	

Figure 6-24 Syslog Host Table Add Row

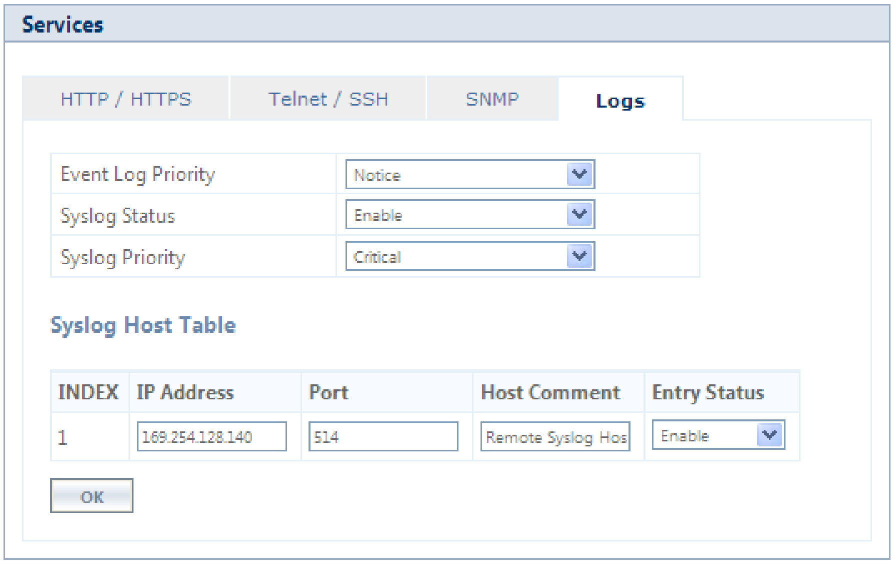
2. **IP Address**: Based on the IP mode, enter IPv4 or IPv6 address of the Syslog host.

   : IPv6 address should be the global IP address and not the link local IP address.

3. **Host Port**: Represents the port on which the Syslog host listens to the log messages sent by the device. The default port is 514.

   : The user must configure the correct port number on which the Syslog host is running. Choice of port number must be in line with the standards for port number assignments defined by Internet Assigned Numbers Authority (IANA).

4. **Comments**: Types comments, if any.
5. Click **Add**. The syslog host is added to the **Syslog Host Table**.



Event Log Priority	Notice
Syslog Status	Enable
Syslog Priority	Critical

Syslog Host Table

INDEX	IP Address	Port	Host Comment	Entry Status
1	169.254.128.140	514	Remote Syslog Hos	Enable

Figure 6-25 Syslog Host Configured

For some reason, if the configured syslog host parameters are changed then you can edit it directly in the **Syslog Host Table** entry. You can change the following parameters:

- **IP Address**
- **Port**
- **Host Comments**
- **Entry Status:**
  - **Enable**: By default, the configured Syslog host is enabled on the device.
  - **Disable**: To disable an entry in the Syslog Host Table, click **Disable**.
  - **Delete**: To delete the configured Syslog host, click **Delete**.

After doing the necessary changes, click **OK** followed by **COMMIT**.

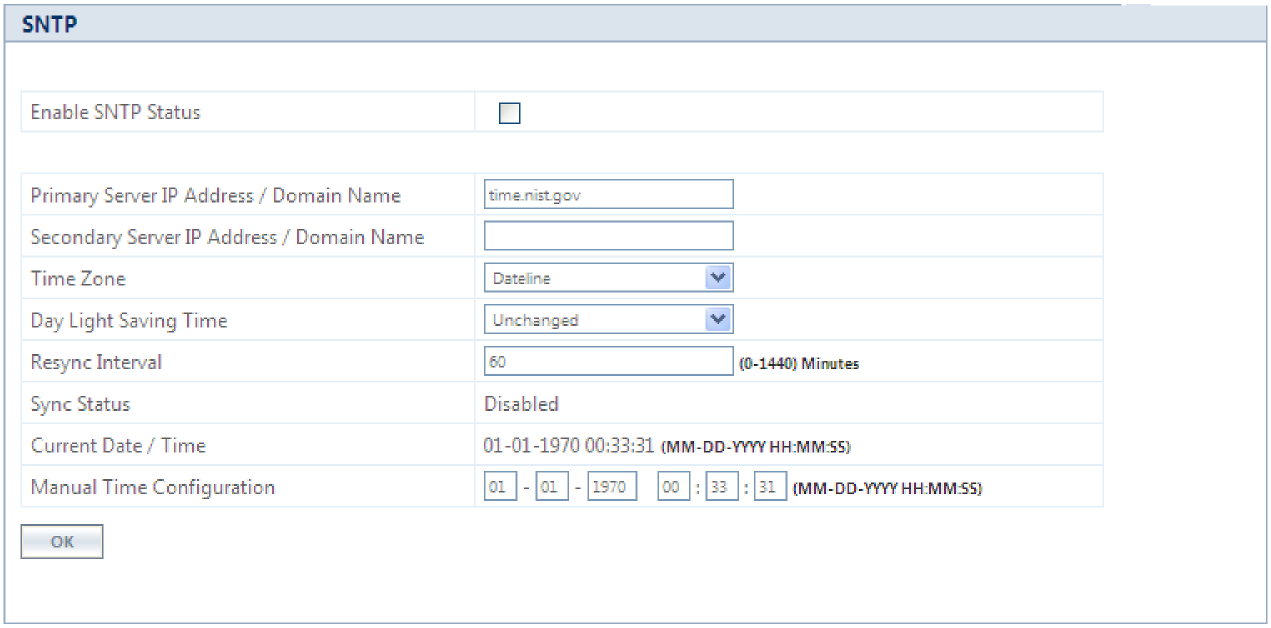
6.4 Simple Network Time Protocol (SNTP)

Proxim's point-to-multipoint and point-to-point devices are furnished with Simple Network Time Protocol (SNTP) Client software that enables to synchronize device's time with the network time servers.

The SNTP Client when enabled on the device(s), sends an NTP (Network Time Protocol) request to the configured time servers. Upon receiving the NTP response, it decodes the response and sets the received date and time on the device after adjusting the time zone and day light saving.

In case, the time servers are not available, then users also have the option to manually set the date and time on the device.

To synchronize device's time with time servers or manually set the time, navigate to **MANAGEMENT > SNTP**. The **SNTP** screen appears:



SNTP

Enable SNTP Status	□
Primary Server IP Address / Domain Name	time.nist.gov
Secondary Server IP Address / Domain Name	
Time Zone	Dateline
Day Light Saving Time	Unchanged
Resync Interval	60 (0-1440) Minutes
Sync Status	Disabled
Current Date / Time	01-01-1970 00:33:31 (MM-DD-YYYY HH:MM:SS)
Manual Time Configuration	01 - 01 - 1970 00 : 33 : 31 (MM-DD-YYYY HH:MM:SS)

Figure 6-26 Time Synchronization

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

Parameter	Description
Enable SNTP Status	Select this parameter to enable SNTP Client on the device. If enabled, the SNTP Client tries to synchronize the device's time with the configured time servers. By default, the SNTP status is disabled.
Primary Server IP Address/Domain Name	Enter the host name, or the IP address based on IP modes (**IPv4 only** or **IPv4 and IPv6**) of the primary SNTP time server. The SNTP Client tries to synchronize device's time with the configured primary server time. : • *If host name is configured, instead of IP address then make sure that DNS server IP is configured on the device.* • *IPv6 address should be the global IP address and not the link local IP address.*
Secondary Server IP Address/Domain Name	Enter the host name, or the IP address based on IP modes (**IPv4 only** or **IPv4 and IPv6**) of the secondary SNTP time server. If the primary server is not reachable, then SNTP client tries to synchronize device's time with the secondary server time. : • *If the SNTP client is not able to sychronize the time with both the servers (primary and secondary), then it tries to synchronize again after every one minute.* • *IPv6 address should be the global IP address and not the link local IP address.*

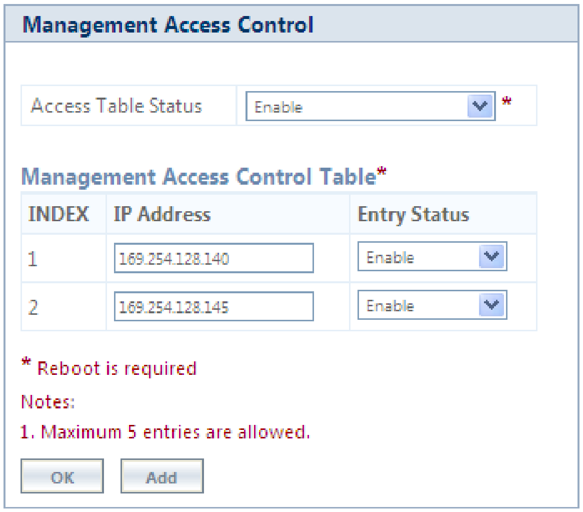
Parameter	Description
Time Zone	Configure the time zone from the available list. This configured time zone is considered before setting the time, received from the time servers, on the device.
Day Light Saving Time	Configure the Day Light Saving time from the available list. This configured Day Light Saving time is considered before setting the time, received from the time servers, on the device.
ReSync Interval	Set ReSync time interval ranging from **0 to 1440** minutes. Once the time is synchronized, the SNTP Client tries to resynchronize with the time servers after every set time interval. By default, the ReSync interval is set to **60** minutes.
Sync Status	Specifies the SNTP Client sync status when it tries to ReSync again with the time servers. The status is as follows: • **Disabled**: The SNTP client will not synchronize the time with the time servers and displays the status as Disabled. • **Synchronizing**: The SNTP client is in the process of synchronzing time with the time servers. • **Synchronized**: The SNTP client has synchronized time with the time servers.
Current Date/Time	Displays the current date and time. If SNTP is enabled, it displays the time the device received from the SNTP server. If SNTP is not enabled, then it displays the time manually set by the user.
Manual Time Configuration	If SNTP Client is disabled on the device or the time servers are not available on the network, then the user can manually set the time. Enter the time manually in the format: MM-DD-YYYY HH:MM:SS. : • *Manual time configuration is not retained across reboots. After every reboot the user has to set the time again.* • *Over a period of time, with manual time configuration, the device may lag behind the actual time. So, it is recommended to periodically check and adjust the time.*

To save the configured parameters, click **OK** and then **COMMIT**.

6.5 Access Control

The **Access Control** tab enables you to control the device management access through specified host(s). You can specify a maximum of five hosts to control device management access.

To configure management access control parameters, navigate to **MANAGEMENT > Access Control**. The **Management Access Control** screen appears:



Management Access Control

Access Table Status	Enable *

Management Access Control Table*

INDEX	IP Address	Entry Status
1	169.254.128.140	Enable
2	169.254.128.145	Enable

* Reboot is required

Notes:

1. Maximum 5 entries are allowed.

Figure 6-27 Management Access Control

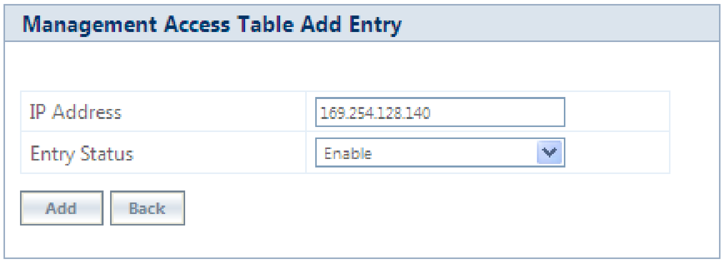
By default, the Management Access Control feature is disabled on the device. To enable, select **Enable** from the **Access Table Status** box and click **OK**. Reboot the device, for the changes to take effect.

: Only when the Access Table Status is enabled, you can add host(s) to the Management Access Control Table.

6.5.0.1 Add Host(s) to Management Access Control Table

To add a host to the Management Access Control Table, do the following:

1. Click **Add** in the **Management Access Control** screen. The **Management Access Table Add Row** screen appears:



Management Access Table Add Entry

IP Address	169.254.128.140
Entry Status	Enable

Figure 6-28 Management Access Table Add Row

2. **IP Address**: Based on the IP mode, configure either IPv4 or IPv6 address of the host that controls the device management access.
3. **Entry Status**: By default, the entry status is enabled meaning which the specified host can control the device management access. Edit the status to **Disable**, if you do not want the host to control the device management access.
4. Click **Add**.

: If MAC ACL is enabled, configure at least one entry in the Management Access Table with the IP address (of the PC or the management station), in order to manage the device.

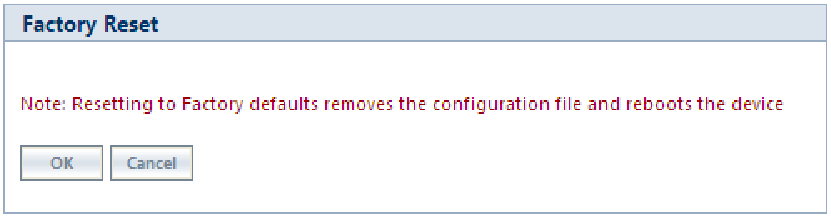
6.5.0.2 Edit Management Access Control Table Entries

Edit the desired host entries and click **OK, COMMIT** and then **REBOOT**.

6.6 Reset to Factory

The **Reset to Factory** tab allows you to reset the device to its factory default state. When this operation is performed, the device will reboot automatically and comes up with default configurations.

To reset the device to its factory defaults, navigate to **MANAGEMENT** > **Reset To Factory**. The Factory Reset screen appears:


Factory Reset

Note: Resetting to Factory defaults removes the configuration file and reboots the device

Figure 6-29 Reset to Factory Defaults

Click **OK**, if you wish to proceed with factory reset, else click **Cancel**.

6.7 Convert QB to MP

The **Convert QB to MP** tab lets you convert a QB to SU so that the converted device can connect to a BSU and operate as a SU.

This feature is applicable only to,

- QB-8200-EPA-G/QB-8200-EPA which converts to a MP-8200-SUA
- QB-8250-EPR-G/QB-8250-EPR which converts to a MP-8250-SUR

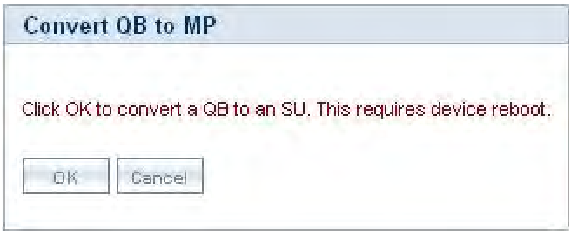
You can convert a QB to SU mode by using two methods:

- **Method 1**: Web Interface
- **Method 2**: Load an SU config file (retrieved from another SU) onto the QB device and then reboot.

: *Even after conversion from QB to MP, the device description still shows as QB.*

To convert a QB to SU using Web Interface, do the following:

1. Navigate to **MANAGEMENT** > **Convert QB to MP**. The **Convert QB to MP** screen appears:


Convert QB to MP

Click OK to convert a QB to an SU. This requires device reboot.

Figure 6-30 Convert QB to MP

2. Click **OK**.

:

- *A QB after converting to SU will function in SU mode only. It will accept only MP firmware for upgrade.*

- *The version of the firmware being upgraded to should be 2.4.0 or later. If earlier version of the firmware is loaded, the device will reset to factory default upon initialization and operate in QB mode.*
- *When upgrading a converted device from Bootloader, it must be done using a QB image, as the device is licensed as QB.*
- *The conversion of the device from QB to SU requires a reboot.*
- *In case of Method 1 (Web Interface) conversion, QB mode configuration will be deleted.*
- *Reset to factory defaults, always results in the device initializing in QB mode.*

6.8 Auto Config Recovery

This feature enables a QB device to fall back to the last successful link configuration when it fails to establish connection with its peer.

:

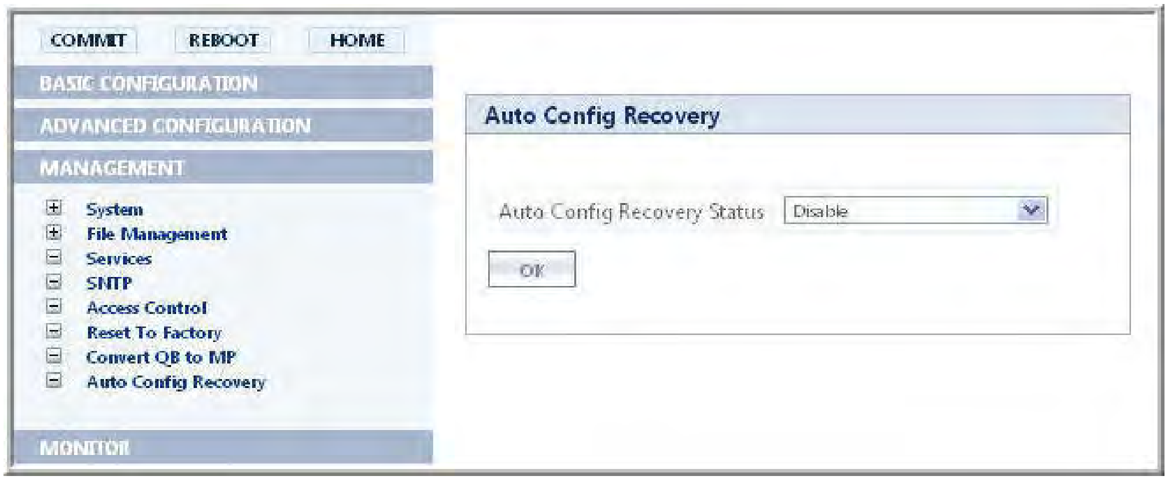
- *It is applicable only to QB-825-EPR/LNK-50$^+$, QB-825-EPR/LNK-100, QB-835-EPR/LNK-25, QB-835-EPR/LNK-50 and QB-82xx Series.*
- *By default, it is disabled on End Point A and enabled on End Point B.*
- *It is started either during device initialization or on COMMIT success.*

The detailed explanation of the feature is given below:

- On successful COMMIT/ device initialization, the WORP link status is checked after the Auto Config Recovery Delay time expires. If the WORP link is established, then the device saves the current configuration as the last successful link configuration.
- If the WORP link is not established, the device will fall back to the last successful link configuration (only if available) and reboot.
- If the WORP link is still not established after the auto config recovery delay time expires, the device will fall back to auto config recovery defaults. The **Auto Config Recovery Defaults** vary from the **Factory Reset Defaults** by the following four parameters:

Parameter	Description
Network Name	Represents the current network name of the device.
Auto Config Recovery Feature Status	This parameter is Enabled.
IP Address	For End Point B (EPB), the IP address is 169.254.128.131.
Radio Mode	For End Point B (EPB), this parameter will come up as EPB only on fallback to auto config recovery defaults

- To enable this feature on End Point A/ B, navigate to Management> Auto Config Recovery. In the following screen, **Enable** the **Auto Config Recovery Status** using the drop-down menu and click **OK**.



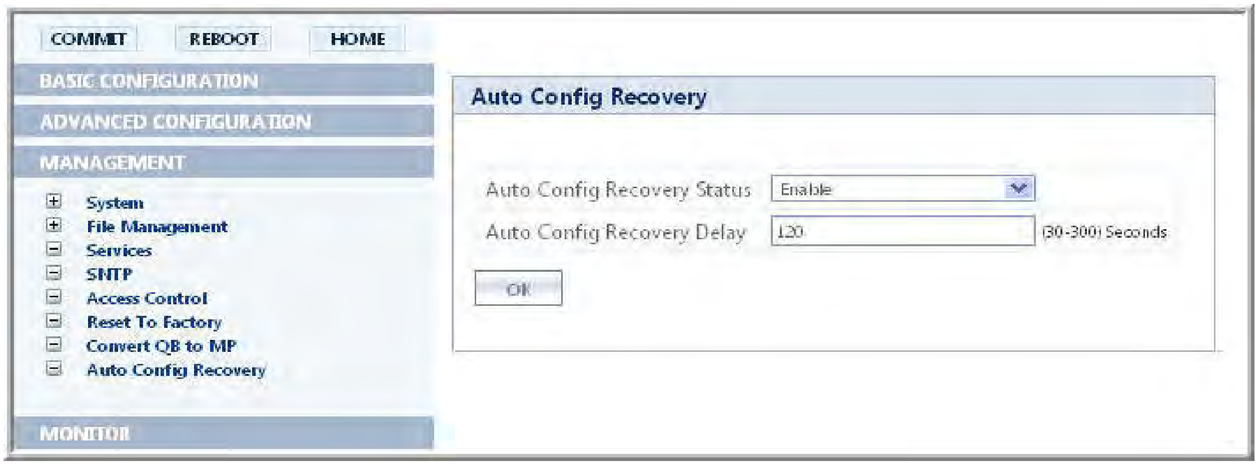
Auto Config Recovery

Auto Config Recovery Status: Disable

Figure 6-31 Auto Config Recovery

- Next, enter the **Auto Config Recovery Delay** as shown in the following screen. By default, it is set to **120** seconds, but the configurable value ranges from **30** – **300** seconds.

: *If ACS is enabled, irrespective of the auto config recovery delay configured time, an extra 3 Minutes is added to the delay.*



Auto Config Recovery

Auto Config Recovery Status: Enable

Auto Config Recovery Delay: 120 (30-300) Seconds

Figure 6-32 Auto Config Recovery

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

:

- *If the 'Recovery delay time' expires during the 'firmware upgrade', then the 'Auto Config Recovery' functionality is not triggered.*
- *During the primary testing/ deployment, it is recommended to **Disable** this feature at both ends of the link and **Enable** it after the successful establishment of WORP link.*
- *This feature does not impact the last known good configuration which is used in case of configuration corruption.*
- *If the configured channel is 'DFS channel', then 'Recovery Delay' starts after the 'CACT 'process is completed.*

Monitor 7

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

- System
- Interface Statistics
- WORP Statistics
- Active VLAN
- Bridge
- Network Layer
- RADIUS (BSU or End Point A only)
- IGMP
- DHCP
- Logs
- Tools
- SNMP v3 Statistics

7.1 System

*: 'System' section is applicable only to **82x devices**.*

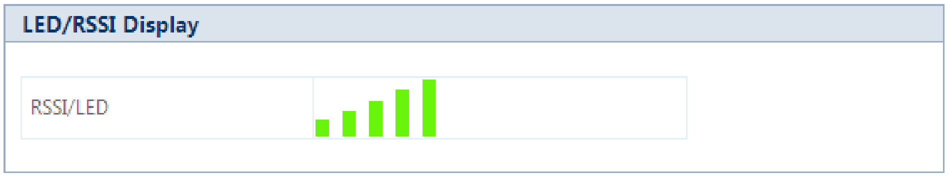
For 82x devices, the System tab enables you to view system specific information namely **LED/RSSI Display** when **Sync/RSSI** is enabled in **LED Display Status**. To configure the LED Display Status, navigate to **Advanced Configuration > System** and select any one of the configurable values: **Disable**, **RSSI**, and **Sync**. Refer, LED Status for more details.

7.1.1 RSSI LED Behavior

When the link is established, the Received Signal Strength Indicator (RSSI) LEDs on the scaling mask glow. Scaling mask LEDs indicate the received signal strength of the link. The more LEDs on the scaling mask glow, better is the signal. By default, **RSSI Display** mode is enabled, if required the user can select the Disable (LEDs Off) mode. In **Disable (LEDs Off)** mode, all the 5 LEDs will be off.

*: 'RSSI LED' feature is applicable only to **82x** devices.*

To view RSSI, navigate to **MONITOR > System**. The **LED/RSSI Display** screen appears as shown below.



LED/RSSI Display

RSSI/LED

Figure 7-1 LED/RSSI Display (RSSI)

– The LED behavior in **RSSI Display mode** is given below:
  - By default all the 5 LEDs will blink for an interval of 1 second to indicate the device is UP.
  - 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.
  - For a SU, if the SU is registered with the BSU, then the LEDs will glow based on the RSSI value else all the 5 LEDs will blink.
  - For a CPE, if the CPE is registered with the BSU, then the LEDs will glow based on the RSSI value else all the 5 LEDs will blink.
  - For QB, if EndPointA is registered with EndPointB, then the LEDs will glow based on the RSSI value of each EndPoint. else all the 5 LEDs will blink.

7.1.2 Sync LED Behavior

If Sync mode is enabled, the third LED behavior of the scaling mask will indicate the Sync status.

To view the Sync status, navigate to **Monitor** > **System.** The **LED/RSSI Display** screen appears as shown below.

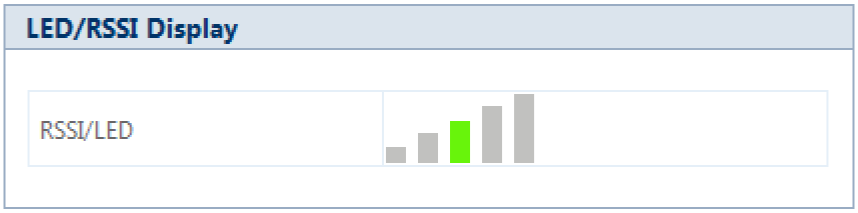


Figure 7-2 LED/RSSI Display (Sync)

– The LED behavior in **Sync mode** is described and tabulated below.

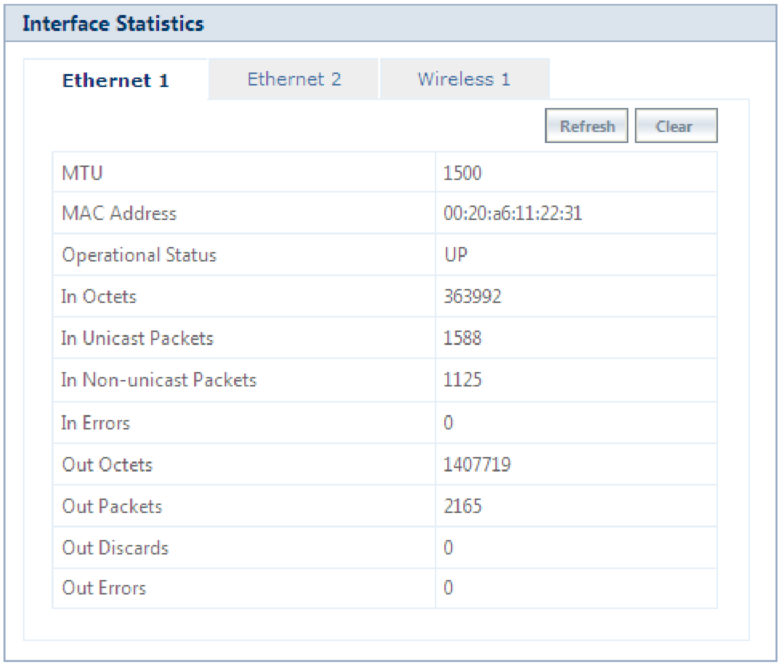
Sync LED Behavior	Sync Status
OFF (Grey)	Synchronous mode is disabled or the device is out of Sync
Blinking (Green-Fast)	Synchronous mode is enabled, but Sync signal is not received
ON (Solid-Green)	Synchronous mode is enabled and Sync signal is received

7.2 Interface Statistics

Interface Statistics allows you to monitor the status and performance of the Ethernet and Wireless interfaces of the device.

7.2.1 Ethernet Statistics

To view the Ethernet interface statistics, click **MONITOR > Interface Statistics**. The **Interface Statistics** screen appears:



MTU	1500
MAC Address	00:20:a6:11:22:31
Operational Status	UP
In Octets	363992
In Unicast Packets	1588
In Non-unicast Packets	1125
In Errors	0
Out Octets	1407719
Out Packets	2165
Out Discards	0
Out Errors	0

Figure 7-3 Ethernet Interface Statistics

To view Ethernet statistics, click **Ethernet 1** or **Ethernet 2** depending on the Ethernet interfaces supported by your device.

Given below is the table which explains the parameters displayed in the Ethernet Statistics screen:

Parameter	Description
MTU	Specifies the largest size of the data packet received or sent on the Ethernet interface. The MTU size varies from 1500 to 1514 depending on the MTU configuration (See System).
MAC Address	Specifies the MAC address at the Ethernet protocol layer.
Operational Status	Specifies the current operational state of the Ethernet interface.
In Octets	Specifies the total number of octets received on the Ethernet interface.
In Unicast Packets	Specifies the number of subnetwork- unicast packets delivered to the higher level protocol.
In Non-unicast Packets	Specifies the number of non-unicast subnetwork packets delivered to the higher level protocol.
In Errors	Specifies the number of inbound packets that contained errors and are restricted from being delivered.
Out Octets	Specifies the total number of octets transmitted out from the Ethernet interface.
Out Packets	Specifies the total number of packets requested by the higher level protocol and then, transmitted.
Out Discards	Specifies the number of error-free outbound packets chosen to be discarded to prevent them from being transmitted. One possible reason for discarding such a packet could be to free up buffer space.

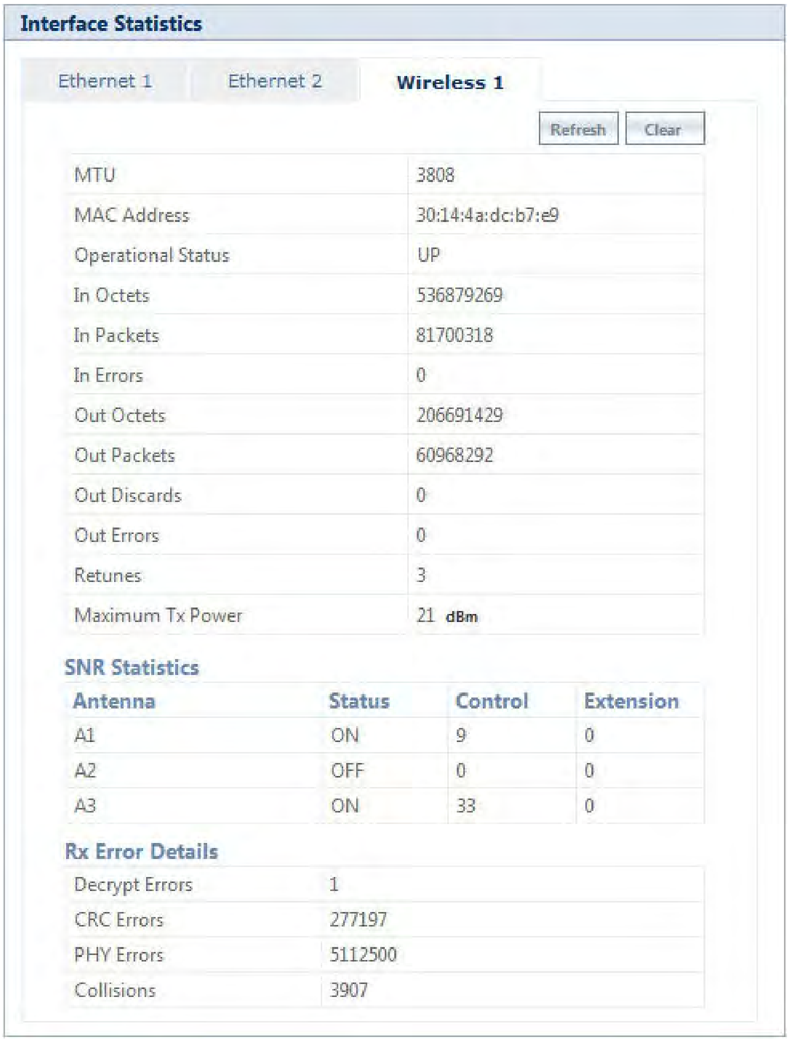
Parameter	Description
Out Errors	Specifies the number of outbound packets that are not transmitted because of errors.

To view the updated Ethernet statistics, click **Refresh**.

To delete the Ethernet statistics, click **Clear**.

7.2.2 Wireless Statistics

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



MTU	3808
MAC Address	30:14:4a:dc:b7:e9
Operational Status	UP
In Octets	536879269
In Packets	81700318
In Errors	0
Out Octets	206691429
Out Packets	60968292
Out Discards	0
Out Errors	0
Retunes	3
Maximum Tx Power	21 dBm

SNR Statistics

Antenna	Status	Control	Extension
A1	ON	9	0
A2	OFF	0	0
A3	ON	33	0

Rx Error Details

Decrypt Errors	1
CRC Errors	277197
PHY Errors	5112500
Collisions	3907

Figure 7-4 Wireless Interface Statistics

Given below is the table which explains the parameters displayed in the Wireless statistics screen:

Parameter	Description
MTU	Specifies the largest size of the data packet received or sent on the wireless interface. 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.
MAC Address	Specifies the MAC address at the wireless protocol layer.
Operational Status	Specifies the current operational state of the wireless interface.
In Octets	Specifies the total number of octets received on the wireless interface.
In Packets	Specifies the number of packets delivered to the higher level protocol.
In Errors	Specifies the number of inbound packets that contained errors and are restricted from being delivered.
Out Octets	Specifies the total number of octets transmitted out from the wireless interface.
Out Packets	Specifies the total number of packets requested by the higher level protocol and then, transmitted.
Out Discards	Specifies the number of error-free outbound packets chosen to be discarded to prevent them from being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Out Errors	Specifies the number of outbound packets that are not transmitted because of errors.
Retunes	Specifies the number of times the radio is re-tuned for better performance of the device.
Max Tx Power	Indicates the maximum power that the radio can radiate.
SNR Statistics SNR Statistics represents the signal strength with regard to the noise at the antenna ports.	
Antenna	Specifies the antenna ports available for the product. Please note that the antenna ports vary depending on the product.
Status	Specifies the configuration status of the antenna ports. **ON** indicates that antenna port is enabled and **OFF** indicates that antenna port is disabled.
Control	Specifies the SNR value of the packet received at the selected channel frequency.
Extension	This parameter is applicable only to the 40 MHz modes, that is, 40 PLUS and 40 Minus. It specifies the SNR value of the packet received on the extension channel (20MHz).
Rx Error Details	
Decrypt Errors	This parameter is applicable only if security is enabled. It indicates the number of received packets that failed to decrypt.
CRC Errors	Specifies the number of received packets with invalid CRC.
PHY Errors	Specifies the total Rx PHY Errors. It generally indicates the interference in the wireless medium.
Collisions	Specifies the total numbers of collisions occurred.

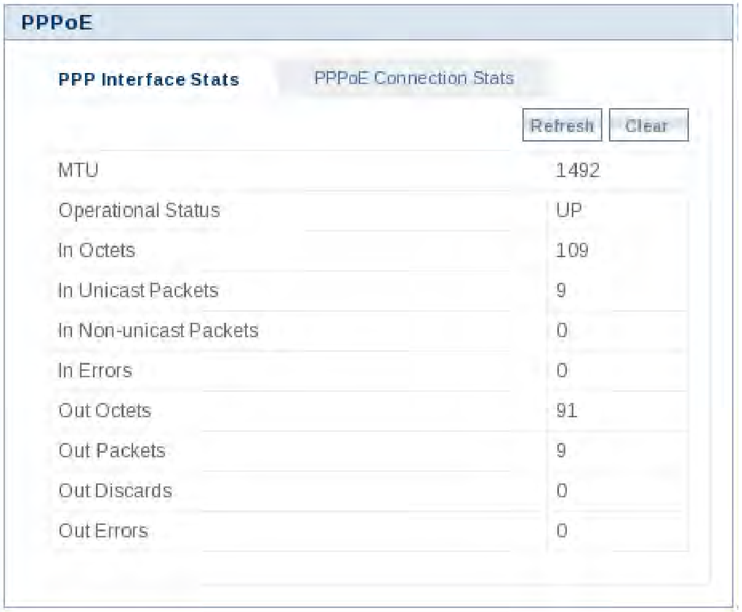
To view the updated Wireless statistics, click **Refresh**.

To delete the Wireless statistics, click **Clear**.

7.2.3 PPPoE Statistics

: Applicable only to an SU in Routing mode.

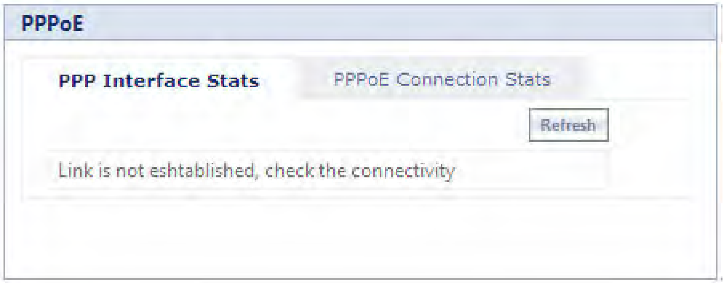
To view PPPoE interface statistics, navigate to **MONITOR** > **Interface Statistics > PPPoE > PPP Interface Stats**.



MTU	1492
Operational Status	UP
In Octets	109
In Unicast Packets	9
In Non-unicast Packets	0
In Errors	0
Out Octets	91
Out Packets	9
Out Discards	0
Out Errors	0

Figure 7-5 PPPoE Interface Statistics

The PPPoE interface parameters are same as the Ethernet interface parameters. Please note that if a link is not established between a PPPoE client and server, then the device displays the following message.

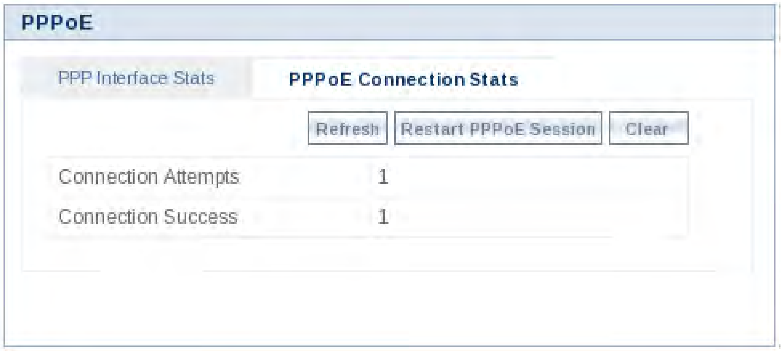


Link is not eshtablished, check the connectivity

Figure 7-6 PPPoE Server - No Link Established

To view the updated PPPoE interface statistics, click **Refresh**. Please note that for every 4 seconds, the interface statistics gets refreshed.

To view the PPPoE connection status such as the number of attempts made to start a session between PPPoE client and server, and the number of attempts failed to establish a connection, click **PPPoE Connection Stats**.



Connection Attempts	1
Connection Success	1

Figure 7-7 PPPoE Connection Statistics

To view updated connection statistics, click **Refresh**.

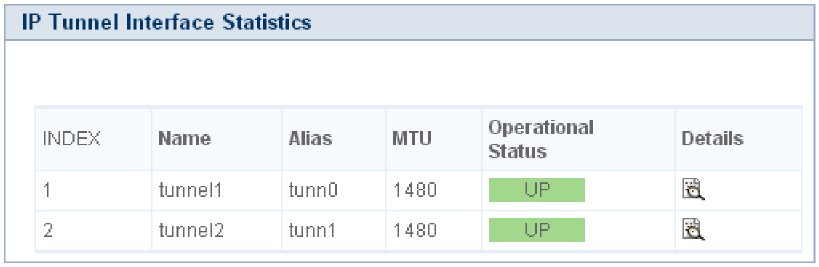
To restart the session between the PPPoE client and server, click **Restart PPPoE Session**. On successfully re-establishing a session, the IP address of the wireless interface will be assigned again by the PPPoE server, if Address Type is set to PPPoE-ipcp.

To clear the existing connection statistics, click **Clear**.

7.2.4 IP Tunnels

: Applicable only in Routing Mode.

To view IP Tunnels interface statistics, click **MONITOR** > **Interface Statistics > IP Tunnels**. The following **IP Tunnel Interface Statistics** screen appears:

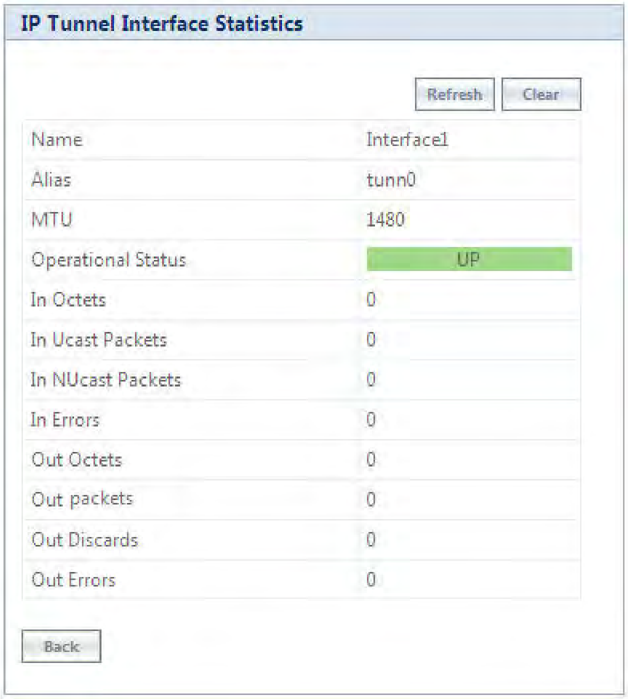


INDEX	Name	Alias	MTU	Operational Status	Details
1	tunnel1	tunn0	1480	UP	
2	tunnel2	tunn1	1480	UP	

Figure 7-8 IP Tunnels Interface Statistics

Given below is an explanation to each of these parameters:

Parameter	Description
Name	Specifies the tunnel interface name.
Alias	Specifies the supplementary tunnel interface name.
Maximum Transmission Unit (MTU)	Specifies the largest size packet or frame that can be sent over the tunnel interface. The MTU of the tunnel interface is derived from the underlying interface: **For IP-IP tunnel interface**: MTU = Underlying interface MTU – 20 bytes (IP header) **For IP-GRE interface**: MTU = Underlying interface MTU – 24 bytes (IP header + gre protocol)

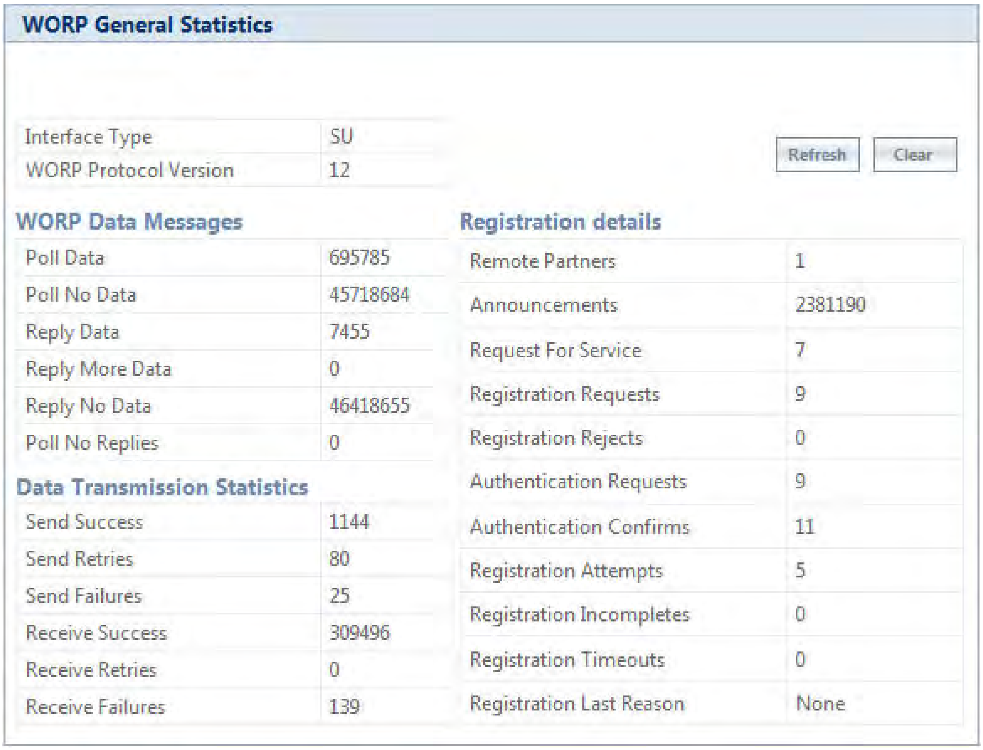
Parameter	Description
Operational Status	The Operational Status indicates only the tunnel interface status. The status can be either UP or DOWN. *: For the tunnel to function correctly both ends should be configured correctly.*
Details	Provides a more detailed statistics about the tunnel interface. To view the detailed statistics, click 🔍.  **IP Tunnel Interface Statistics** Name: Interface1 Alias: tunn0 MTU: 1480 Operational Status: UP In Octets: 0 In Ucast Packets: 0 In NUcast Packets: 0 In Errors: 0 Out Octets: 0 Out packets: 0 Out Discards: 0 Out Errors: 0 **Figure 7-9 Detailed IP Tunnels Interface Statistics** The detailed tunnel interface parameters are similar to the Ethernet Interface Statistics. Please refer to Ethernet Statistics.

7.3 WORP Statistics

7.3.1 General Statistics

WORP General Statistics provides general statistics about the WORP.

To view General Statistics, navigate to **MONITOR > WORP Statistics > Interface 1 > General Statistics**. The following **WORP General Statistics** screen appears.



WORP General Statistics

Interface Type	SU
WORP Protocol Version	12

WORP Data Messages

Poll Data	695785
Poll No Data	45718684
Reply Data	7455
Reply More Data	0
Reply No Data	46418655
Poll No Replies	0

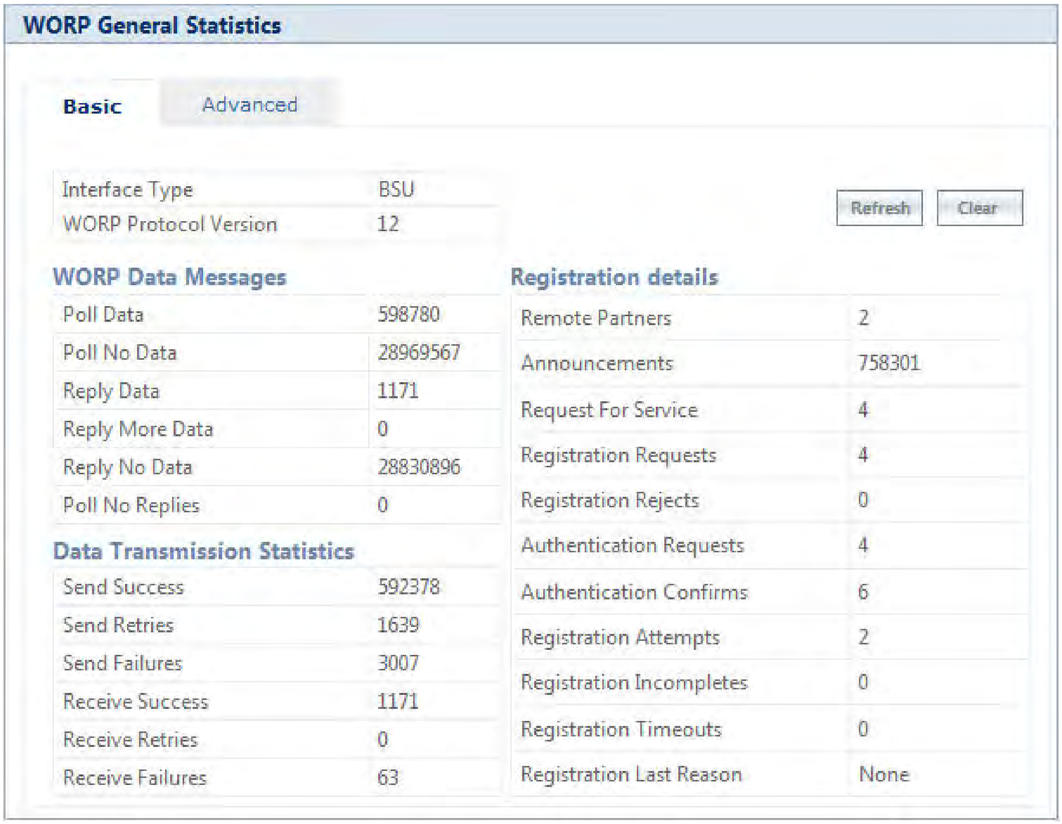
Data Transmission Statistics

Send Success	1144
Send Retries	80
Send Failures	25
Receive Success	309496
Receive Retries	0
Receive Failures	139

Registration details

Remote Partners	1
Announcements	2381190
Request For Service	7
Registration Requests	9
Registration Rejects	0
Authentication Requests	9
Authentication Confirms	11
Registration Attempts	5
Registration Incompletes	0
Registration Timeouts	0
Registration Last Reason	None

Figure 7-10 WORP General Statistics (SU/End Point A/End Point B)



WORP General Statistics

Interface Type	BSU
WORP Protocol Version	12

WORP Data Messages

Poll Data	598780
Poll No Data	28969567
Reply Data	1171
Reply More Data	0
Reply No Data	28830896
Poll No Replies	0

Data Transmission Statistics

Send Success	592378
Send Retries	1639
Send Failures	3007
Receive Success	1171
Receive Retries	0
Receive Failures	63

Registration details

Remote Partners	2
Announcements	758301
Request For Service	4
Registration Requests	4
Registration Rejects	0
Authentication Requests	4
Authentication Confirms	6
Registration Attempts	2
Registration Incompletes	0
Registration Timeouts	0
Registration Last Reason	None

Figure 7-11 WORP General Statistics (BSU)

7.3.1.1 Basic Statistics

Given below is an explanation to the basic parameters:

Parameter	Description
Interface Type	Specifies the type of radio interface.
WORP Protocol Version	Specifies the version of the WORP Protocol used. This information is useful to the customer support team for debugging purpose only.
WORP Data Messages Specifies the sent or received data frames through wireless interface.	
Poll Data	Refers to the number of polls with data messages sent or received.
Poll No Data	Refers to the number of polls with no data messages sent or received.
Reply Data	Refers to the number of poll replies with data messages sent or received.
Reply More Data	Refers to the number of poll replies with more data messages sent or received.
Reply No Data	Refers to the number of poll replies with no data messages sent or received.
Poll No Replies	Refers to the number of times the poll messages are sent by a BSU/End Point A and received no reply from SU/End Point B. This parameter is applicable only to a BSU.
Data Transmission Statistics Specifies the number of transmissions occurred through the interface.	
Send Success	Refers to the number of data messages sent and acknowledged by the peer successfully.
Send Retries	Refers to the number of data messages that are re-transmitted and acknowledged by the peer successfully.
Send Failures	Refers to the number of data messages that are not acknowledged by the peer even after the specified number of retransmissions.
Receive Success	Refers to the number of data messages received and acknowledged successfully.
Receive Retries	Refers to the number of successfully received re-transmitted data messages.
Receive Failures	Refers to the number of data messages that were not received successfully.
Registration Details Specifies the status of the entire registration process.	
Remote Partners	Refers to the number of remote partners. For an SU/End Point A/End Point B, the number of remote partners is always zero or one.
Announcements	Refers to the number of Announcement messages sent or received on WORP interface.
Request For Service	Refers to the number of requests for service messages sent or received.
Registration Requests	Refers to the number of registration request messages sent or received on WORP interface.
Registration Rejects	Refers to the number of registration reject messages sent or received on WORP interface.
Authentication Requests	Refers to the number of authentication request messages sent or received on WORP interface.

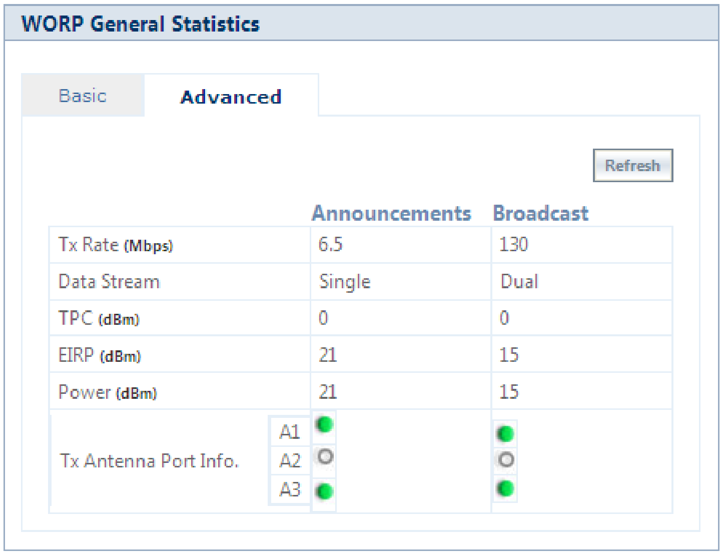
Parameter	Description
Authentication Confirms	Refers to the number of authentication confirm messages sent or received on WORP interface.
Registration Attempts	Refers to the number of times a registration attempt has been initiated.
Registration Incompletes	Refers to the number of registration attempts that are not yet completed.
Registration Timeouts	Refers to the number of times the registration procedure timed out.
Registration Last Reason	Refers to the reason for the last registration getting aborted or failed.

: For better results, the Send Failure or Send Retrieve must be low in comparison to Send Success. The same applies for Receive Retries or Receive Failure.

Click Clear to delete existing general statistics. Click **Refresh** to view updated WORP general statistics.

7.3.1.2 Advanced Statistics

Advanced statistics is applicable only to the BSU. The **Advanced Statistics** screen displays the wireless transmission values used by the BSU to send announcement and broadcast messages.



		Announcements	Broadcast
Tx Rate (Mbps)		6.5	130
Data Stream		Single	Dual
TPC (dBm)		0	0
EIRP (dBm)		21	15
Power (dBm)		21	15
Tx Antenna Port Info.	A1	●	●
	A2	○	○
	A3	●	●

Figure 7-12 WORP Advanced Statistics

Given below is an explanation to the advanced parameters:

Parameter	Description
Tx Rate	Displays the Data Transmission Rate used by the BSU.
Data Stream	Displays the Data Streams used by the BSU.

Parameter	Description
TPC	Displays the TPC value currently applied by the device to adjust the transmit power radiated by the radio.
EIRP	Displays the current EIRP that a radio antenna radiates (after applying the TPC).
Power	Displays the current transmit power radiated by the radio (after applying the TPC).
Tx Antenna Ports	Indicates the status of the antenna ports at the BSU end.

Click **Refresh** to view updated WORP advanced statistics.

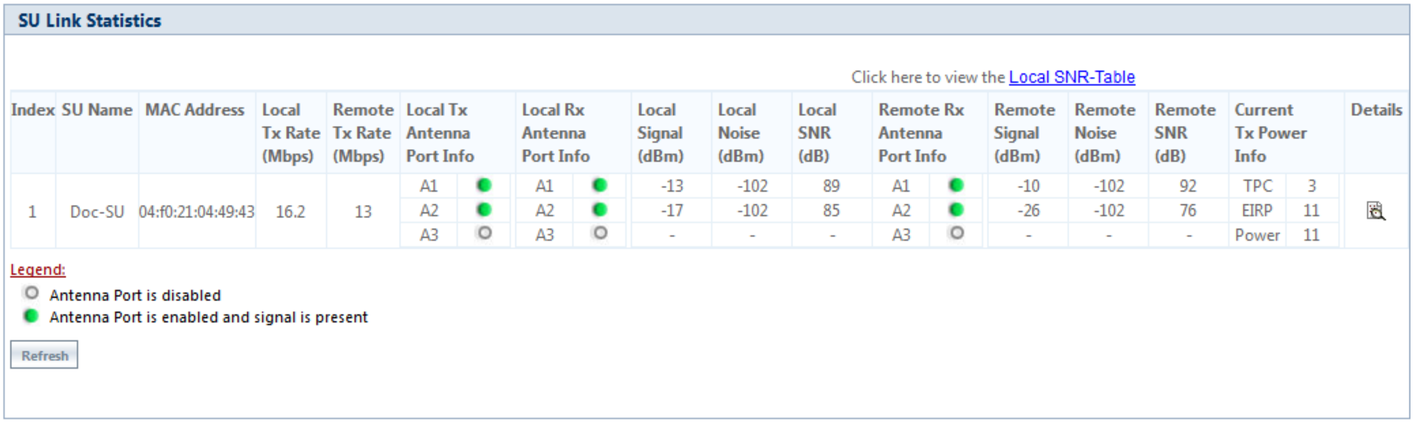
7.3.2 Link Statistics

7.3.2.1 SU / End Point B Link Statistics

: SU Link Statistics is applicable only to a BSU, and End Point B Link Statistics is applicable only to a End Point A device.

SU Link statistics provides information about the SUs connected to a BSU. Similarly, End Point B Link Statistics provides information about an End Point B currently connected to an End Point A device.

To view link statistics, navigate to **MONITOR > WORP Statistics > Interface 1 > SU Link Statistics**.



SU Link Statistics

Click here to view the Local SNR-Table

Index	SU Name	MAC Address	Local Tx Rate (Mbps)	Remote Tx Rate (Mbps)	Local Tx Antenna Port Info		Local Rx Antenna Port Info		Local Signal (dBm)	Local Noise (dBm)	Local SNR (dB)	Remote Rx Antenna Port Info		Remote Signal (dBm)	Remote Noise (dBm)	Remote SNR (dB)	Current Tx Power Info		Details
1	Doc-SU	04:f0:21:04:49:43	16.2	13	A1	●	A1	●	-13	-102	89	A1	●	-10	-102	92	TPC	3	
					A2	●	A2	●	-17	-102	85	A2	●	-26	-102	76	EIRP	11	
					A3	○	A3	○	-	-	-	A3	○	-	-	-	Power	11	

Legend:

○ Antenna Port is disabled

● Antenna Port is enabled and signal is present

Figure 7-13 An Example - SU Link Statistics

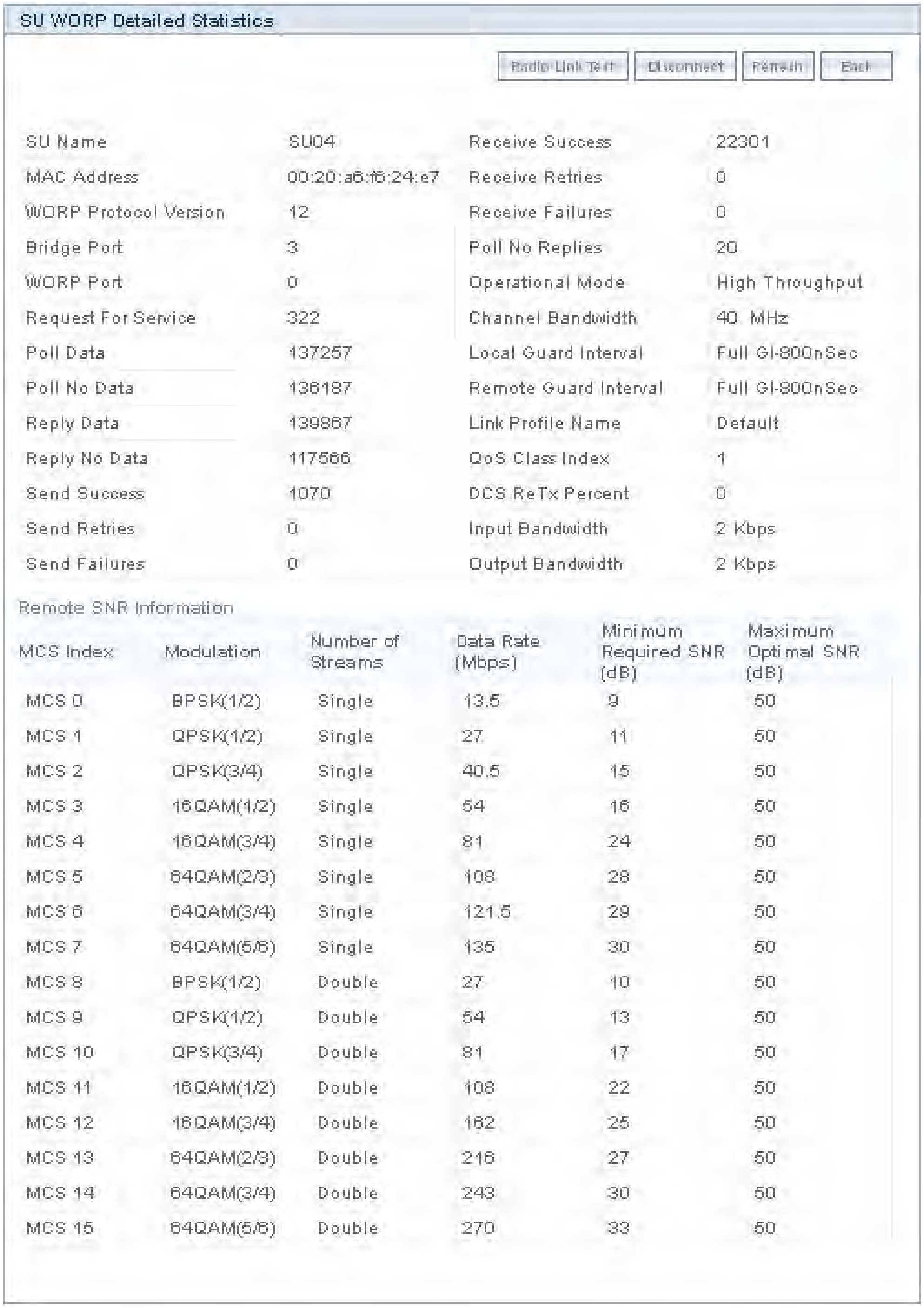
Given below is an explanation to each of these parameters:

Parameter	Description
SU Name/ End Point B Name	Represents the name of the SU/End Point B connected to a BSU/End Point A respectively.
MAC Address	Represents the MAC address of the SU/End Point B connected to a BSU/End Point A respectively.
Local Tx Rate (Mbps)	Represents the data transmission rate at the local (current device) end.

Parameter	Description
Remote Tx Rate (Mbps)	Represents the data transmission rate at the remote (peer) end.
Local Tx Antenna Port Info	Indicates the status of the antenna ports at the transmitting end. The following symbols indicate the status of the antenna ports. ○ Indicates the antenna port is disabled. ● Indicates the antenna port is enabled and signal is present.
Local Rx Antenna Port Info	Indicates the status of the antenna ports at the receiving end. The following symbols indicate the status of the antenna ports. ○ Indicates the antenna port is disabled. ● Indicates the antenna port is enabled and signal is present.
Local Signal (dBm)	Represents the signal level with which the device at the local end receives frames from the device at the remote end, through wireless medium.
Local Noise (dBm)	Represents the noise measured at the local end antenna ports.
Local SNR (dB)	Represents the SNR measured by the receiver at the local end and is based on the Local Signal and Local Noise.
Remote Rx Antenna Port Info	Indicates the status of the remote end antenna ports. The antenna ports status is same as explained in Local Antenna Port Info.
Remote Signal (dBm)	Represents the signal level with which the device at the remote end receives frames, through wireless medium.
Remote Noise (dBm)	Represents the noise measured at the remote end antenna ports.
Remote SNR (dB)	Represents the SNR measured by the receiver at the remote end and is based on the Remote Signal and Remote Noise.
Current Tx Power (dBm)	• **TPC**: Displays the TPC value currently applied by the device to adjust the transmit power radiated by the radio antenna. *: For a given data rate, if the configured TPC value is greater than the maximum transmit power supported by the radio then maximum transmit power supported by radio value is applied.* • **EIRP**: Displays the current EIRP that a radio antenna radiates (after applying the TPC). • **Power**: Displays the current transmit power radiated by the radio (after applying the TPC).

Click **Refresh** to view updated link statistics.

To view detailed SU/End Point B Link statistics, click **Details** icon in the **SU/End Point B Link Statistics** screen. The following screen appears depending on your device:



SU Name	SU04	Receive Success	22301
MAC Address	00:20:a6:f6:24:e7	Receive Retries	0
WORP Protocol Version	12	Receive Failures	0
Bridge Port	3	Poll No Replies	20
WORP Port	0	Operational Mode	High Throughput
Request For Service	322	Channel Bandwidth	40 MHz
Poll Data	137257	Local Guard Interval	Full GI-800nSec
Poll No Data	136187	Remote Guard Interval	Full GI-800nSec
Reply Data	139867	Link Profile Name	Default
Reply No Data	117566	QoS Class Index	1
Send Success	1070	DCS ReTx Percent	0
Send Retries	0	Input Bandwidth	2 Kbps
Send Failures	0	Output Bandwidth	2 Kbps

Remote SNR Information

MCS Index	Modulation	Number of Streams	Data Rate (Mbps)	Minimum Required SNR (dB)	Maximum Optimal SNR (dB)
MCS 0	BPSK(1/2)	Single	13.5	9	50
MCS 1	QPSK(1/2)	Single	27	11	50
MCS 2	QPSK(3/4)	Single	40.5	15	50
MCS 3	16QAM(1/2)	Single	54	16	50
MCS 4	16QAM(3/4)	Single	81	24	50
MCS 5	64QAM(2/3)	Single	108	28	50
MCS 6	64QAM(3/4)	Single	121.5	29	50
MCS 7	64QAM(5/6)	Single	135	30	50
MCS 8	BPSK(1/2)	Double	27	10	50
MCS 9	QPSK(1/2)	Double	54	13	50
MCS 10	QPSK(3/4)	Double	81	17	50
MCS 11	16QAM(1/2)	Double	108	22	50
MCS 12	16QAM(3/4)	Double	162	25	50
MCS 13	64QAM(2/3)	Double	216	27	50
MCS 14	64QAM(3/4)	Double	243	30	50
MCS 15	64QAM(5/6)	Double	270	33	50

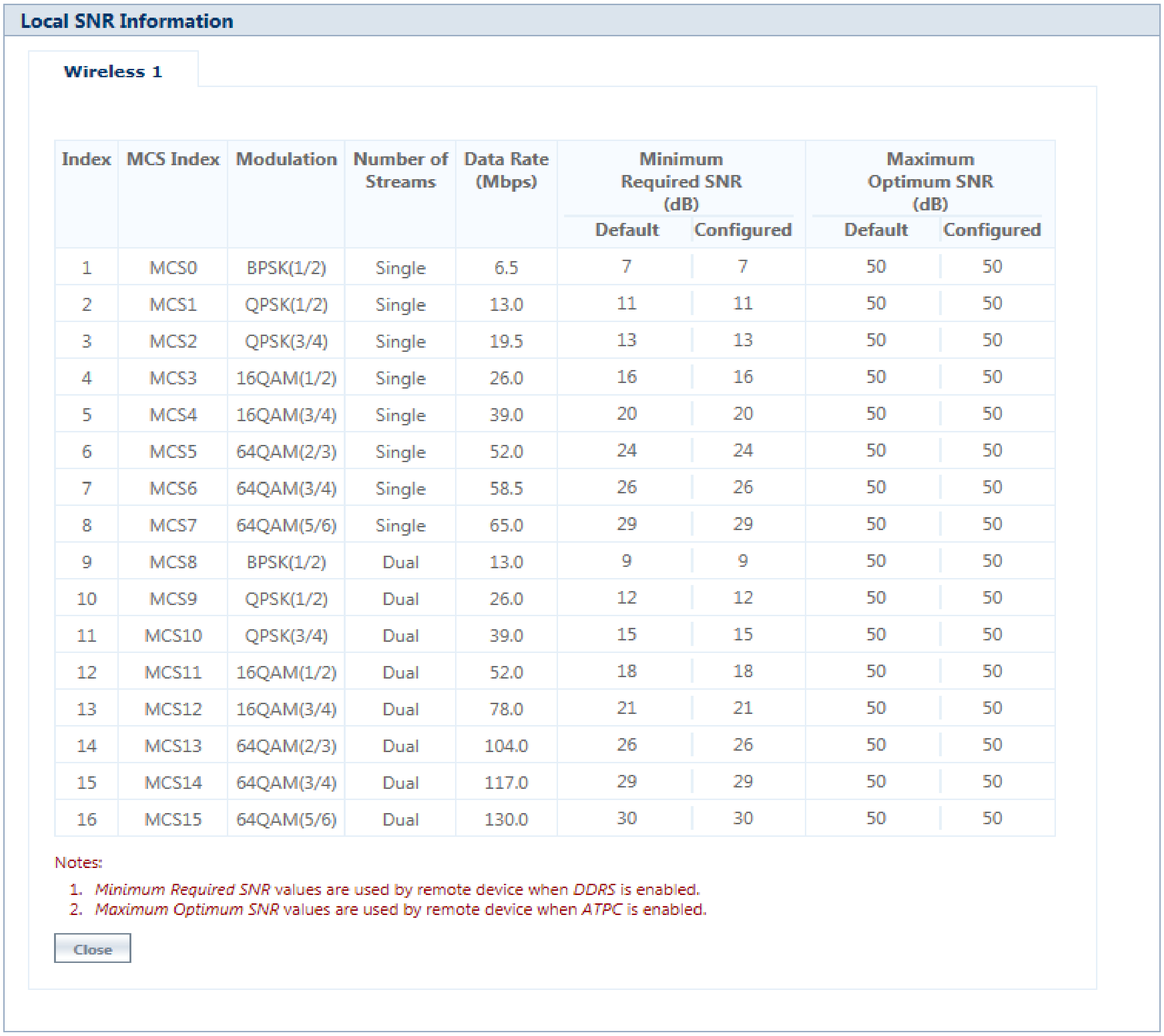
Figure 7-14 An Example - SU Detailed Statistics

The detailed page displays Remote SNR information, that is, the Minimum Required SNR and the Maximum Optimal SNR value for a given data rate or modulation, to achieve optimal throughput.

To disconnect an SU/End Point B from BSU/End Point A respectively, click **Disconnect**.

To view updated detailed statistics, click **Refresh**.

To view the local SNR table, there is an option as Click here to view the Local SNR-Table on the top-right corner of **SU/End Point B Link Statistics** screen. you can also refer An Example - SU Link Statistics for more details. The following screen appears depending on your device:



Local SNR Information

Index	MCS Index	Modulation	Number of Streams	Data Rate (Mbps)	Minimum Required SNR (dB)		Maximum Optimum SNR (dB)	
					Default	Configured	Default	Configured
1	MCS0	BPSK(1/2)	Single	6.5	7	7	50	50
2	MCS1	QPSK(1/2)	Single	13.0	11	11	50	50
3	MCS2	QPSK(3/4)	Single	19.5	13	13	50	50
4	MCS3	16QAM(1/2)	Single	26.0	16	16	50	50
5	MCS4	16QAM(3/4)	Single	39.0	20	20	50	50
6	MCS5	64QAM(2/3)	Single	52.0	24	24	50	50
7	MCS6	64QAM(3/4)	Single	58.5	26	26	50	50
8	MCS7	64QAM(5/6)	Single	65.0	29	29	50	50
9	MCS8	BPSK(1/2)	Dual	13.0	9	9	50	50
10	MCS9	QPSK(1/2)	Dual	26.0	12	12	50	50
11	MCS10	QPSK(3/4)	Dual	39.0	15	15	50	50
12	MCS11	16QAM(1/2)	Dual	52.0	18	18	50	50
13	MCS12	16QAM(3/4)	Dual	78.0	21	21	50	50
14	MCS13	64QAM(2/3)	Dual	104.0	26	26	50	50
15	MCS14	64QAM(3/4)	Dual	117.0	29	29	50	50
16	MCS15	64QAM(5/6)	Dual	130.0	30	30	50	50

Notes:

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

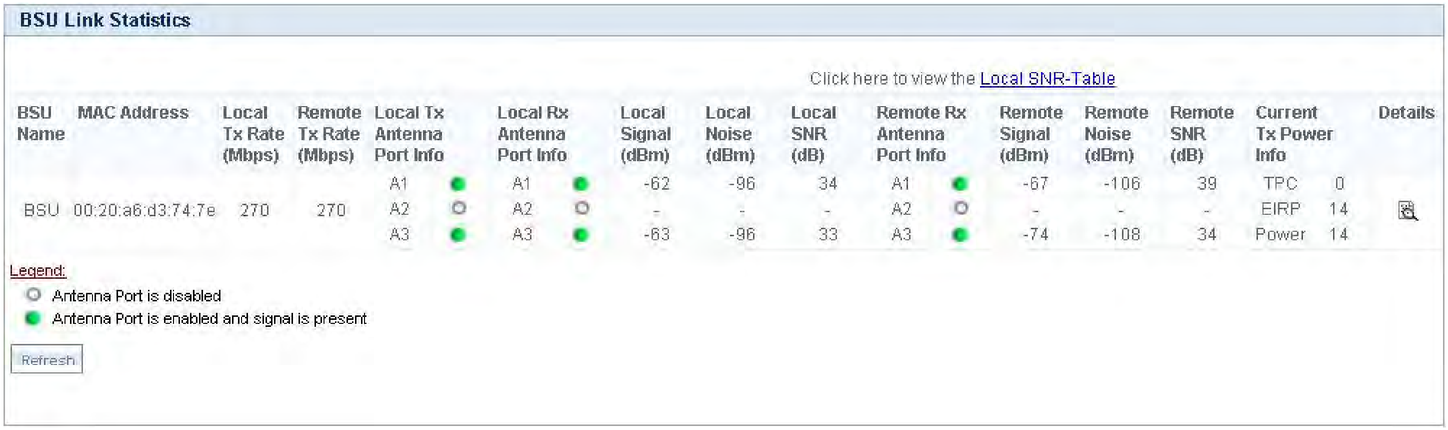
Figure 7-15 An Example - Local SNR Information

These configured values are used by ATPC and DDRS to derive TPC and data rate for optimal throughput.

7.3.2.2 BSU/End Point A Link Statistics

: BSU Link Statistics is applicable only to an SU, and End Point A Link Statistics is applicable only to an End Point B device.

BSU Link statistics provides information about the BSU to which SUs are connected. Similarly, End Point A Link Statistics provides information about an End Point A currently linked to an End Point B device.



BSU Link Statistics

Click here to view the Local SNR-Table

BSU Name	MAC Address	Local Tx Rate (Mbps)	Remote Tx Rate (Mbps)	Local Tx Antenna Port Info	Local Rx Antenna Port Info	Local Signal (dBm)	Local Noise (dBm)	Local SNR (dB)	Remote Rx Antenna Port Info	Remote Signal (dBm)	Remote Noise (dBm)	Remote SNR (dB)	Current Tx Power Info	Details
BSU	00:20:a6:d3:74:7e	270	270	A1 ● A2 ○ A3 ●	A1 ● A2 ○ A3 ●	-62 - -63	-96 - -96	34 - 33	A1 ● A2 ○ A3 ●	-67 - -74	-106 - -108	39 - 34	TPC 0 EIRP 14 Power 14	🔍

Legend:
- ○ Antenna Port is disabled
- ● Antenna Port is enabled and signal is present

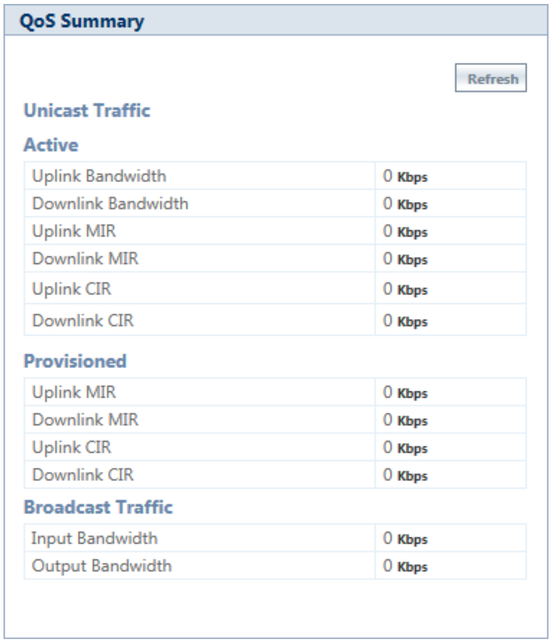
Figure 7-16 An Example - BSU Link Statistics

To access the Radio Link Test Tool, navigate to MONITOR > WORP Statistics > Interface 1 > SU/BSU Link Statistics > Details. Click . The SU/BSU WORP Detailed Statistics screen appears. In this screen, click the Radio Link Test button. For detailed description of this tool, refer Radio Link Test Tool.

7.3.3 QoS Statistics (BSU or End Point A Only)

: This parameter is applicable only to BSU or End Point A radio modes.

To view QoS Statistics, navigate to **MONITOR > WORP Statistics > Interface 1 > QoS Statistics.** The following **QoS Summary** screen appears.



QoS Summary

Unicast Traffic

Active

Uplink Bandwidth	0 Kbps
Downlink Bandwidth	0 Kbps
Uplink MIR	0 Kbps
Downlink MIR	0 Kbps
Uplink CIR	0 Kbps
Downlink CIR	0 Kbps

Provisioned

Uplink MIR	0 Kbps
Downlink MIR	0 Kbps
Uplink CIR	0 Kbps
Downlink CIR	0 Kbps

Broadcast Traffic

Input Bandwidth	0 Kbps
Output Bandwidth	0 Kbps

Figure 7-17 QoS Summary

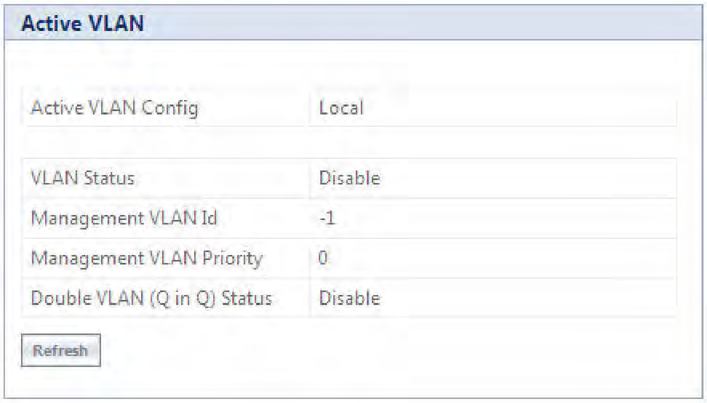
This screen shows the total, minimum and maximum bandwidth allocated per BSU/End Point A, and the minimum and maximum bandwidth allocated for each SU/End Point B registered with the BSU/End Point A respectively.

7.4 Active VLAN

: Active VLAN is applicable only to a device in SU (Bridge) mode.

The Active VLAN page enables you to identify the VLAN Configuration mode applied on a device in SU mode.

To view active VLAN applied on the device in SU mode, navigate to **MONITOR** > **Active VLAN**. The **Active VLAN** page appears:



Active VLAN

Active VLAN Config	Local
VLAN Status	Disable
Management VLAN Id	-1
Management VLAN Priority	0
Double VLAN (Q in Q) Status	Disable

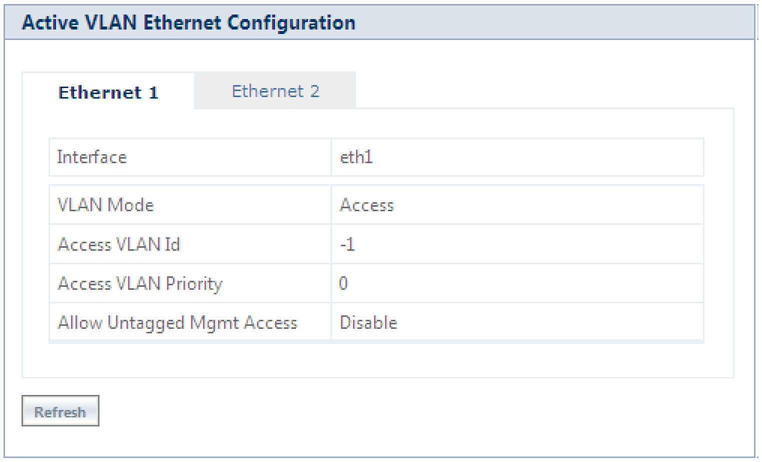
Figure 7-18 Active VLAN

The **Active VLAN Config** parameter helps you to identify the current VLAN configuration applied on the device in SU mode.

- **Local**: VLAN configuration is done locally from the device.
- **Remote**: VLAN configuration is done through RADIUS Server.

This page also displays the VLAN parameters and their values that are configured either locally or remotely.

To view active VLAN Ethernet Configuration, navigate to **MONITOR** > **Active VLAN > Ethernet**. The **Active VLAN Ethernet Configuration** page appears:



Active VLAN Ethernet Configuration

Interface	eth1
VLAN Mode	Access
Access VLAN Id	-1
Access VLAN Priority	0
Allow Untagged Mgmt Access	Disable

Figure 7-19 Active VLAN Ethernet Configuration

This page displays the VLAN Ethernet parameters and their values that are configured either locally or remotely.

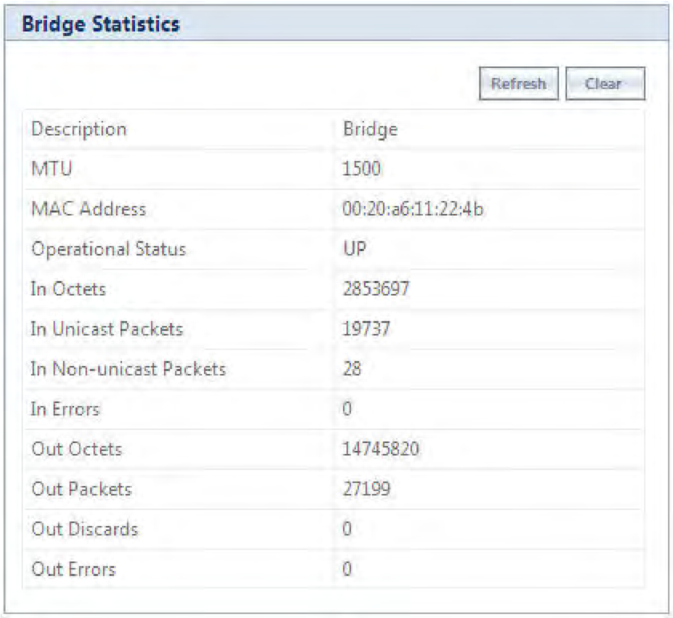
: Please note that the number of Ethernets vary depending on the device.

7.5 Bridge

7.5.1 Bridge Statistics

The Bridge Statistics allows you to monitor the statistics of the Bridge.

To view the **Bridge Statistics**, navigate to **MONITOR > Bridge > Bridge Statistics**. The following **Bridge Statistics** screen appears:



Bridge Statistics

Description	Bridge
MTU	1500
MAC Address	00:20:a6:11:22:4b
Operational Status	UP
In Octets	2853697
In Unicast Packets	19737
In Non-unicast Packets	28
In Errors	0
Out Octets	14745820
Out Packets	27199
Out Discards	0
Out Errors	0

Figure 7-20 Bridge Statistics

The following table lists the parameters and their description**:**

Parameter	Description
Description	This parameter provides a description about the bridge.
MTU	Represents the largest size of the data packet sent on the bridge.
MAC Address	Represents the MAC address at the bridge protocol layer.
Operational Status	Represents the current operational status of the bridge: **UP** (ready to pass packets) or **DOWN** (not ready to pass packets).
In Octets	Represents the total number of octets received on the bridge interface, including the framing characters.
In Unicast Packets	Represents the number of unicast subnetwork packets delivered to the higher level protocol.
In Non-unicast Packets	Represents the number of non-unicast subnetwork packets delivered to the higher level protocol.
In Errors	Represents the number of inbound packets with errors and that are restricted from being delivered.

Parameter	Description
Out Octets	Represents the total number of octets transmitted out of the bridge, including the framing characters.
Out Packets	Represents the total number of packets requested by higher-level protocols to be transmitted out of the bridge interface to a sub-network address, including those that were discarded or not sent.
Out Discards	Represents the number of error-free outbound packets which are discarded to prevent them from being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Out Errors	Represents the number of outbound packets that could not be transmitted because of errors.

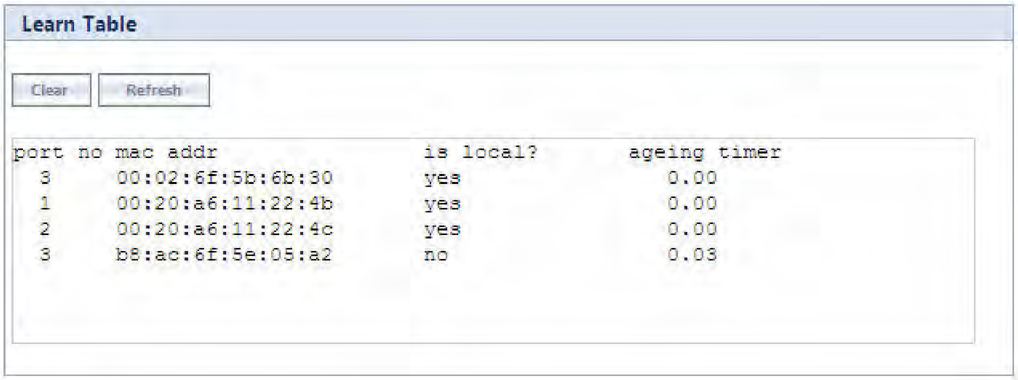
To view updated Bridge statistics, click **Refresh**.

To clear the Bridge statistics, click **Clear**.

7.5.2 Learn Table

Learn Table allows you to view all the MAC addresses that the device has learnt on all of its interfaces.

To view Learn Table statistics, navigate to **MONITOR > Bridge > Learn Table**. The **Learn Table** screen appears.



```
port no mac addr             is local?     ageing timer
  3     00:02:6f:5b:6b:30    yes              0.00
  1     00:20:a6:11:22:4b    yes              0.00
  2     00:20:a6:11:22:4c    yes              0.00
  3     b8:ac:6f:5e:05:a2    no               0.03
```

Figure 7-21 Learn Table

The Learn Table displays the MAC address of the learnt device, the bridge port number, aging timer for each device learnt on an interface, and the local (DUT's local interfaces)/remote (learned entries through bridging) status of the learnt device.

To view updated learn table statistics, click **Refresh**.

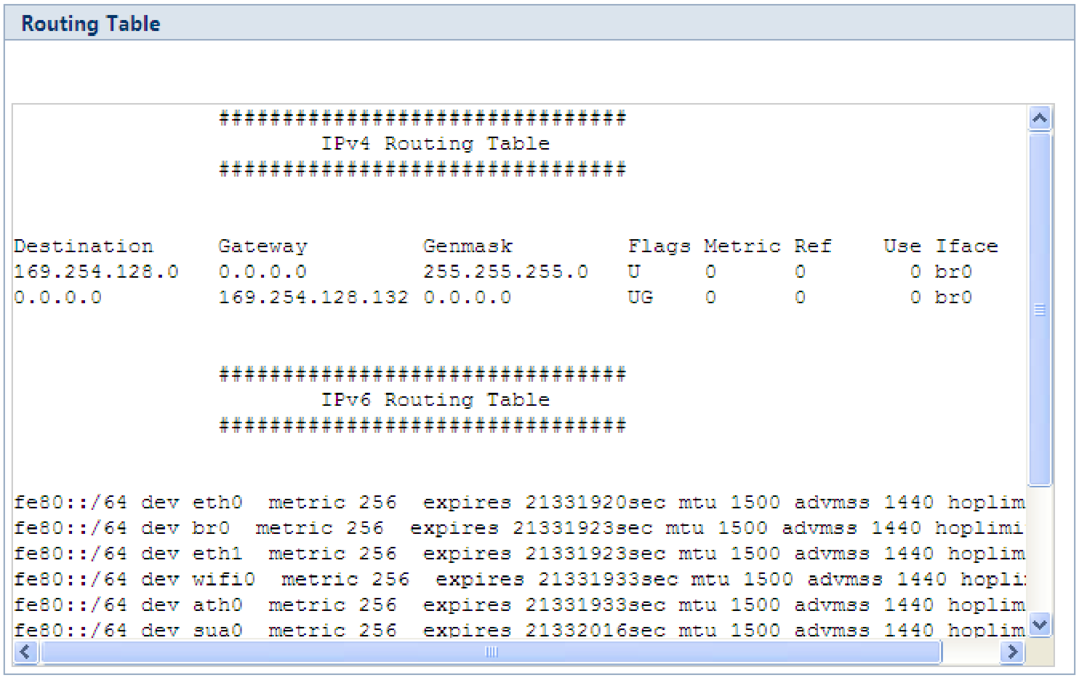
To clear learn table statistics, click **Clear**.

7.6 Network Layer

7.6.1 Routing Table

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

To view the Routing Table, navigate to **MONITOR > Network Layer > Routing Table**. The **Routing Table** screen appears:



Routing Table

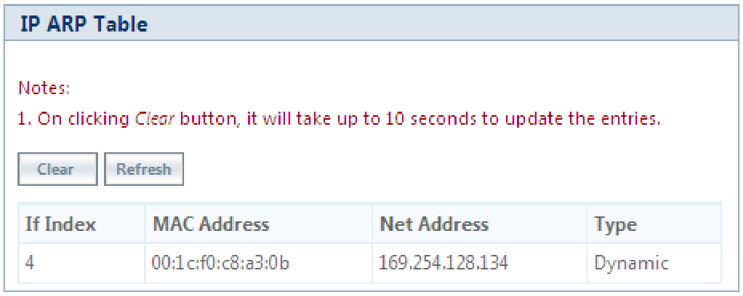
```
                ################################
                        IPv4 Routing Table
                ################################


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


                ################################
                        IPv6 Routing Table
                ################################


fe80::/64 dev eth0  metric 256  expires 21331920sec mtu 1500 advmss 1440 hoplim
fe80::/64 dev br0  metric 256  expires 21331923sec mtu 1500 advmss 1440 hoplimi
fe80::/64 dev eth1  metric 256  expires 21331923sec mtu 1500 advmss 1440 hoplim
fe80::/64 dev wifi0  metric 256  expires 21331933sec mtu 1500 advmss 1440 hopli
fe80::/64 dev ath0  metric 256  expires 21331933sec mtu 1500 advmss 1440 hoplim
fe80::/64 dev sua0  metric 256  expires 21332016sec mtu 1500 advmss 1440 hoplim
```

Figure 7-22 Routing Table

7.6.2 IP ARP

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical address on the network. The IP ARP table is used to maintain a correlation between each IP address and its corresponding MAC address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

To view IP Address Resolution Protocol (ARP) statistics, navigate to **MONITOR > Network Layer > IP ARP**. The **IP ARP Table** screen appears.



IP ARP Table

Notes:

1. On clicking *Clear* button, it will take up to 10 seconds to update the entries.

If Index	MAC Address	Net Address	Type
4	00:1c:f0:c8:a3:0b	169.254.128.134	Dynamic

Figure 7-23 IP ARP Table

The **IP ARP Table** contains the following information:

- **Index:** Represents the interface type.
- **MAC Address:** Represents the MAC address of a node on the network.
- **Net Address**: This parameter represents the corresponding IP address of a node on the network.
- **Type**: This parameter represents the type of mapping, that is, Dynamic or Static.

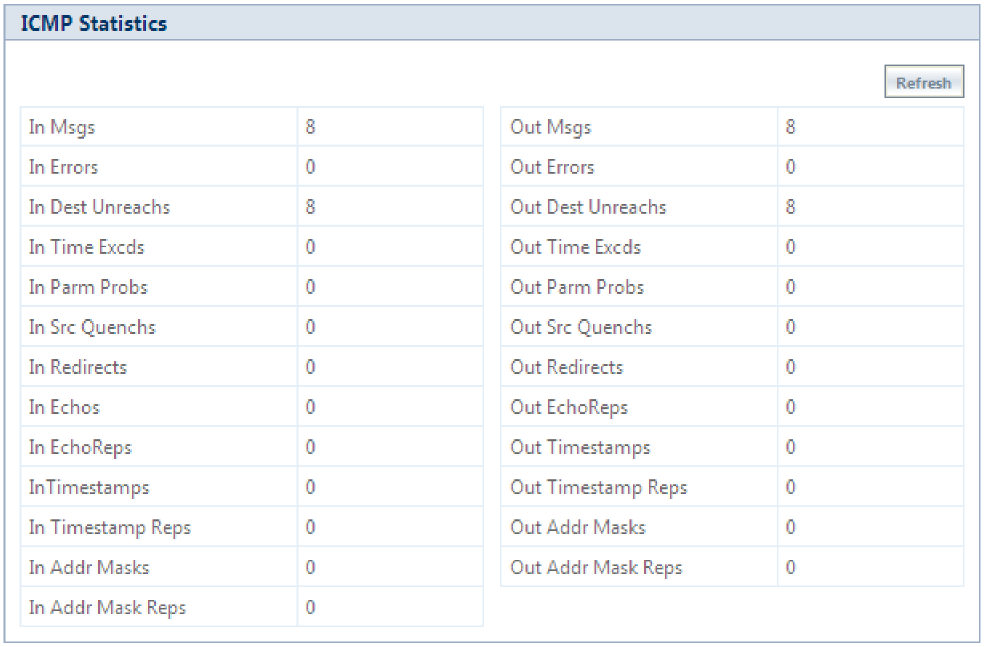
To view updated IP ARP entries, click **Refresh**.

To clear the IP ARP entries, click **Clear**.

7.6.3 ICMP Statistics

The ICMP Statistics attributes enable you to monitor the message traffic that is received and transmitted by the device.

To view ICMP statistics, navigate to **MONITOR > Network Layer > ICMP Statistics**. The **ICMP Statistics** screen appears.



In Msgs	8	Out Msgs	8
In Errors	0	Out Errors	0
In Dest Unreachs	8	Out Dest Unreachs	8
In Time Excds	0	Out Time Excds	0
In Parm Probs	0	Out Parm Probs	0
In Src Quenchs	0	Out Src Quenchs	0
In Redirects	0	Out Redirects	0
In Echos	0	Out EchoReps	0
In EchoReps	0	Out Timestamps	0
InTimestamps	0	Out Timestamp Reps	0
In Timestamp Reps	0	Out Addr Masks	0
In Addr Masks	0	Out Addr Mask Reps	0
In Addr Mask Reps	0		

Figure 7-24 ICMP Statistics

The following table lists the ICMP Statistics parameters and their description**:**

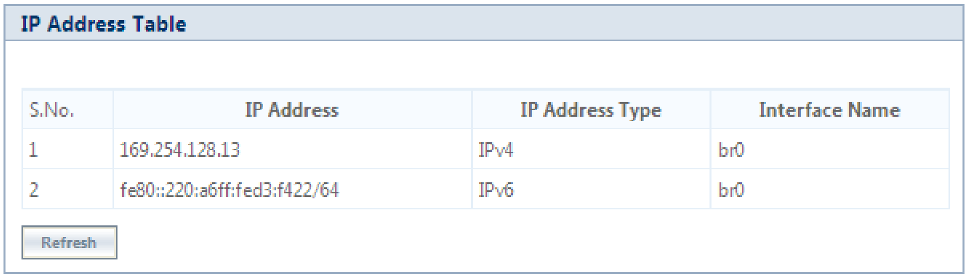
Parameter	Description
In Msgs or Out Msgs	Represents the number of ICMP messages that are received/transmitted by the device.
In Errors or Out Errors	Represents the number of ICMP messages that are received/transmitted by the device but determined as having ICMP-specific errors such as Bad ICMP checksums, bad length and so on.
In Dest Unreachs or Out Dest Unreachs	Represents the number of ICMP destination unreachable messages that are received/transmitted by the device.
In Time Excds or Out Time Excds	Represents the number of ICMP time exceeded messages that are received/transmitted by the device.
In Parm Probs or Out Parm Probs	Represents the number of ICMP parameter problem messages that are received/transmitted by the device.
In Srec Quenchs or Out Srec Quenchs	Represents the number of ICMP source quench messages that are received/transmitted by the device.
In Redirects or Out Redirects	Represents the rate at which the ICMP redirect messages are received/transmitted by the device.
In Echos	Represents the rate at which the ICMP echo messages are received.
In EchoReps or Out EchoReps	Represents the rate at which the ICMP echo reply messages are received/transmitted by the device.

Parameter	Description
In Timestamps or Out Timestamps	Represents the rate at which the ICMP timestamp (request) messages are received/transmitted by the device.
In Timestamps Reps or Out Timestamps Reps	Represents the rate at which the ICMP timestamp reply messages are received/transmitted by the device.
In Addr Masks or Out Addr Masks	Represents the number of ICMP address mask request messages that are received/transmitted by the device.
In Addr Mask Reps or Out Addr Mask Reps	Represents the number of ICMP address mask reply messages that are received/transmitted by the device.

To view updated ICMP Statistics, click **Refresh**.

7.6.4 IP Address Table

The **IP Address Table** shows all IP addresses of the device. The IP Address Table screen contains IP addresses of the interface. To view table, navigate to **MONITOR > Network Layer > IP Address Table**. The **IP Address Table** screen appears.



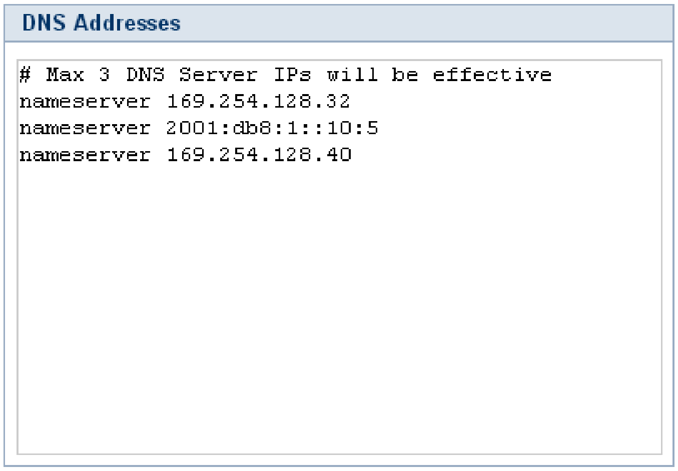
IP Address Table

S.No.	IP Address	IP Address Type	Interface Name
1	169.254.128.13	IPv4	br0
2	fe80::220:a6ff:fed3:f422/64	IPv6	br0

Figure 7-25 IP Address Table

7.6.5 DNS Addresses

It shows DNS Addresses currently active on the device. To view DNS addresses, navigate to **MONITOR > Network Layer > DNS Addresses**. The **DNS Addresses** screen appears.



DNS Addresses

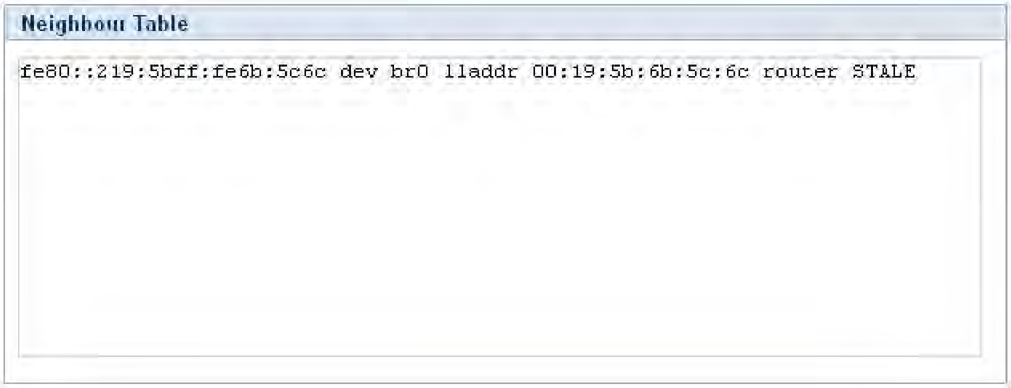
```
# Max 3 DNS Server IPs will be effective
nameserver 169.254.128.32
nameserver 2001:db8:1::10:5
nameserver 169.254.128.40
```

Figure 7-26 DNS Addresses

7.6.6 Neighbour Table

: This parameter is applicable only in **IPv4 and IPv6** mode, not in **IPv4 only** mode.

The Neighbour Table contains a list of neighbouring routers and information about them. To view Neighbour Table, navigate to **MONITOR > Network Layer > Neighbour Table**. The **Neighbour table** screen appears.



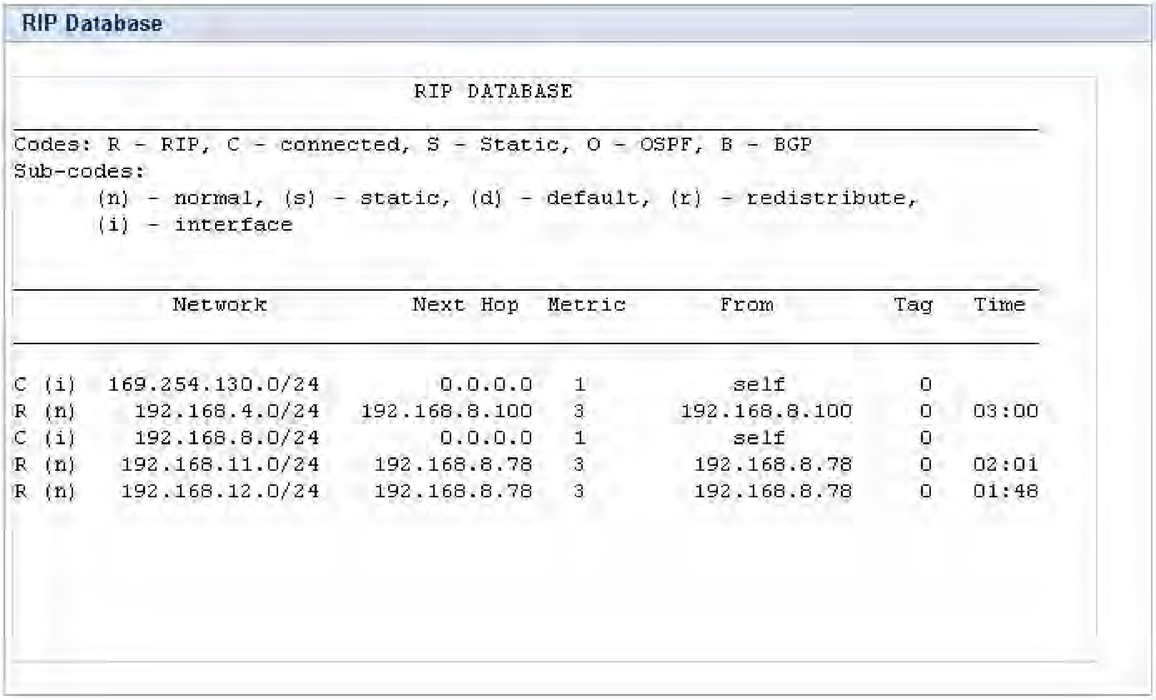
```
fe80::219:5bff:fe6b:5c6c dev br0 lladdr 00:19:5b:6b:5c:6c router STALE
```

Figure 7-27 Neighbour Table

7.6.7 RIP Database

: *Applicable only in routing mode.*

The **RIP Database** screen contains routes (Routing Information Protocol updates) learnt from other routers.



```
                         RIP DATABASE
---------------------------------------------------------------------------
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
      (n) - normal, (s) - static, (d) - default, (r) - redistribute,
      (i) - interface

---------------------------------------------------------------------------
            Network          Next Hop  Metric      From         Tag   Time
---------------------------------------------------------------------------

C (i)  169.254.130.0/24        0.0.0.0    1         self         0
R (n)    192.168.4.0/24  192.168.8.100    3     192.168.8.100    0   03:00
C (i)    192.168.8.0/24        0.0.0.0    1         self         0
R (n)   192.168.11.0/24   192.168.8.78    3      192.168.8.78    0   02:01
R (n)   192.168.12.0/24   192.168.8.78    3      192.168.8.78    0   01:48
```

Figure 7-28 RIP Database

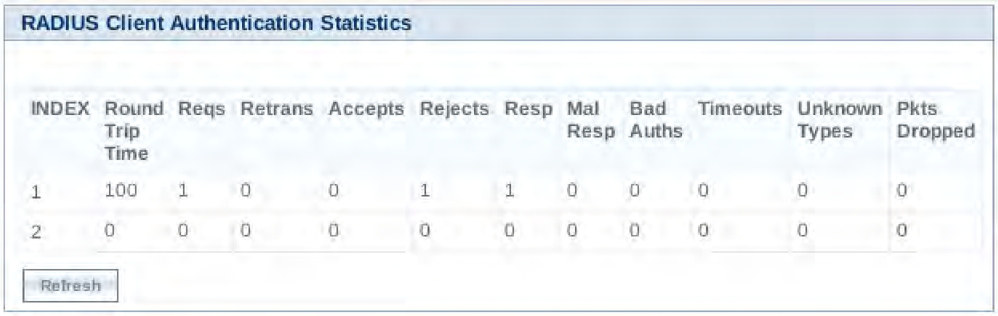
7.7 RADIUS (BSU or End Point A only)

: RADIUS is applicable only to a BSU or an End Point A device.

7.7.1 Authentication Statistics

Authentication Statistics provides information on RADIUS Authentication for both the primary and backup servers for each RADIUS server profile.

To view Authentication statistics, navigate to **MONITOR > RADIUS > Authentication Statistics**. The **RADIUS Client Authentication Statistics** screen appears:



RADIUS Client Authentication Statistics

INDEX	Round Trip Time	Reqs	Retrans	Accepts	Rejects	Resp	Mal Resp	Bad Auths	Timeouts	Unknown Types	Pkts Dropped
1	100	1	0	0	1	1	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0

Figure 7-29 Radius Client Authentication Statistics

The following table lists the Authentication Statistics parameters and their description**:**

Parameter	Description
Round Trip Time	Represents the round trip time for messages exchanged between RADIUS client and authentication server since the client startup.
Reqs	Represents the number of RADIUS access request messages transmitted from the RADIUS client to the authentication server since client startup**.**
RTMS	This parameter represents the number of times the RADIUS access requests are being transmitted to the server from the device since the client startup.
Accepts	Represents the number of RADIUS access accept messages received by the device since client startup.
Rejects	Represents the number of RADIUS access reject messages received by the device since client startup.
Resp	Represents the number of RADIUS response packets received by the device since client startup.
Mal Resp	Represents the number of malformed RADIUS access response messages received by the device since client startup.
Bad Auths	Represents the number of malformed RADIUS access response messages containing invalid authenticators received by the device since client startup.
Time Outs	Represents the total number of timeouts for RADIUS access request messages since client startup.

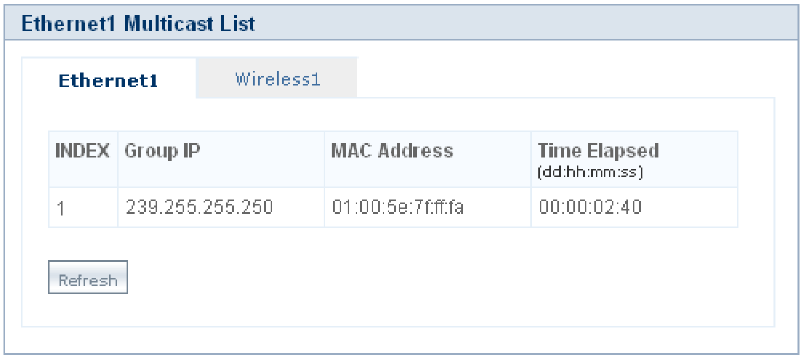
Parameter	Description
UnKnown Types	This parameter specifies the number of messages with unknown RADIUS message code since client startup.
Packets Dropped	Represents the number of RADIUS packets dropped by the device.

To view updated RADIUS Client Authentication statistics, click **Refresh**.

7.8 IGMP

: Applicable in Bridge mode only.

To view IGMP statistics, navigate to **MONITOR > IGMP > IGMP Snooping Stats**. The **Ethernet or Wireless Multicast List** screen appears:



INDEX	Group IP	MAC Address	Time Elapsed (dd:hh:mm:ss)
1	239.255.255.250	01:00:5e:7f:ff:fa	00:00:02:40

Figure 7-30 Ethernet1 Multicast List

7.8.1 Ethernet or Wireless Multicast List

The Multicast List table contains the IGMP Multicast IP and Multicast MAC address details for the Ethernet or Wireless interfaces. The following table lists the parameters and their description.

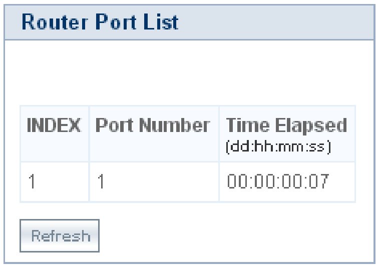
Parameter	Description
Group IP	Represents the IP address of the multicast group for Ethernet or Wireless interface learned by IGMP snooping.
MAC Address	Represents the MAC address of the multicast group for Ethernet or Wireless interface learned by IGMP snooping.
Time Elapsed	Represents the time elapsed since the multicast entry has been created for the Ethernet or Wireless interface.

To view updated IGMP statistics, click **Refresh**.

7.8.2 Router Port List

The Router Port List displays the list of ports on which multicast routers are attached.

To view Router Port List, navigate to **MONITOR > IGMP > Router Port List**. The **Router Port List** screen appears:



Router Port List

INDEX	Port Number	Time Elapsed (dd:hh:mm:ss)
1	1	00:00:00:07

Figure 7-31 Router Port List

The following table lists the parameters and their description.

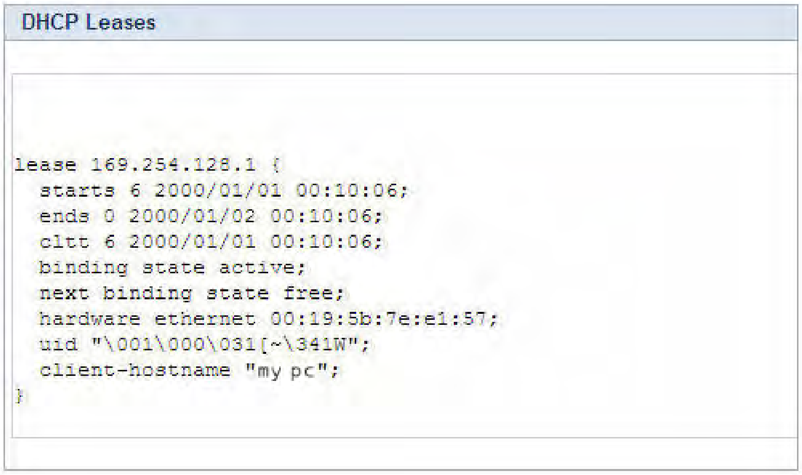
Parameter	Description
Port Number	Represents the port number on which multicast router is attached (on which IGMP Query has been received).
Time Elapsed	Represents the time elapsed since the port is marked as the router port.

To view updated Router Port list, click **Refresh**.

7.9 DHCP

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

To view DHCP Leases, navigate to **MONITOR > DHCP > Leases**.



DHCP Leases

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

Figure 7-32 DHCP Leases

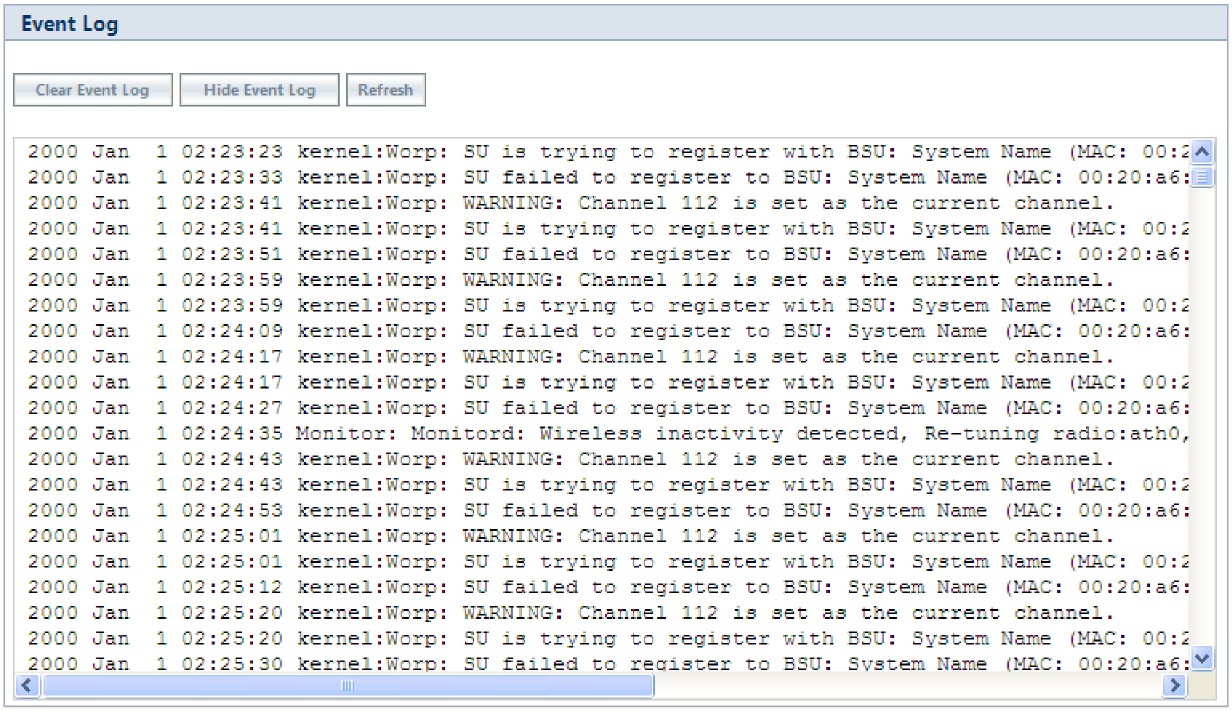
7.10 Logs

7.10.1 Event Log

Event Log file keeps track of events that occur during the operation of the device. It displays the event occurring time, event type, and the name of the error or the error message. Based on the priority (the log priority is set under **MANAGEMENT** > **Services** > **Logs**), the event details are logged and can be used for any future reference or troubleshooting.

7.10.1.1 View Event Log

To view the event log messages, navigate to **MONITOR > Logs > Event Log**. The following **Event Log** screen appears:



```
2000 Jan  1 02:23:23 kernel:Worp: SU is trying to register with BSU: System Name (MAC: 00:2
2000 Jan  1 02:23:33 kernel:Worp: SU failed to register to BSU: System Name (MAC: 00:20:a6:
2000 Jan  1 02:23:41 kernel:Worp: WARNING: Channel 112 is set as the current channel.
2000 Jan  1 02:23:41 kernel:Worp: SU is trying to register with BSU: System Name (MAC: 00:2
2000 Jan  1 02:23:51 kernel:Worp: SU failed to register to BSU: System Name (MAC: 00:20:a6:
2000 Jan  1 02:23:59 kernel:Worp: WARNING: Channel 112 is set as the current channel.
2000 Jan  1 02:23:59 kernel:Worp: SU is trying to register with BSU: System Name (MAC: 00:2
2000 Jan  1 02:24:09 kernel:Worp: SU failed to register to BSU: System Name (MAC: 00:20:a6:
2000 Jan  1 02:24:17 kernel:Worp: WARNING: Channel 112 is set as the current channel.
2000 Jan  1 02:24:17 kernel:Worp: SU is trying to register with BSU: System Name (MAC: 00:2
2000 Jan  1 02:24:27 kernel:Worp: SU failed to register to BSU: System Name (MAC: 00:20:a6:
2000 Jan  1 02:24:35 Monitor: Monitord: Wireless inactivity detected, Re-tuning radio:ath0,
2000 Jan  1 02:24:43 kernel:Worp: WARNING: Channel 112 is set as the current channel.
2000 Jan  1 02:24:43 kernel:Worp: SU is trying to register with BSU: System Name (MAC: 00:2
2000 Jan  1 02:24:53 kernel:Worp: SU failed to register to BSU: System Name (MAC: 00:20:a6:
2000 Jan  1 02:25:01 kernel:Worp: WARNING: Channel 112 is set as the current channel.
2000 Jan  1 02:25:01 kernel:Worp: SU is trying to register with BSU: System Name (MAC: 00:2
2000 Jan  1 02:25:12 kernel:Worp: SU failed to register to BSU: System Name (MAC: 00:20:a6:
2000 Jan  1 02:25:20 kernel:Worp: WARNING: Channel 112 is set as the current channel.
2000 Jan  1 02:25:20 kernel:Worp: SU is trying to register with BSU: System Name (MAC: 00:2
2000 Jan  1 02:25:30 kernel:Worp: SU failed to register to BSU: System Name (MAC: 00:20:a6:
```

Figure 7-33 Event Log Messages

To retrieve the event log file from the device, see Retrieve From Device.

The maximum size of the event log file is 65 KB. If the file size exceeds 65 KB, then all the log messages are moved to a backup file and only the recent 100 lines are displayed in the log file. When the size of the log file exceeds again then it overwrites the backup file.

Backup files can be retrieved by using 'retrieve' CLI command. For more details, see **Tsunami 800 and 8000 Series Reference guide** available at http://my.proxim.com.

: Log messages can be stored in the log file approximately up to 6 days with logging interval of 5 minutes.

7.10.1.2 Hide Event Log

To hide the event log messages, click **Hide Event Log**.

7.10.1.3 Clear Event Log

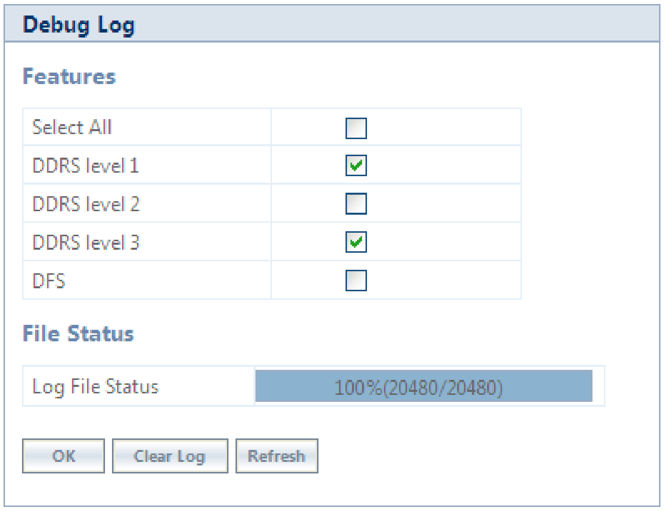
To clear the event log messages, click **Clear Event Log**. The messages are cleared and moved to the backup file leaving the event log file empty. An event is generated on clearing the event log messages.

: The current and the backed up event logs are stored in the flash memory and can be retrieved even after device reboot.

7.10.2 Debug Log

Debug Log helps you to debug issues related to important features of the device. Currently, this feature supports only DDRS and DFS. This feature helps the engineering team to get valuable information from the field to analyze the issues and provide faster solution. This feature should be used only in consultation with the Proxim Customer Support team. Once logging is enabled, the Debug Log file can be retrieved via HTTP or TFTP.

To enable Debug Log, navigate to **MONITOR > Logs > Debug Log**. The **Debug Log** screen appears:



Debug Log

Features

Select All	□
DDRS level 1	☑
DDRS level 2	□
DDRS level 3	☑
DFS	□

File Status

Log File Status	100%(20480/20480)

Figure 7-34 Debug Log

Features: Select the appropriate features to be logged. The available features are Select All, DDRS Level 1, DDRS Level 2, DDRS Level 3 and DFS.

File Status: This parameter displays the current size of the Debug Log file.

After selecting the **DDRS level**, click **OK**.

To delete the **Debug Log**, click **Clear Log**.

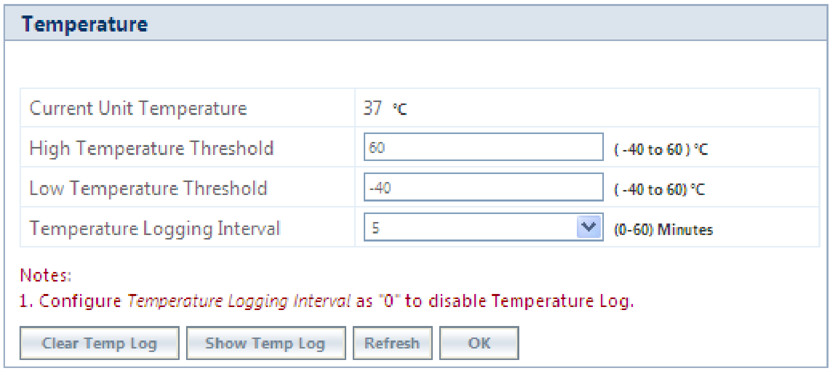
To get the updated status of the **Debug Log** File, Click **Refresh.**

7.10.3 Temperature Log

: Temperature Log is not applicable to MP-825-CPE-50, MP-825-CPE-100, MP-835-CPE-10, MP-835-CPE-25, MP-835-CPE-50, MP-835-CPE-100, MP-820-SUA-50$^+$, MP-820-SUA-100, MP-822-SUA-100, MP-825-SUR-50$^+$, MP-825-SUR-100 and QB-826-EPR/LNK-100 devices.

Temperature Log feature is used to log the internal temperature of the device for the configured temperature logging interval (By default, it is 5 minutes). It also generates a trap and an event message when the internal temperature of the device reaches or exceeds the configured threshold range. The device issues a warning trap when the temperature is 5° Celsius less than the configured threshold range.

To access this feature, navigate to **MONITOR > Logs > Temperature Log**. The following **Temperature** screen appears:



Temperature

Current Unit Temperature	37 °C	
High Temperature Threshold	60	(-40 to 60) °C
Low Temperature Threshold	-40	(-40 to 60) °C
Temperature Logging Interval	5	(0-60) Minutes

Notes:
1. Configure *Temperature Logging Interval* as "0" to disable Temperature Log.

Figure 7-35 Temperature Log

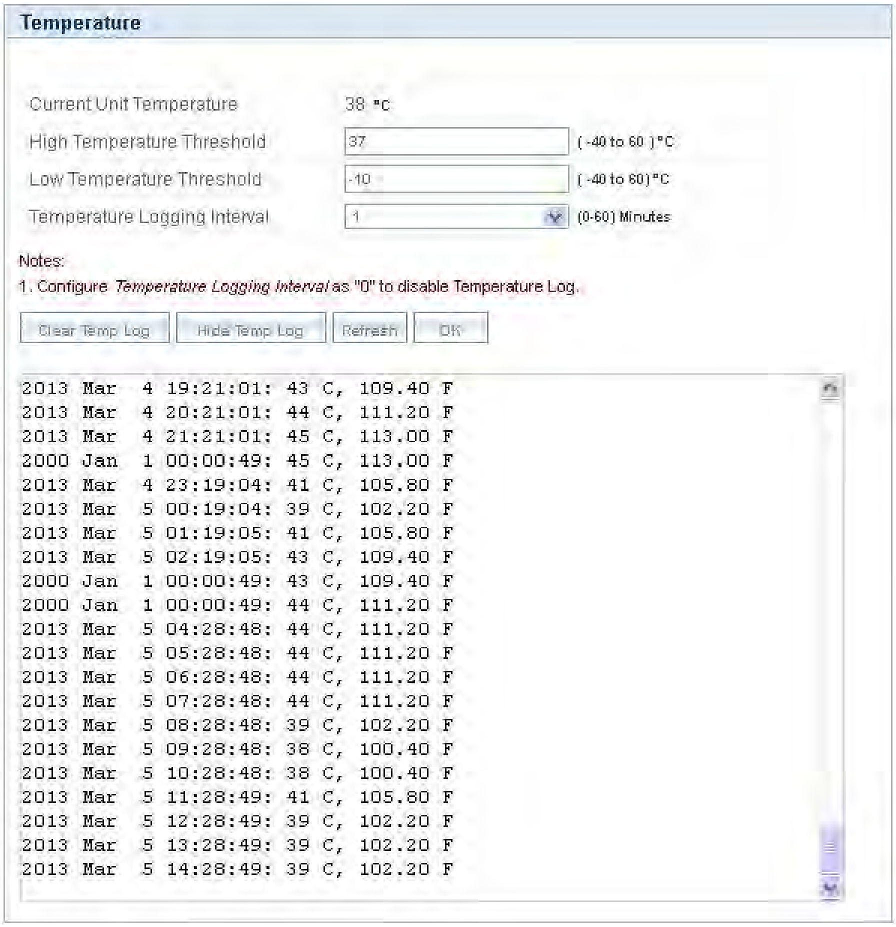
- **Current Unit Temperature**: Displays the current internal temperature of the device in Celsius.
- **High and Low Temperature Threshold**:
  - Configure the high temperature threshold ranging from -40°C to 60°C. By default, it is set to 60°C.
  - Configure the low temperature threshold ranging from -40°C to 60°C. By default, it is set to -40°C.
  - When the current internal temperature of the device reaches or exceeds this threshold range, then a trap and event message is generated for every one hour (as long as it stays in the same state). If the temperature of the device further changes, then the device will immediately generates another trap and an event message.
  - For example, lets say the configured threshold range is -30(low) to 40 (high). If the device temperature reaches 50 then a trap and event message is generated for every one hour till it remains at 50. So, when the temperature increases to 51 then it will immediately generate another trap and an event message.
- **Temperature Logging Interval**: A logging interval from 1 to 60 minutes with 5 minute increment can be selected. For example, if you configure logging interval as 10 minutes then the device temperature is logged for every 10 minutes.

: If the logging interval is configured '0', then the temperature log feature will be disabled.

- After configuring the parameters, click **OK** followed by **COMMIT**.

7.10.3.1 View Temperature Log

To view the temperature Log, click **Show Temp Log**.



Current Unit Temperature 38 °C

High Temperature Threshold 37 (-40 to 60)°C

Low Temperature Threshold -10 (-40 to 60)°C

Temperature Logging Interval 1 (0-60) Minutes

Notes:

1. Configure *Temperature Logging Interval* as "0" to disable Temperature Log.

```
2013 Mar  4 19:21:01: 43 C, 109.40 F
2013 Mar  4 20:21:01: 44 C, 111.20 F
2013 Mar  4 21:21:01: 45 C, 113.00 F
2000 Jan  1 00:00:49: 45 C, 113.00 F
2013 Mar  4 23:19:04: 41 C, 105.80 F
2013 Mar  5 00:19:04: 39 C, 102.20 F
2013 Mar  5 01:19:05: 41 C, 105.80 F
2013 Mar  5 02:19:05: 43 C, 109.40 F
2000 Jan  1 00:00:49: 43 C, 109.40 F
2000 Jan  1 00:00:49: 44 C, 111.20 F
2013 Mar  5 04:28:48: 44 C, 111.20 F
2013 Mar  5 05:28:48: 44 C, 111.20 F
2013 Mar  5 06:28:48: 44 C, 111.20 F
2013 Mar  5 07:28:48: 44 C, 111.20 F
2013 Mar  5 08:28:48: 39 C, 102.20 F
2013 Mar  5 09:28:48: 38 C, 100.40 F
2013 Mar  5 10:28:48: 38 C, 100.40 F
2013 Mar  5 11:28:49: 41 C, 105.80 F
2013 Mar  5 12:28:49: 39 C, 102.20 F
2013 Mar  5 13:28:49: 39 C, 102.20 F
2013 Mar  5 14:28:49: 39 C, 102.20 F
```

Figure 7-36 View Temperature Log

To retrieve the temperature log file from the device, see Retrieve From Device.

The maximum size of the temperature log file is 65 KB. If the file size exceeds 65 KB, then all the log messages are moved to a backup file and only the recent 100 lines are displayed in the log file. When the size of the log file exceeds again then it overwrites the backup file.

Backup files can be retrieved by using ‘retrieve’ CLI command. For more details, see **Tsunami 800 and 8000 Series Reference guide** available at http://my.proxim.com.

: Log messages can be stored in the log file approximately up to 6 days with logging interval of 5 minutes.

7.10.3.2 Hide Temperature Log

To hide the temperature log messages, click **Hide Temp Log**.

7.10.3.3 Clear Temperature Log

To clear the temperature log messages, click **Clear Temp Log**. The messages are cleared and moved to the backup file leaving the temperature log file empty. An event is generated on clearing the temperature log messages.

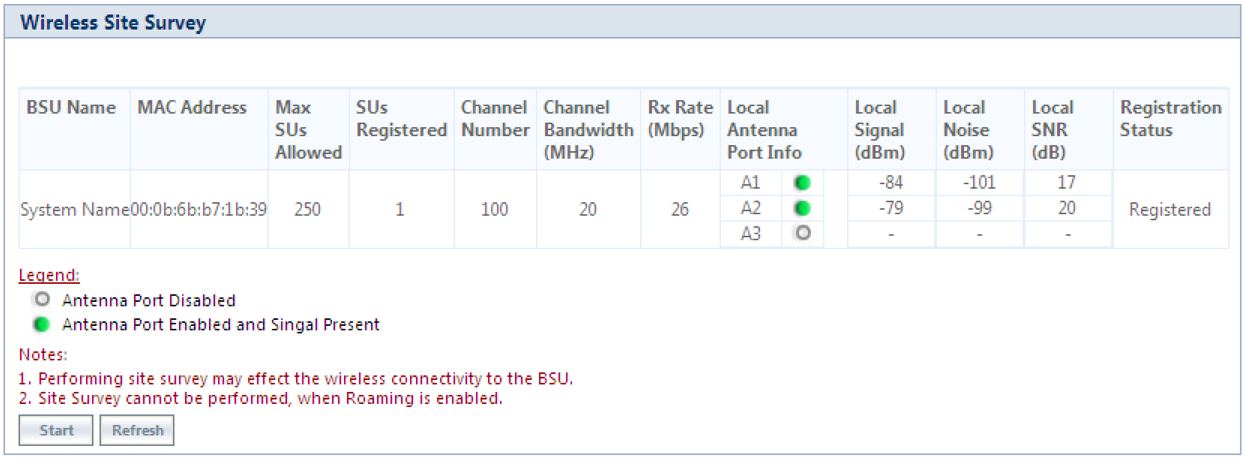
: The current and the backed up temperature logs are stored in the flash memory and can be retrieved even after device reboot.

7.11 Tools

7.11.1 Wireless Site Survey

: Applicable only to a device in SU or End Point B mode.

Wireless Site Survey is done by the SU or End Point B only. This feature scans all the available channels according to the current Channel Bandwidth, and collects information about all BSUs or Endpoint A configured with the same network name as SUs or End Point B.



Wireless Site Survey

BSU Name	MAC Address	Max SUs Allowed	SUs Registered	Channel Number	Channel Bandwidth (MHz)	Rx Rate (Mbps)	Local Antenna Port Info	Local Signal (dBm)	Local Noise (dBm)	Local SNR (dB)	Registration Status
System Name	00:0b:6b:b7:1b:39	250	1	100	20	26	A1 ●	-84	-101	17	Registered
							A2 ●	-79	-99	20	
							A3 ○	-	-	-	

Legend:

○ Antenna Port Disabled

● Antenna Port Enabled and Singal Present

Notes:

1. Performing site survey may effect the wireless connectivity to the BSU.
2. Site Survey cannot be performed, when Roaming is enabled.

Figure 7-37 Wireless Site Survey - SU Mode

To initialize the survey process, click **Start**. This process list the details of all the available BSUs or End Point A. To stop the site survey process, click Stop.

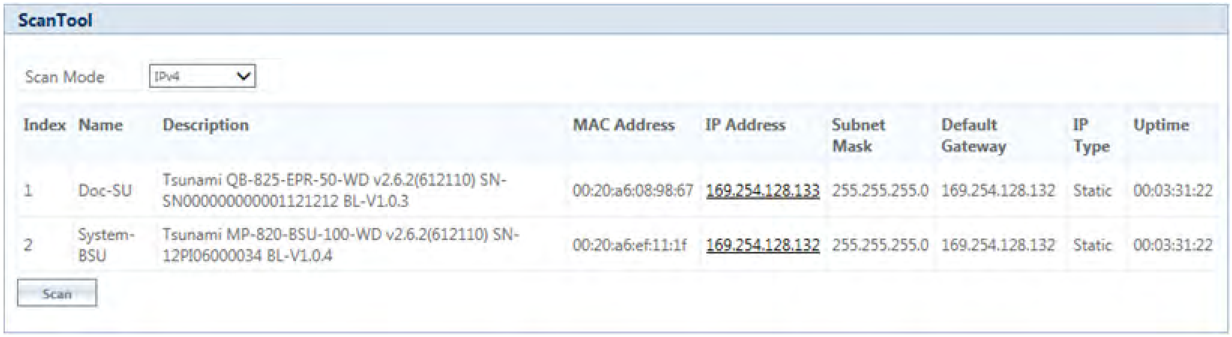
During the scan process, click **Refresh** to view the latest discovered BSU/End Point A.

: Site Survey cannot be performed, when Roaming is enabled.

7.11.2 Scan Tool

With Scan Tool, you can scan all the Proxim devices available on the network.

To scan the devices, navigate to **MONITOR** > **Tools** > **Scan Tool**. The **Scan Tool** screen appears. In the Scan Tool screen, select **Scan Mode** as **IPv4.** Click **Scan** to scan and refresh the devices on the network. The scanned devices are displayed as shown below:



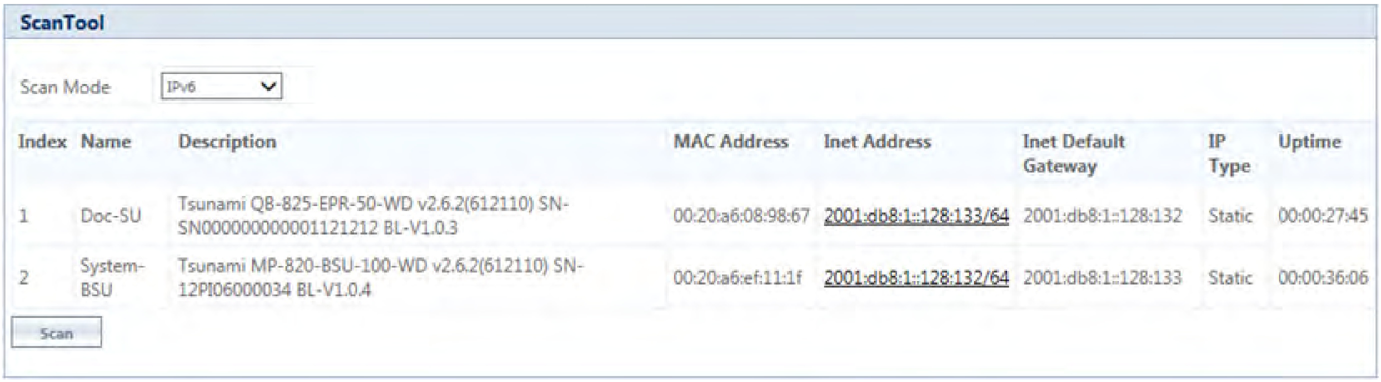
ScanTool

Scan Mode: IPv4

Index	Name	Description	MAC Address	IP Address	Subnet Mask	Default Gateway	IP Type	Uptime
1	Doc-SU	Tsunami QB-825-EPR-50-WD v2.6.2(612110) SN-SN000000000001121212 BL-V1.0.3	00:20:a6:08:98:67	169.254.128.133	255.255.255.0	169.254.128.132	Static	00:03:31:22
2	System-BSU	Tsunami MP-820-BSU-100-WD v2.6.2(612110) SN-12PI06000034 BL-V1.0.4	00:20:a6:ef:11:1f	169.254.128.132	255.255.255.0	169.254.128.132	Static	00:03:31:22

Figure 7-38 An Example - Scanned Devices (IPv4)

In the Scan Tool screen, select **Scan Mode** as **IPv6** to scan the **82x devices** with IPv6 mode. Click **Scan** to scan and refresh the devices on the network. The scanned 82x devices are displayed as shown below:



ScanTool

Scan Mode: IPv6

Index	Name	Description	MAC Address	Inet Address	Inet Default Gateway	IP Type	Uptime
1	Doc-SU	Tsunami QB-825-EPR-50-WD v2.6.2(612110) SN-SN000000000001121212 BL-V1.0.3	00:20:a6:08:98:67	2001:db8:1::128:133/64	2001:db8:1::128:132	Static	00:00:27:45
2	System-BSU	Tsunami MP-820-BSU-100-WD v2.6.2(612110) SN-12PI06000034 BL-V1.0.4	00:20:a6:ef:11:1f	2001:db8:1::128:132/64	2001:db8:1::128:133	Static	00:00:36:06

Figure 7-39 An Example - Scanned Devices (IPv6)

- *ScanTool IPv6 support is applicable only for the **82x** devices with IPv6 mode.*
- *ScanTool can display a maximum of **50** devices.*

7.11.3 sFlow®

Proxim's point-to-multipoint and point-to-point devices support sFlow® technology, developed by InMon Corporation. The sFlow® technology provides the ability to measure network traffic on all interfaces simultaneously by collecting, storing, and analyzing traffic data.

Depicted below is the sFlow architecture that consists of a sFlow Agent and a sFlow Receiver.

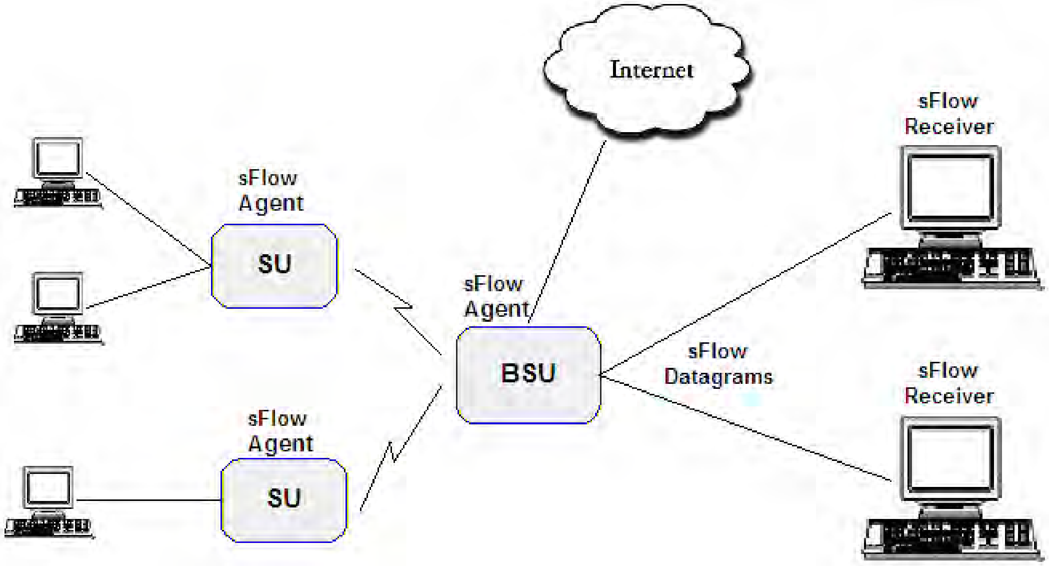


Figure 7-40 sFlow Architecture - An Example with a BSU and SUs

The **sFlow Agent**, which is running on devices, captures traffic information received on all the Ethernet interfaces, and sends sampled packets to the **sFlow Receiver** for analysis.

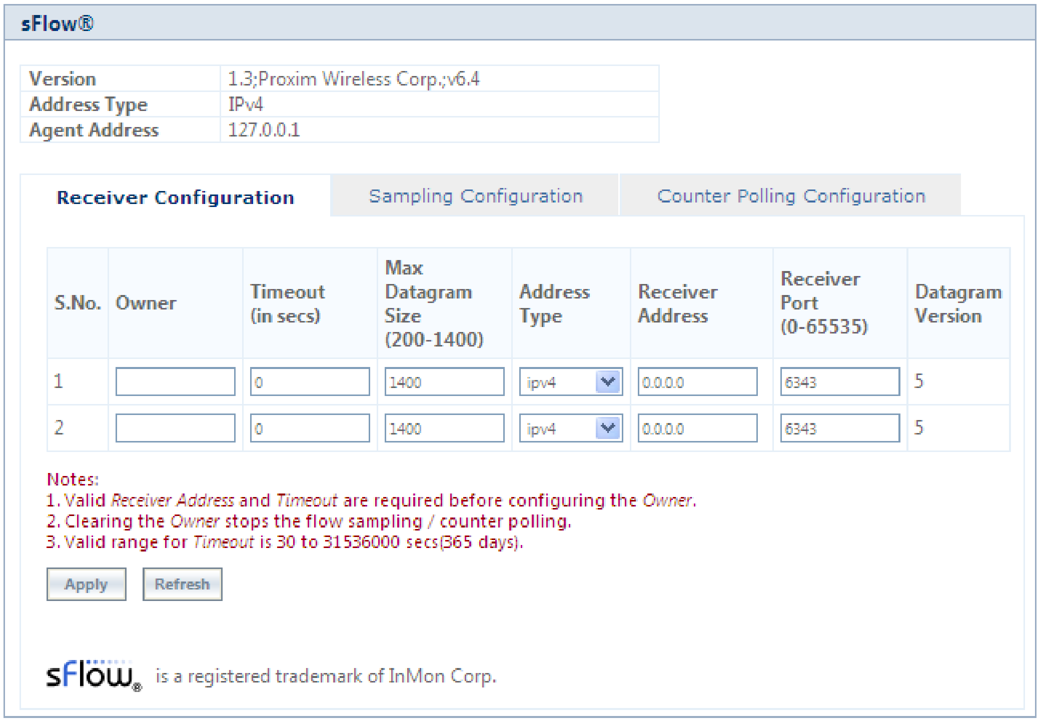
The sampling mechanism used to sample data are as follows:

- **Packet Flow Sampling**: In this sampling, the data packets received on the Ethernet interface of the device are sampled based on a counter. With each packet received, the counter is decremented. When the counter reaches zero, the packet is packaged and sent to the sFlow Receiver for analysis. These packets are referred to as Packet Flow Samples.
- **Counter Polling Sampling**: In this sampling, the sFlow Agent sends counters periodically to the sFlow Receiver based on the set polling interval. If polling interval is set to 5 seconds then the sFlow Agent sends counters to sFlow Receiver every 5 seconds. These packets are referred to as Counter Polling Samples.

The Packet Flow Samples and Counter Polling Samples are collectively sent to the sFlow Receiver as sFlow Datagrams. It is possible to enable either or both types of sampling.

sFlow Sampling effects the system performance and hence care must be taken in configuring the sFlow parameters.

To configure sFlow, navigate to **MONITOR** > **Tools** > **sFlow**. The following **sFlow®** screen appears:



sFlow®

Version	1.3;Proxim Wireless Corp.;v6.4
Address Type	IPv4
Agent Address	127.0.0.1

S.No.	Owner	Timeout (in secs)	Max Datagram Size (200-1400)	Address Type	Receiver Address	Receiver Port (0-65535)	Datagram Version
1		0	1400	ipv4	0.0.0.0	6343	5
2		0	1400	ipv4	0.0.0.0	6343	5

Notes:
1. Valid *Receiver Address* and *Timeout* are required before configuring the *Owner*.
2. Clearing the *Owner* stops the flow sampling / counter polling.
3. Valid range for *Timeout* is 30 to 31536000 secs(365 days).

sFlow® is a registered trademark of InMon Corp.

Figure 7-41 sFLOW

This screen displays the following information about the sFlow Agent:

- **Version**: The version displayed is **1.3;Proxim Wireless Corp.; v6.4**. The version comprises the following information:
  1. **sFlow MIB Version**: Indicates the agent's MIB version. The MIB specifies how the agent extracts and bundles sampled data, and the sFlow receiver must support the agent's MIB. The sFlow MIB version is 1.3. so the sFlow Receiver's version must also be at least 1.3.
  2. **Organization**: Specifies the organization implementing sFlow Agent functionality on the device, that is, **Proxim Wireless Corp.**
  3. **Revision**: Specifies the sFlow Agent version, that is, **v6.4**.
- **Address Type**: Specifies the protocol version for IP addresses.
- **Agent Address**: Specifies the sFlow Agent's IP address.

7.11.3.1 sFlow Receiver Configuration

The Receiver Configuration page allows you to configure sFlow Receiver(s), which receives samples from all agents on the network, combines and analyzes the samples to produce a report of network activity.

To configure sFlow Receiver, navigate to **MONITOR** > **Tools** > **sFlow** and select **Receiver Configuration** tab.

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

Parameter	Description
S.No.	Represents the Receiver index number. Please note that the number of indexes depends on the Ethernet interfaces your device supports.
Owner	Enter a string, which uniquely identifies the sFlow Receiver.
Time Out	Enter a value ranging from 30 to 31536000 seconds (365 days) in the **Time Out** box. The sFlow Agent sends sampled packets to the specified sFlow Receiver till it reaches zero. At zero, all the Receiver parameters are set to default values.
Max Datagram Size	Enter the maximum size of a sFlow datagram (in bytes), which the Receiver can receive, in the **Max Datagram Size** box. By default, the maximum datagram size is set to 1400 bytes. It can range from 200 to 1400 bytes.
Address Type	The address type supported by sFlow Receiver is ipv4, which is by default selected. *: Only IPv4 is currently supported.*
Receiver Address	Enter the sFlow Receiver's IP address in the **Receiver Address** box.
Receiver Port	By default, the sFlow Receiver listens to the sFlow datagrams on 6343 port. To change the port, enter a valid port ranging from 0 to 65535 in the **Receiver Port** box.
Datagram Version	The sFlow datagram version used is 5.

Click **Apply**, to save the sFlow Receiver configuration parameters.

Once the Receiver configurations are done, either Packet Flow sampling or Counter Polling Sampling or both can be started.

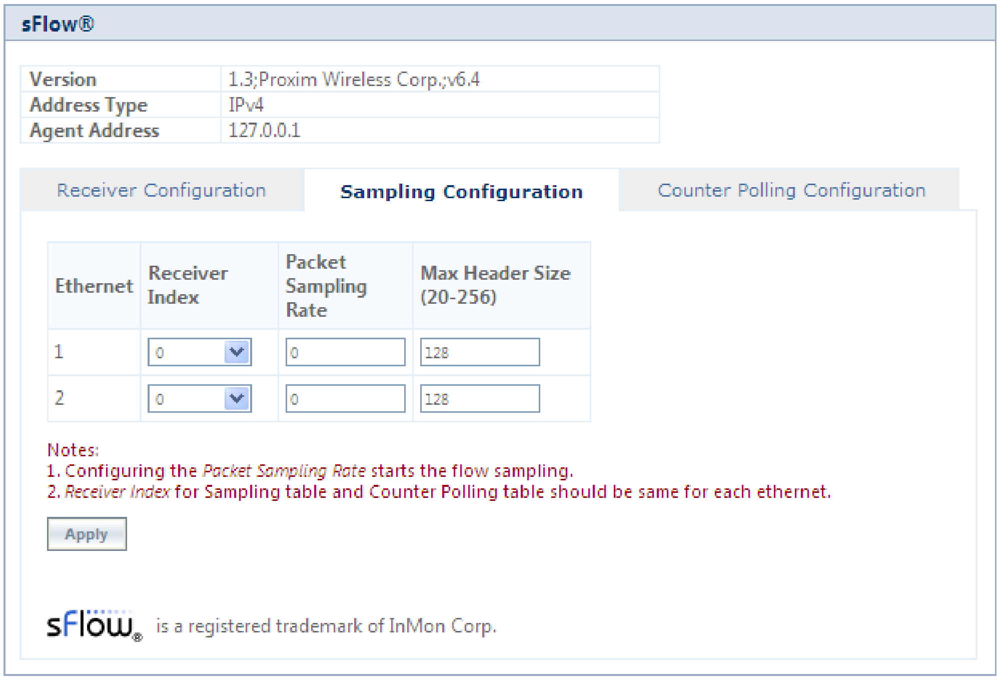
:

- *Enabling sampling effects the system performance and hence care should be taken in setting the right values for Timeout and Max Datagram Size.*
- *When the Owner string is cleared, the Flow Sampling and Counter Polling stops.*

7.11.3.2 Sampling Configuration

To configure and start packet flow sampling, do the following:

1. Navigate to **MONITOR** > **Tools** > **sFlow** and select **Sampling Configuration** tab.



sFlow®

Version	1.3;Proxim Wireless Corp.;v6.4
Address Type	IPv4
Agent Address	127.0.0.1

Ethernet	Receiver Index	Packet Sampling Rate	Max Header Size (20-256)
1	0	0	128
2	0	0	128

Notes:
1. Configuring the *Packet Sampling Rate* starts the flow sampling.
2. *Receiver Index* for Sampling table and Counter Polling table should be same for each ethernet.

sFlow® is a registered trademark of InMon Corp.

Figure 7-42 sFlow Sampling Configuration

2. From the **Receiver Index** drop-down box, select the receiver index number associated with the sFlow Receiver to which the sFlow Agent should send the sFlow Datagrams.

: If device has two Ethernet interfaces, then configure different Receiver indexes for each of the interface.

3. Type a value in the **Packet Sampling Rate** box. This value determines the number of packets the sFlow Agent samples from the total number of packets passing through the Ethernet interface of the device.
4. Type a value in the **Maximum Header Size** box, to set the amount of data (in bytes) to be included in the sFlow datagram. The sFlow Agent samples the specified number of bytes. For example, if you set the Maximum Header Size to 100, the sFlow Agent places the first 100 bytes of every sampled frame in the datagram. The value should match the size of the frame and packet header so that the entire header is forwarded. The default size is 128 bytes. The header size can range from 20 to 256 bytes.
5. Next, click **Apply** to start packet flow sampling. Once it starts, the **Time Out** parameter (see sFlow Receiver Configuration) keeps decrementing till it reaches a zero value. On reaching zero, the corresponding Receiver and Sampling values are set to default values.

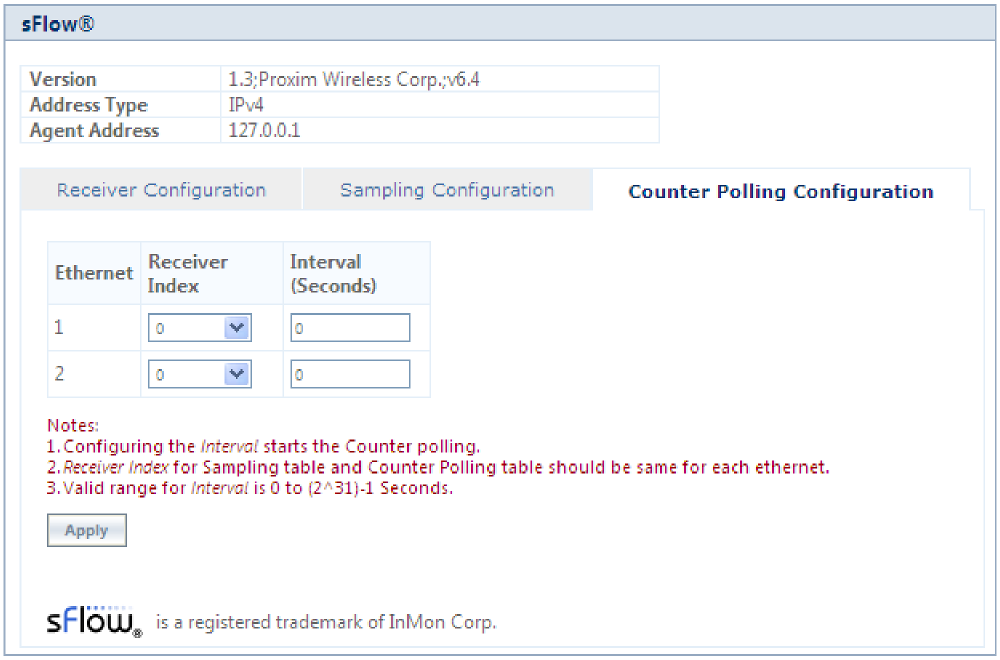
:

- *Enabling sFlow packet sampling effects the system performance, and hence care must be taken when choosing the right value for Packet Sampling Rate and Maximum Header Size.*
- *Receiver Index for packet Sampling table and Counter Polling table should be same for each Ethernet interface.*

7.11.3.3 Counter Polling Configuration

To configure and start Counter Polling sampling, do the following:

1. Navigate to **MONITOR** > **Tools** > **sFlow** and select **Counter Polling Configuration** tab.



Version	1.3;Proxim Wireless Corp.;v6.4
Address Type	IPv4
Agent Address	127.0.0.1

Ethernet	Receiver Index	Interval (Seconds)
1	0	0
2	0	0

Notes:
1. Configuring the *Interval* starts the Counter polling.
2. *Receiver Index* for Sampling table and Counter Polling table should be same for each ethernet.
3. Valid range for *Interval* is 0 to (2^31)-1 Seconds.

is a registered trademark of InMon Corp.

Figure 7-43 Counter Polling Configuration

2. From the **Receiver Index** drop-down box, choose the receiver index number associated with the sFlow Receiver to which the sFlow Agent sends the counters.

: If Packet Flow Sampling is already configured and running, then you should configure the Receiver index same as configured in the Packet Flow Sampling for each Ethernet interface.

3. Set the polling interval by typing a value in the **Interval** box. Lets say, the polling interval is set to 30 seconds. So for every 30 seconds, the counters are collected and send to the sFlow Receiver. The valid range for polling interval is 0 to 2^{31} - 1 seconds.
4. Next, click **Apply** to start Counter Polling Sampling. Once it starts, the **Time Out** parameter (see sFlow Receiver Configuration) keeps decrementing till it reaches a zero value. On reaching zero, the corresponding Receiver and Counter Polling values are set to default values.

- *Enabling sFlow counter sampling effects the system performance, and hence care must be taken when choosing the right value sampling interval.*
- *Receiver Index for packet Sampling table and Counter Polling table should be same for each Ethernet interface.*
- *If a sampling starts and there is already another sampling running then we consider the time out value of the current/already running sampling.*

7.11.4 Console Commands

The **Console Commands** feature helps Proxim's Technical Support team to debug field issues.

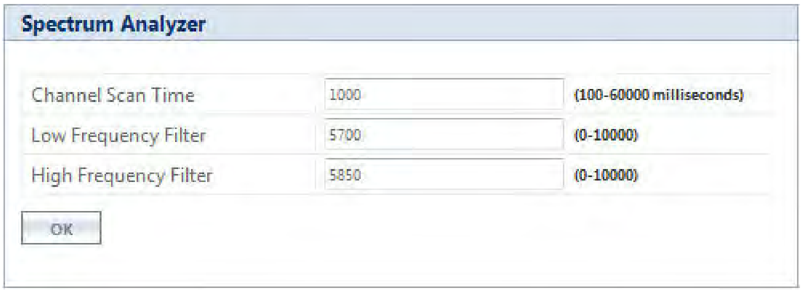
7.11.5 Spectrum Analyzer

Spectrum Analyzer helps to analyze a spectrum for interference, and select a relatively low interference channel. This tool is not a replacement for the commercial Spectrum Analyzers as this is only intended to help with channel selection and diagnose performance issues.

: *Only an administrator user can use Spectrum Analyzer to scan the spectrum. However, the Monitor user can view the last scanned results.*

To scan all the channels in the configured frequency domain, do the following:

- Navigate to **MONITOR > Tools > Spectrum Analyzer**. The following **Spectrum Analyzer** screen appears:



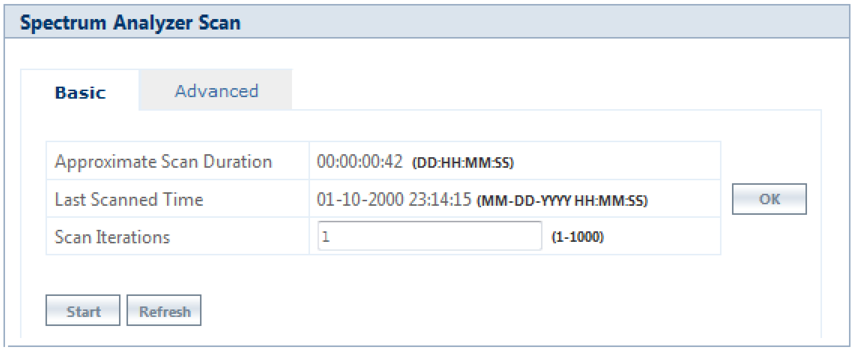
Spectrum Analyzer

Channel Scan Time	1000	(100-60000 milliseconds)
Low Frequency Filter	5700	(0-10000)
High Frequency Filter	5850	(0-10000)

Figure 7-44 Spectrum Analyzer

  - **Channel Scan Time**: Enter the time (ranging from 100 to 60000 milliseconds) to scan each channel. By default, the scan time is set to 1000 milliseconds.
  - **Low Frequency Filter & High Frequency Filter**: Enter the appropriate low and high frequency filter values to limit the number of channels to scan.
  - Next, click **OK**.

- Navigate to **Spectrum Analyzer > Scan**. The following **Spectrum Analyzer Scan** screen appears. In this screen, you can either select **Basic** or **Advanced** tab.



Spectrum Analyzer Scan

Approximate Scan Duration	00:00:00:42 (DD:HH:MM:SS)
Last Scanned Time	01-10-2000 23:14:15 (MM-DD-YYYY HH:MM:SS)
Scan Iterations	1 (1-1000)

Figure 7-45 Spectrum Analyzer Scan

:

- *The total duration of scan depends on the number of channels available, channel scan time and scan iterations.*
- *While scanning, Spectrum Analyzer does not consider channel offset.*
- *Spectrum Analyzer detects only 802.11 modulated signals.*
- *A minor variation in Spectrum Analyzer results can be expected due to the following reasons: variation in the radio properties between various device models and Satellite Density Configuration.*

:

- ***When the Spectrum Analyzer starts, the wireless link, if established, is terminated and re-established after the scan is completed.***
- ***As the wireless link is down during spectrum analysis, the remote device cannot be accessed. Hence, if Spectrum Analyzer is started on a remote device, the results will not be available until spectrum scan is completed and wireless link gets re-established.***

7.11.5.1 Basic Mode

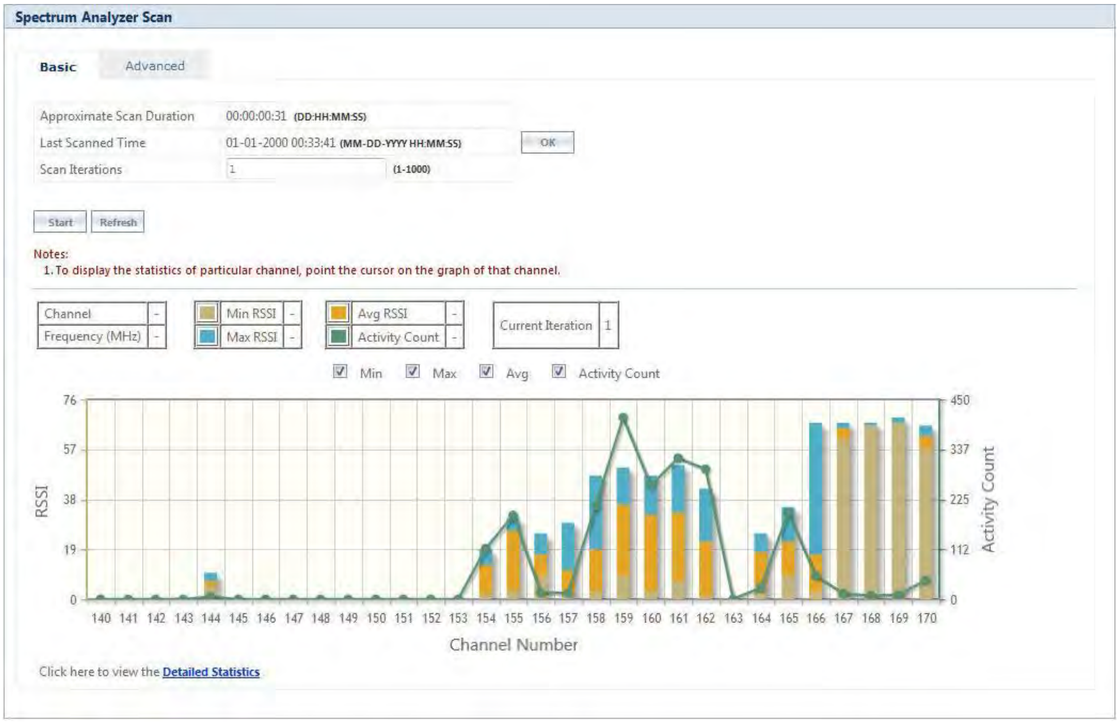
This mode helps to collect SNR and packet statistics report. The parameters under the **Basic** tab are described and tabulated below:

Parameter	Description
Approximate Scan Duration	This parameter displays the total time (dd:hh:mm:ss) required to complete the scan.
Last Scanned Time	This parameter displays the time at which the last spectrum scan was done.
Scan Iterations	This parameter specifies the number of times the scan iterates. By default, the scan iteration is set to **1**. The configurable value can range from **1** - **1000**.

After configuring the Scan iteration value, click **OK**. Next, click **Start**, to scan. The scanned results are displayed in the form of a graph as follows:

:

- *The frequencies are scanned by 5MHz slice starting from the lower edge of the frequency filter, and displays the results captured at that particular instance.*
- *When working in a high interference network, ensure to run the spectrum analyzer with multiple iterations (increase the Scan Time) to get accurate results.*



Spectrum Analyzer Scan

Approximate Scan Duration	00:00:00:31 **(DD:HH:MM:SS)**	
Last Scanned Time	01-01-2000 00:33:41 **(MM-DD-YYYY HH:MM:SS)**	OK
Scan Iterations	1 **(1-1000)**	

Notes:
1. To display the statistics of particular channel, point the cursor on the graph of that channel.

Channel	-	▨ Min RSSI	-	🟧 Avg RSSI	-	Current Iteration	1
Frequency (MHz)	-	🟦 Max RSSI	-	🟩 Activity Count	-		

☑ Min ☑ Max ☑ Avg ☑ Activity Count

Click here to view the Detailed Statistics

Figure 7-46 An Example - Scanned Results (Basic Mode)

Graph Results Interpretation

Consider a network with a device operating on channel 159 with 20 MHz channel bandwidth. In the same vicinity, when we run the Spectrum Analyzer on a Tsunami radio it will display the results as shown in Figure 7-46. From the results, we see interfering signals on channels 153 to 170. It also shows strong interfering signal on channels 157 to163 indicating the presence of a device operating on channel 159, and moderate interfering signals on channels 153-156 and 164-166 (which are side band signals from the same interference source).

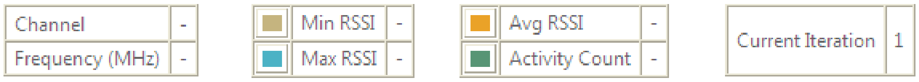
We recommend to avoid using these channels while installing Tsunami products, otherwise radio will report huge PHY and CRC errors. However, to make these channels usable and to ignore the low interference signals, we recommend configuring Satellite Density on the devices.

By default, for each channel, the graph represents the following statistics:

Parameter	Description	Legend
Maximum RSSI	Represents the maximum RSSI of all the signals received during the scan on a given channel.	🟦
Minimum RSSI	Represents the minimum RSSI of all the signals received during the scan on a given channel.	🟫
Average RSSI	Represents the average RSSI of all the signals received during the scan on a given channel.	🟧
Activity Count	Represents the total wireless activities (including OFDM Signal and Errors) during the scan on a given channel.	🟩

Please note that the **Current Iteration** parameter helps to learn the current scan iteration. For example, if **Scan Iteration** is configured as 2, and currently only one scan cycle is complete then Current Iteration parameter displays 1.

To view the statistics of a particular channel, point the cursor to that channel on the graph. The statistics is displayed as shown below:



Channel -
Frequency (MHz) -

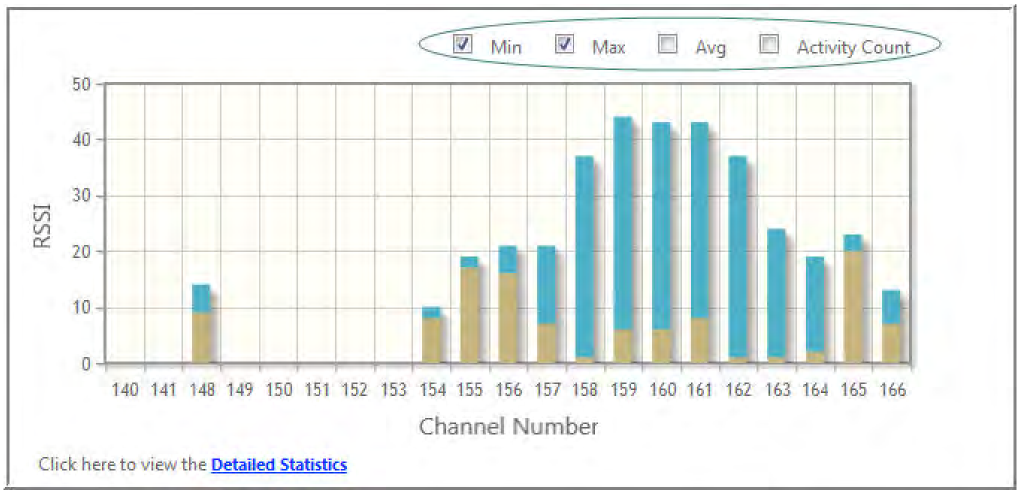
🟫 Min RSSI -
🟦 Max RSSI -

🟧 Avg RSSI -
🟩 Activity Count -

Current Iteration 1

Figure 7-47 Channel Statistics

It is also possible to view only the selected statistics on the graph. For example, to view only Minimum and Maximum RSSI on the graph, uncheck the box against **Activity Count** and **Avg** on the top of the graph.



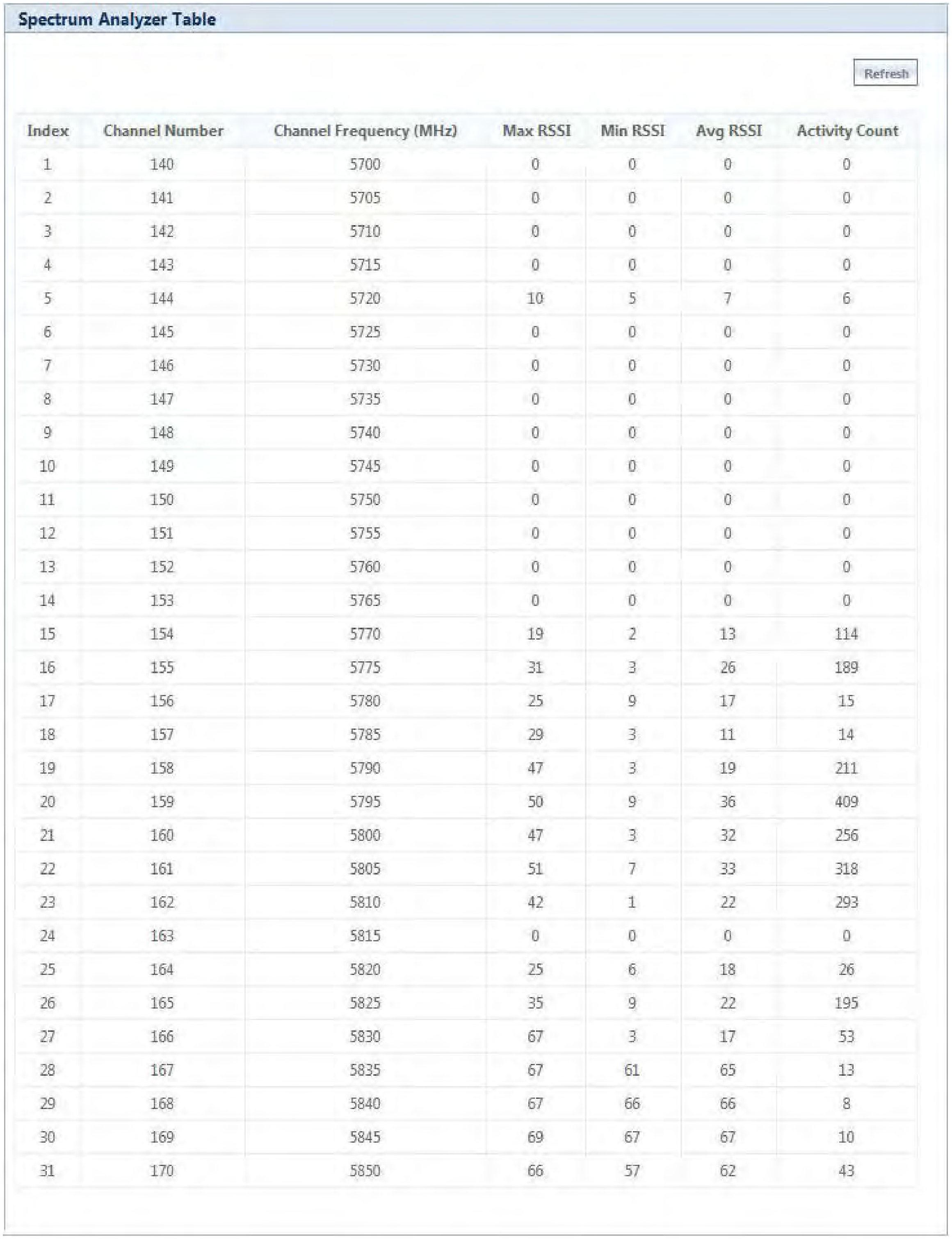
☑ Min ☑ Max □ Avg □ Activity Count

Click here to view the Detailed Statistics

Figure 7-48 An Example - Selective Graph Statistics

At a time, the graph represents the statistics of a maximum of 32 channels. To view the graph(s) of the remaining channels, click **Next** (available on the upper right corner of the graph). Click **Previous** to view the statistics of the previous channels.

To view the tabular format of the graph statistics, click **Detailed Statistics** on the bottom left of the graph. The detailed statistics is displayed as follows:



Spectrum Analyzer Table

Index	Channel Number	Channel Frequency (MHz)	Max RSSI	Min RSSI	Avg RSSI	Activity Count
1	140	5700	0	0	0	0
2	141	5705	0	0	0	0
3	142	5710	0	0	0	0
4	143	5715	0	0	0	0
5	144	5720	10	5	7	6
6	145	5725	0	0	0	0
7	146	5730	0	0	0	0
8	147	5735	0	0	0	0
9	148	5740	0	0	0	0
10	149	5745	0	0	0	0
11	150	5750	0	0	0	0
12	151	5755	0	0	0	0
13	152	5760	0	0	0	0
14	153	5765	0	0	0	0
15	154	5770	19	2	13	114
16	155	5775	31	3	26	189
17	156	5780	25	9	17	15
18	157	5785	29	3	11	14
19	158	5790	47	3	19	211
20	159	5795	50	9	36	409
21	160	5800	47	3	32	256
22	161	5805	51	7	33	318
23	162	5810	42	1	22	293
24	163	5815	0	0	0	0
25	164	5820	25	6	18	26
26	165	5825	35	9	22	195
27	166	5830	67	3	17	53
28	167	5835	67	61	65	13
29	168	5840	67	66	66	8
30	169	5845	69	67	67	10
31	170	5850	66	57	62	43

Figure 7-49 An Example - Detailed Statistics

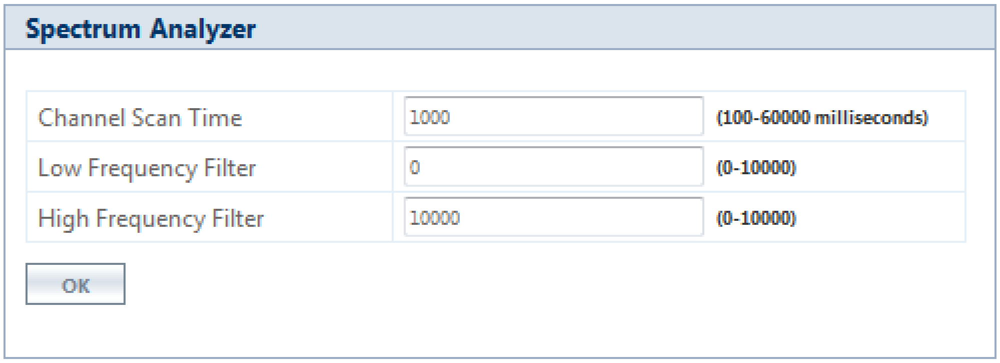
7.11.5.2 Advanced

This mode helps to scan the user configured bandwidth to identify the other devices operating on different channels. This displays the device information such as Bandwidth, Channel Number, MAC Address, System Name, Mode, Encryption, SNR, and Packet count along with the information provided in Basic scanning mode.

:

- *The frequencies are scanned based on the configured Scan Bandwidth slice starting from the lower edge of the frequency filter, and displays the results captured at that particular instance.*
- *By default, the scan iteration is always **1** in Advanced scanning mode.*

For example, let us consider the configuration values shown in the **Spectrum Analyzer** screen given below:

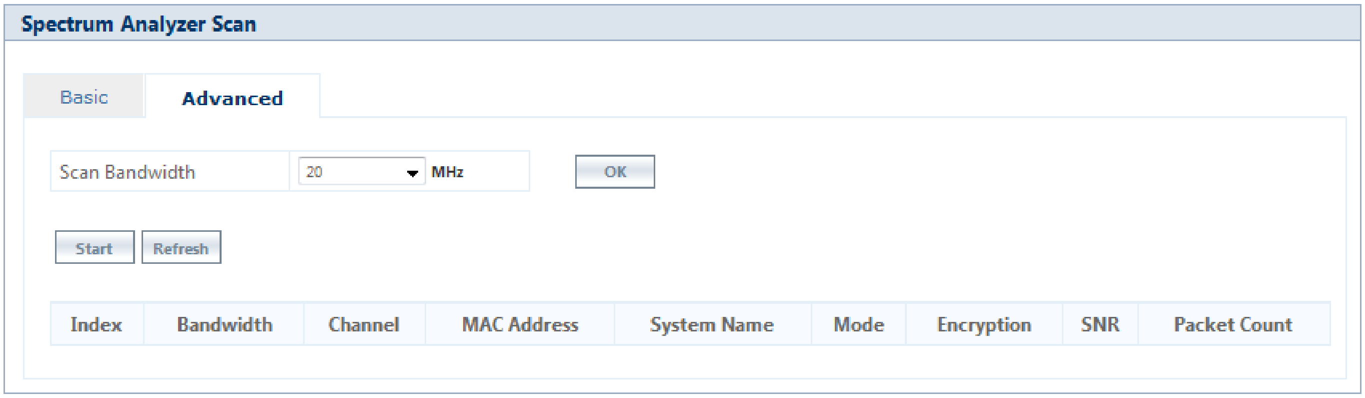


Spectrum Analyzer

Channel Scan Time	1000	(100-60000 milliseconds)
Low Frequency Filter	0	(0-10000)
High Frequency Filter	10000	(0-10000)

Figure 7-50 An Example - Spectrum Analyzer

Next, navigate to **Spectrum Analyzer > Scan**. Select the **Advance** tab and the following **Spectrum Analyzer Scan** screen appears.



Spectrum Analyzer Scan

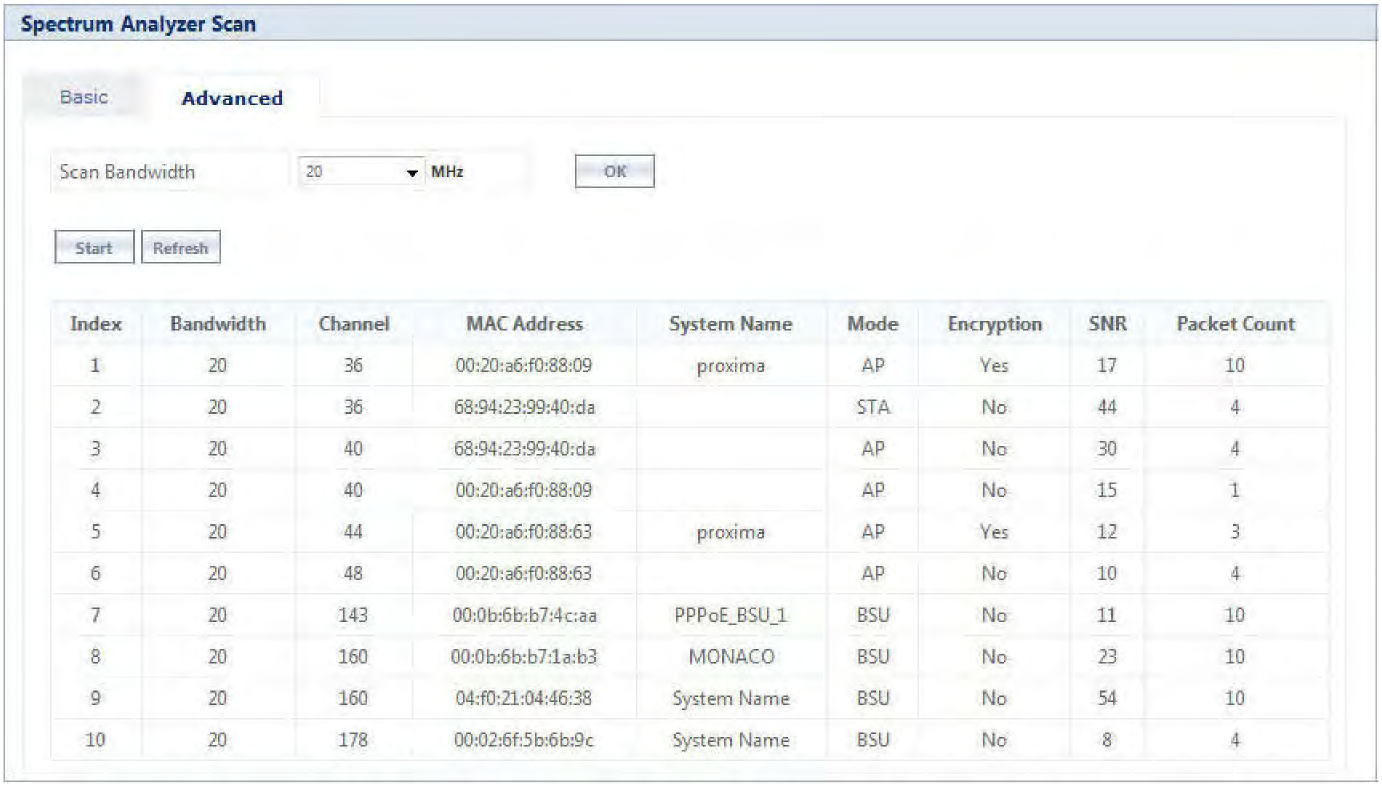
Scan Bandwidth: 20 MHz

Index	Bandwidth	Channel	MAC Address	System Name	Mode	Encryption	SNR	Packet Count

Figure 7-51 An Example - Spectrum Analyzer Scan (Advance Mode)

- **Scan Bandwidth**: Select the appropriate bandwidth from the drop-down menu and click **OK**.
- Next, click the **Start** button to scan.

The scanned results for the detected devices are displayed as shown below:



Scan Bandwidth 20 MHz

Index	Bandwidth	Channel	MAC Address	System Name	Mode	Encryption	SNR	Packet Count
1	20	36	00:20:a6:f0:88:09	proxima	AP	Yes	17	10
2	20	36	68:94:23:99:40:da		STA	No	44	4
3	20	40	68:94:23:99:40:da		AP	No	30	4
4	20	40	00:20:a6:f0:88:09		AP	No	15	1
5	20	44	00:20:a6:f0:88:63	proxima	AP	Yes	12	3
6	20	48	00:20:a6:f0:88:63		AP	No	10	4
7	20	143	00:0b:6b:b7:4c:aa	PPPoE_BSU_1	BSU	No	11	10
8	20	160	00:0b:6b:b7:1a:b3	MONACO	BSU	No	23	10
9	20	160	04:f0:21:04:46:38	System Name	BSU	No	54	10
10	20	178	00:02:6f:5b:6b:9c	System Name	BSU	No	8	4

Figure 7-52 An Example - Spectrum Analyzer Scanned Results (Advance Mode)

The device information displayed in **Advance** Scanning mode are described and tabulated below.

Parameter	Description
Bandwidth	This parameter displays Bandwidth of the detected device.
Channel Number	This parameter displays the channel number on which the detected device is operating.
MAC Address	This parameter displays the MAC Address of the detected device.
System Name	This parameter displays either the Device Name or the SSID of the detected device.
Mode	This parameter displays the Mode of the detected device. • **BSU**: Base Station Unit • **SU**: Subscriber Unit • **AP**: Access Point • **STA**: Station
Encryption	This parameter indicates whether encryption is enabled on the detected device.
SNR	This parameter displays the Signal-to-Noise Ratio (SNR) value of the detected device in the scanned channel.
Packet Count	This parameter displays the Packet Count for the detected device.

7.11.6 Radio Link Test Tool

: *It is applicable to* ***82x / 8xxx*** *devices.*

In general, whenever the network has some performance issue, it is required to identify whether the issue is due to the wireless link or due to other network parameters. The Radio Link Test (RLT) tool helps to measure and diagnose any performance issues in the wireless link. At MAC level, this tool internally generates the traffic between the two radios, monitors the traffic, and generates a test report.The test report will help in analyzing the wireless link performance and other related issues such as interference, lower throughput, and wireless errors. Especially for the static link establishment, this is very helpful to check the link between the two radios when installing for the first time or if any performance issues are noticed after the installation. If the link between the radios is of expected quality, then there is no issue with the wireless link. In case, if there is any issue due to wireless parameters, the link may need some tuning in configuration such as channel, Data Rate, Tx power or distance between the radios. In spite of all the testing and tuning, if the performance still fails to improve, then it may be due to installation related issues such as antenna alignment or the physical path. In the worst case, it may be a hardware related issue.

:

- *This is not a replacement for other wireless performance measuring tools and should be used in conjunction with other tools like Iperf or any other commercial tools.*
- *It is recommended to use this tool with caution on live networks as it will be generating internal traffic which may impact the network performance.*
- *Radio Link test is an experimental feature and will be improved in future releases.*
- *This tool can be accessed through web interface, console commands, and CLI.*
- *Both ends of a link cannot simultaneously run this test.*

7.11.6.1 Configuration Options

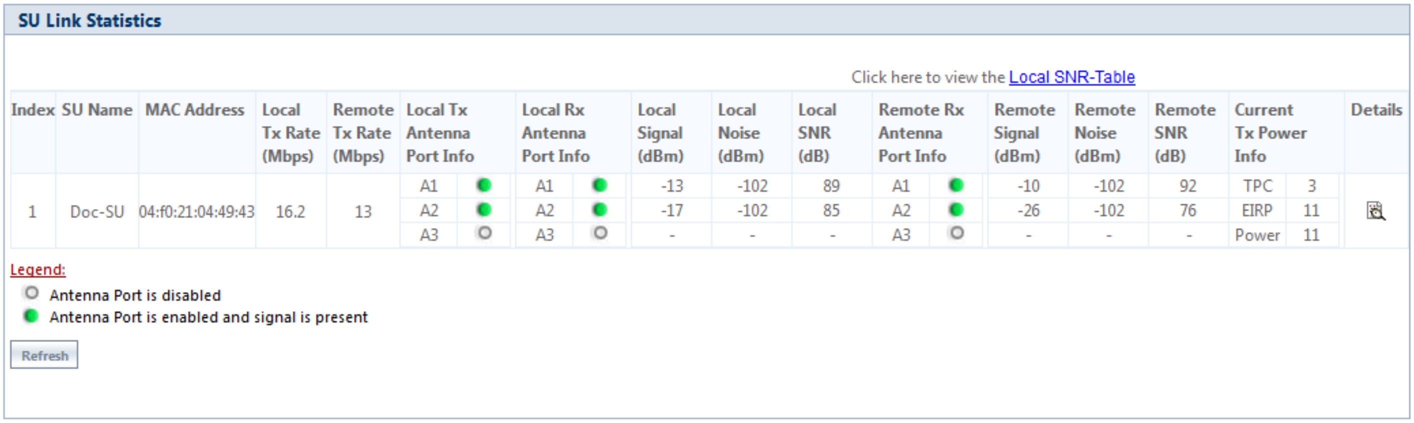
The configuration options for the Radio Link Test tool are tabulated below:

Parameter	Description
Test Duration	Time duration for which the Radio Link Test is performed (Default: 60 seconds)
Traffic Direction	Direction of the traffic (Downlink/Uplink /Bi-directional)
Traffic Rate	Amount of traffic to be generated (K bps)
Periodic Report Interval	Time interval in which the report is presented to the user interface (seconds)
Packet Size	Generate packet size (Default value: 1500 bytes)
MAC Address	Wireless MAC address of the device running in server mode
Verbose Mode	Detailed statistics information
Help	List of possible options (Usage)
Version	Display tool version information

:

- *The following parameters can also be configured/modified through Console commands and CLI:* ***Test Duration, Traffic Rate, Periodic Packet Interval,*** *and* ***Packet Size.***
- *Please refer* rlt Command Options *section for detailed explanation of* ***rlt*** *commands.*

To access this tool through web interface, navigate to **MONITOR > WORP Statistics > Interface 1 > BSU/SU Link Statistics > Details.** Click as shown in An Example - SU Link Statistics.



SU Link Statistics

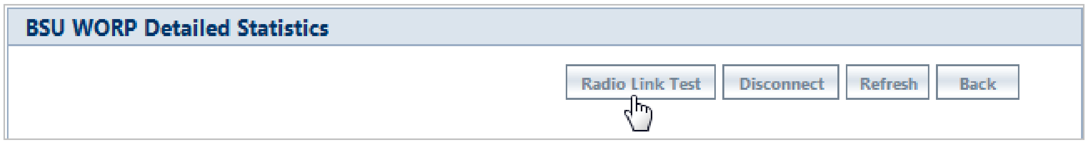
Click here to view the Local SNR-Table

Index	SU Name	MAC Address	Local Tx Rate (Mbps)	Remote Tx Rate (Mbps)	Local Tx Antenna Port Info		Local Rx Antenna Port Info		Local Signal (dBm)	Local Noise (dBm)	Local SNR (dB)	Remote Rx Antenna Port Info		Remote Signal (dBm)	Remote Noise (dBm)	Remote SNR (dB)	Current Tx Power Info		Details
1	Doc-SU	04:f0:21:04:49:43	16.2	13	A1	●	A1	●	-13	-102	89	A1	●	-10	-102	92	TPC	3	
					A2	●	A2	●	-17	-102	85	A2	●	-26	-102	76	EIRP	11	
					A3	○	A3	○	-	-	-	A3	○	-	-	-	Power	11	

Legend:
- ○ Antenna Port is disabled
- ● Antenna Port is enabled and signal is present

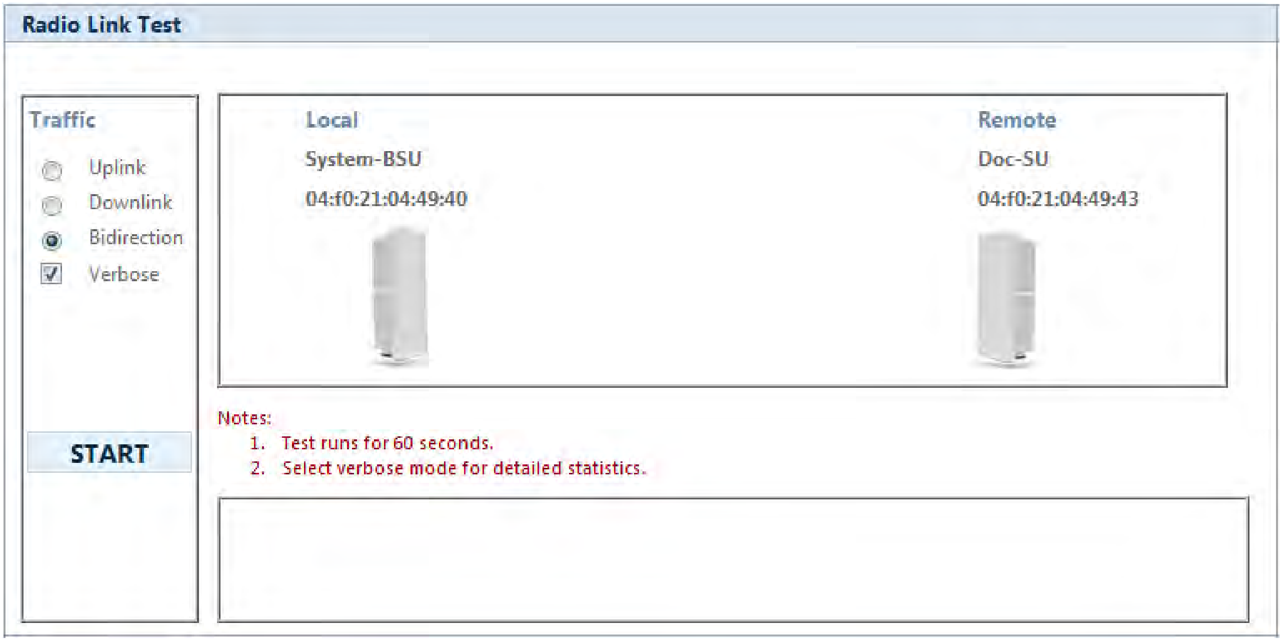
Figure 7-53 An Example - SU Link Statistics

The following **BSU/SU WORP Detailed Statistics** screen appears.



BSU WORP Detailed Statistics

Click the **Radio Link Test** Button. The following **Radio Link Test** screen appears.



Radio Link Test

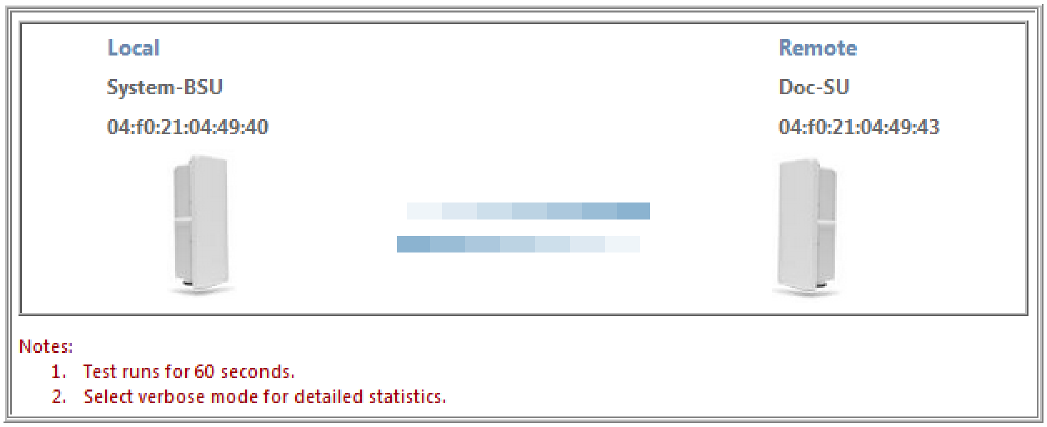
Traffic
- ○ Uplink
- ○ Downlink
- ● Bidirection
- ☑ Verbose

Local	Remote
System-BSU	Doc-SU
04:f0:21:04:49:40	04:f0:21:04:49:43

Notes:
1. Test runs for 60 seconds.
2. Select verbose mode for detailed statistics.

Figure 7-54 Radio Link Test Tool

In the Radio Link Test screen, you can select the required type of traffic from the given options namely **Uplink**, **Downlink**, and **Bidirection**. By selecting **Verbose** along with any one of the traffic options, you can get a detailed test report for the traffic selected. In the above screen, for example, select **Bidirection** and **Verbose**. Next, click the **START** button.



Local
System-BSU
04:f0:21:04:49:40

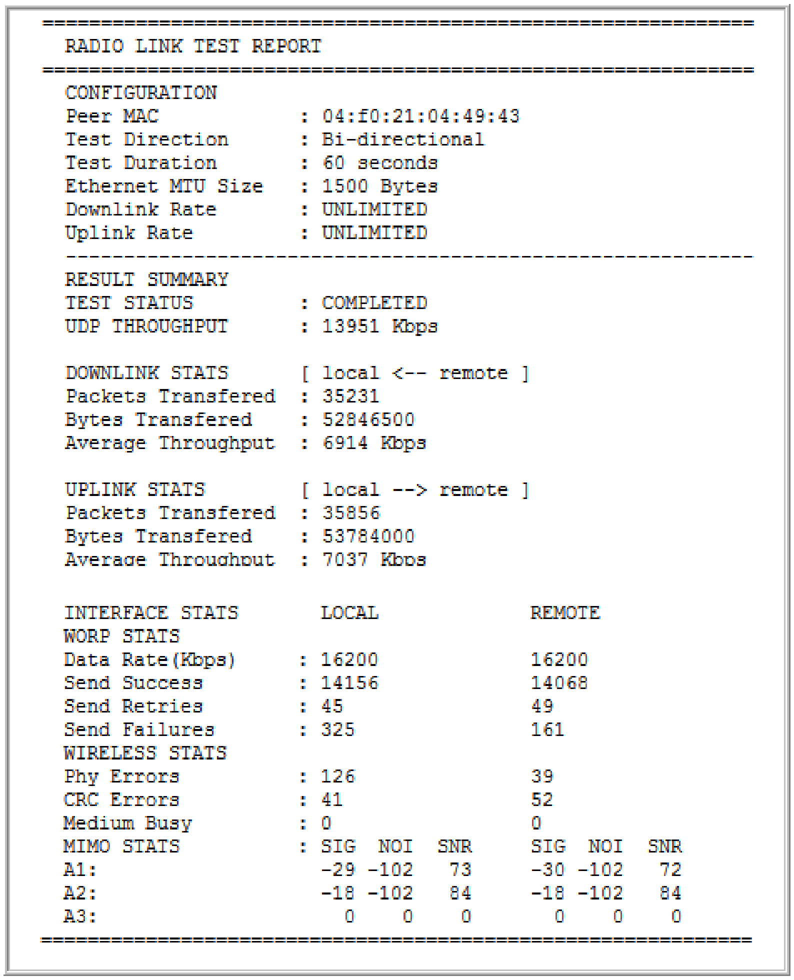
Remote
Doc-SU
04:f0:21:04:49:43

Notes:

1. Test runs for 60 seconds.
2. Select verbose mode for detailed statistics.

Figure 7-55 An Example - Radio Link Test (Bidirectional Traffic with Verbose mode)

The test runs for 60 seconds and displays the Radio Link Test Report as shown below.



```
==============================================================
  RADIO LINK TEST REPORT
==============================================================
  CONFIGURATION
  Peer MAC             : 04:f0:21:04:49:43
  Test Direction       : Bi-directional
  Test Duration        : 60 seconds
  Ethernet MTU Size    : 1500 Bytes
  Downlink Rate        : UNLIMITED
  Uplink Rate          : UNLIMITED
  ------------------------------------------------------------
  RESULT SUMMARY
  TEST STATUS          : COMPLETED
  UDP THROUGHPUT       : 13951 Kbps

  DOWNLINK STATS       [ local <-- remote ]
  Packets Transfered   : 35231
  Bytes Transfered     : 52846500
  Average Throughput   : 6914 Kbps

  UPLINK STATS         [ local --> remote ]
  Packets Transfered   : 35856
  Bytes Transfered     : 53784000
  Average Throughput   : 7037 Kbps

  INTERFACE STATS        LOCAL             REMOTE
  WORP STATS
  Data Rate(Kbps)      : 16200             16200
  Send Success         : 14156             14068
  Send Retries         : 45                49
  Send Failures        : 325               161
  WIRELESS STATS
  Phy Errors           : 126               39
  CRC Errors           : 41                52
  Medium Busy          : 0                 0
  MIMO STATS           : SIG  NOI  SNR     SIG  NOI  SNR
  A1:                    -29 -102   73     -30 -102   72
  A2:                    -18 -102   84     -18 -102   84
  A3:                      0    0    0       0    0    0
==============================================================
```

Figure 7-56 An Example - Test Report (Bidirectional Traffic with Verbose mode)

7.11.6.2 Statistics Options

The test report can be analyzed by using the statistics options tabulated below:

Parameter	Description
Traffic Statistics	
Tx Packets	Total packets transmitted from the moment user initiated the test.
Rx Packets	Total packets received from the moment user initiated the test.
Lost Packets	Packets lost due to any reason.
Duplicated Packets	Number of packets received in duplicate for the already received packets.
Tx Rate	The rate at which the packets are sent.
Rx Rate	The rate at which the packets are received.
Wireless Statistics	
Phy Errors	Total number of error packets received from the moment user initiated the test . The possible reasons: • It indicates the interference in the wireless medium • Low signal level
CRC Errors	Number of packets received with invalid CRC. The possible reasons: • It indicates the interference in the wireless medium • Low signal level
Medium Busy	Number of times the radio detected busy medium while trying to transmit the frame. This could be due to interference on that specific channel.
WORP Statistics	
Send success	Refers to the number of data messages sent and acknowledged by the peer successfully.
Send failure	Refers to the number of data messages that are not acknowledged by the peer even after the specified number of retransmissions.
Send retires	Refers to the number of data messages that are re-transmitted and acknowledged by the peer successfully.
Receive success	Refers to the number of data messages received and acknowledged successfully.
Receive failures	Refers to the number of successfully received re-transmitted data messages.
Receive retires	Refers to the number of data messages that were not received successfully.
Signal Statistics	

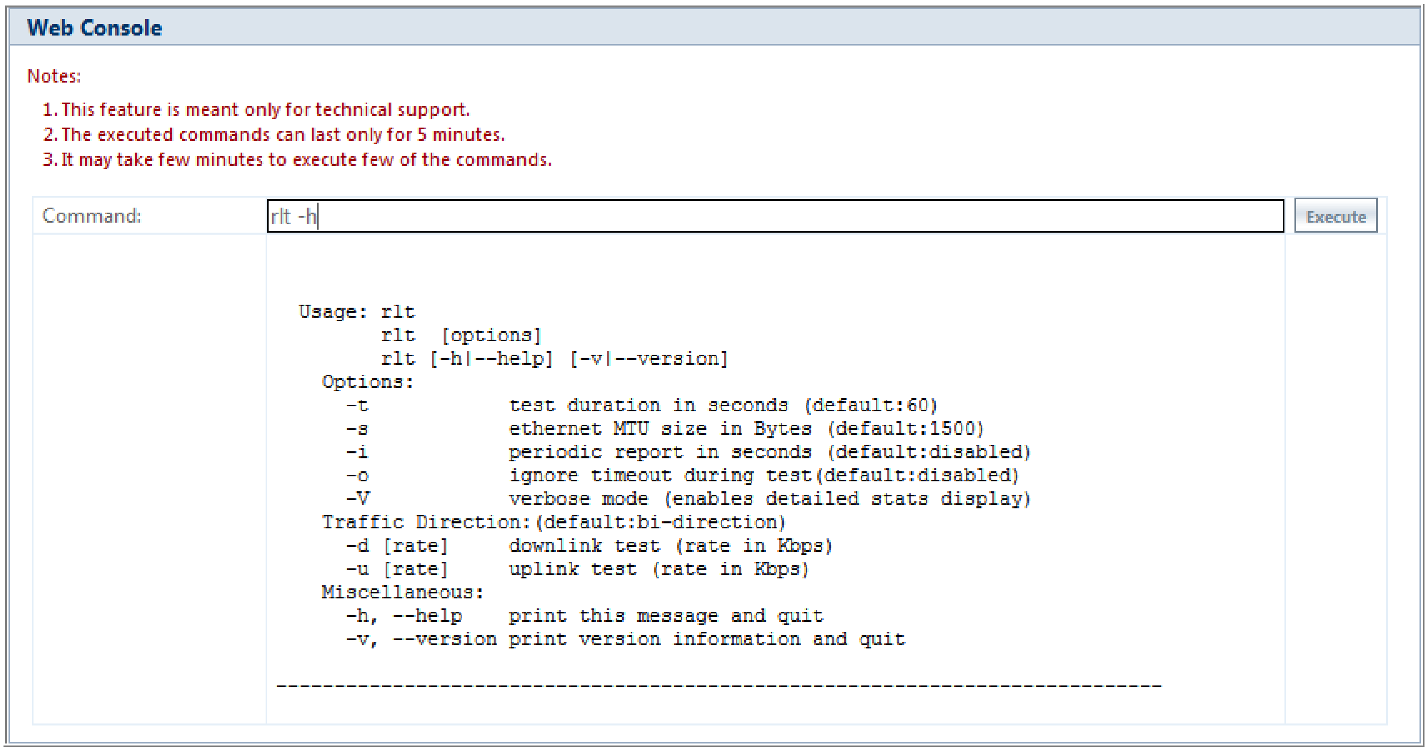
Parameter	Description
Signal	Signal measured at the radio port
Noise	Noise detected at the radio port
SNR	Signal to Noise Ratio (dB)

7.11.6.3 rlt Command Options

Using the **rlt** command options tabulated below, you run the radio link test tool through **Web Console**.

Options	Description
-t	Test duration (Default: 60 seconds)
-i	Periodic report display interval (Default: 0 - disabled)
-s	Packet size (Default: 1500 bytes)
-o	Ignore timeout during test (Default: do not ignore)
Traffic Direction	
-d	Downlink throughput test with specified traffic rate in K bps (Default: Unlimited)
-u	Uplink throughput test with specified traffic rate in K bps (Default: Unlimited)
No option	Default: Bi-Directional test with unlimited rate
Miscellaneous	
-h, --help	Tool usage
-v, --version	Tool version number
-V	Verbose mode (Enables detailed statistics display)
The “-i” option to display the test report at regular intervals works only with the “-V” verbose option for all traffic directions.	

To access this tool through **Web Console**, navigate to **MONITOR > Tools** > **Console Commands**. In the **Web Console** screen do the following:



Web Console

Notes:

1. This feature is meant only for technical support.
2. The executed commands can last only for 5 minutes.
3. It may take few minutes to execute few of the commands.

Command: rlt -h

```
Usage: rlt
       rlt  [options]
       rlt [-h|--help] [-v|--version]
  Options:
    -t            test duration in seconds (default:60)
    -s            ethernet MTU size in Bytes (default:1500)
    -i            periodic report in seconds (default:disabled)
    -o            ignore timeout during test(default:disabled)
    -V            verbose mode (enables detailed stats display)
  Traffic Direction:(default:bi-direction)
    -d [rate]     downlink test (rate in Kbps)
    -u [rate]     uplink test (rate in Kbps)
  Miscellaneous:
    -h, --help    print this message and quit
    -v, --version print version information and quit

---------------------------------------------------------------------------
```

Figure 7-57 An Example - Radio Link Test Through Web Console

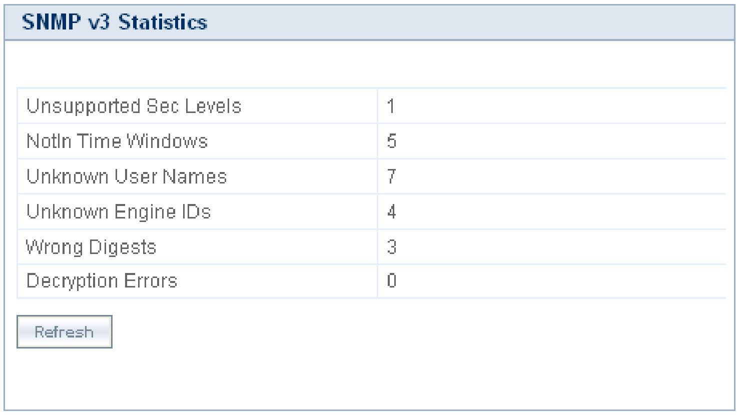
- **Command**: Type the required **rlt** command. Click the **Execute** button.
- The command execution is displayed in the Web Console screen.

To run the Radio Link Test tool through Command Line Interface (CLI), refer the *Tsunami® 800 and 8000 Series Reference Guide.*

7.12 SNMP v3 Statistics

SNMP v3 statistics can be viewed only when SNMPv3 feature is enabled on the device. See SNMP.

To view the **SNMPv3 Statistics**, navigate to **MONITOR > SNMPV3 Statistics**. The following **SNMP v3 Statistics** screen appears:



SNMP v3 Statistics

Unsupported Sec Levels	1
NotIn Time Windows	5
Unknown User Names	7
Unknown Engine IDs	4
Wrong Digests	3
Decryption Errors	0

Figure 7-58 SNMP v3 Statistics

The following table lists the SNMP v3 parameters and their description**:**

Parameter	Description
Unsupported Sec Levels	This parameter specifies the total number of packets dropped by the SNMP engine because they requested a security level that was unknown to the SNMP engine or otherwise unavailable.
Not In Time Windows	This parameter specifies the total number of packets dropped by the SNMP engine because they appeared outside the authoritative SNMP engine's window.
Unknown User Names	This parameter specifies the total number of packets dropped by the SNMP engine because they correspond to a user that is unknown to an SNMP engine.
Unknown Engine IDs	This parameter specifies the total number of packets dropped by the SNMP engine because they correspond to an SNMP Engine ID that is unknown to an SNMP engine.
Wrong Digests	This parameter specifies the total number of packets dropped by the SNMP engine because they do not contain the expected digest value.
Decryption Errors	This parameter specifies the total number of packets dropped by the SNMP engine because they could not be decrypted.

Troubleshooting 8

This chapter helps you to address the problems that might arise while using our device. If the procedures discussed in this chapter does not provide a solution, or the solution does not solve your problem, check our support site at http://my.proxim.com which stores all resolved problems in its solution database. Alternatively, you can post a question on the support site, to a technical person who will reply to your email.

Before you start troubleshooting, check the details in the product documentation available on the support site. For details about RADIUS, TFTP, Terminal and Telnet programs, and Web Browsers, refer to their appropriate documentation.

In some cases, rebooting the device solves the problem. If nothing else helps, refer to Recovery Procedures.

This chapter provides information on the following:

- PoE Injector
- Connectivity Issues
- Surge or Lightning Issues (For Connectorized devices)
- Setup and Configuration Issues
- Application Specific Troubleshooting
- Wireless Link Issues
- Wired (Ethernet) Interface Validation
- Wireless Interface Validation
- Recovery Procedures
- Spectrum Analyzer
- Miscellaneous

8.1 PoE Injector

Problem	Solution
The Device Does Not Work	• Make sure that you are using a standard UTP – Category 5e/6 cable in case of MP-8100-SUA, MP-8150-SUR, MP-8150-SUR-100, MP-8200-BSU-G, MP-8250-BS9-G, MP-8250-BS1-G, MP-8200-BSU, MP-8250-BS9, MP-8250-BS1, MP-820-BSU-100, MP-822-BSU-100, MP-825-BS3-100, MP-8200-SUA, MP-820-SUA-50$^+$, MP-820-SUA-100, MP-822-SUA-100, MP-825-SUR-50$^+$, MP-825-SUR-100, QB-8200-LNK-G, QB-8200-LNK, QB-825-EPR/LNK-50$^+$, QB-825-EPR/LNK-100, QB-835-EPR/LNK-25 and QB-835-EPR/LNK-50 devices – Category 5/5e cable in case of MP-835-CPE-10, MP-835-CPE-10, MP-835-CPE-25, MP-835-CPE-50, MP-835-CPE-100,MP-825-CPE-50, MP-825-CPE-100 and QB-826-EPR/LNK-100. • Try a different port on the same PoE Injector hub (remember to move the input port accordingly) – if it works then there is a problem in the previous RJ45 port or a bad RJ45 port connection. • Try to connect the device to a different PoE Injector hub. • Try using a different Ethernet cable – if it works, there is probably a fault in the cable or its connection. • Check the power plug and hub. • If the Ethernet link goes down, check the cable, cable type, switch and hub.
There is No Data Link	• Verify that the indicator on the device port is "ON." • Verify that the Ethernet cable from PoE Injector hub to the Ethernet port of the device is properly connected. • Make sure that you are using a standard UTP – Category 5e/6 cable in case of MP-8100-SUA, MP-8150-SUR, MP-8150-SUR-100, MP-8200-BSU-G, MP-8250-BS9-G, MP-8250-BS1-G, MP-8200-BSU, MP-8250-BS9, MP-8250-BS1, MP-820-BSU-100, MP-822-BSU-100, MP-825-BS3-100, MP-8200-SUA, MP-820-SUA-50$^+$, MP-820-SUA-100, MP-822-SUA-100, MP-825-SUR-50$^+$, MP-825-SUR-100, QB-8200-LNK-G, QB-8200-LNK, QB-825-EPR/LNK-50$^+$, QB-825-EPR/LNK-100, QB-835-EPR/LNK-25 and QB-835-EPR/LNK-50 devices – Category 5/5e cable in case of MP-835-CPE-10, MP-835-CPE-25, MP-835-CPE-50, MP-835-CPE-100, MP-825-CPE-50, MP-825-CPE-100 and QB-826-EPR/LNK-100. The length of the cable from the Ethernet port of the device to the PoE should be less than 100 meters (approximately 325 feet). • Try to connect a different device to the same port on the PoE Injector hub – if it works and a link is established then there is probably a fault in the data link of the device. • Try to re-connect the cable to a different output port (remember to move the input port accordingly) – if it works then there is a fault probably in the output or input port of the PoE Injector hub or a bad RJ45 connection.
Overload Indications	• Connect the device to a PoE Injector. • Ensure that there is no short over on any of the connected cables. • Move the device into a different output port (remember to move the input port accordingly) - if it works then there is a fault probably in the previous RJ45 port or bad RJ45 port connection.

8.2 Connectivity Issues

Connectivity issues include any problem that prevents from powering or connecting to the device.

Problem	Solution
Does Not Boot - No LED Activity	• Make sure the power source is ON. • Make sure all the cables to the device are connected properly.
Ethernet Link Does Not Work	Check the Ethernet LED • **Solid Green**: The Ethernet link is up. • **Blinking Green**: The Ethernet link is down.
Serial Link Does Not Work	• Double-check the physical network connections. • Make sure your PC terminal program (such as HyperTerminal) is active and configured to the following values: – Com Port: (COM1, COM2 and so on depending on your computer); – Baud rate: 115200; Data bits: 8; Stop bits: 1; Flow Control: None; Parity: None; – Line Feeds with Carriage Returns • (In HyperTerminal select: **File > Properties > Settings > ASCII Setup > Send Line Ends with Line Feeds**) 📝: *Not applicable to MP-835-CPE-10, MP-835-CPE-25, MP-835-CPE-50, MP-835-CPE-100, MP-825-CPE-50 and MP-825-CPE-100 as it does not support serial interface.*
Cannot Access the Web Interface	• Open a command prompt window and type the Ping command along with the IP address of the device. For example, **ping 10.0.0.1**. If the device does not respond, check if you have the correct IP address. If the device responds then it means the Ethernet connection is working properly. • Ensure that you are using Microsoft Internet Explorer 7.0 (or later) or Mozilla Firefox 3.0 (or later). • Ensure that you are not using a proxy server for the network connection with your Web browser. • Ensure that you have not exceeded the maximum number of Web Interfaces or CLI sessions. • Double-check the physical network connections. Use a well-known device to ensure the network connection is functioning properly. • Troubleshoot the network infrastructure (check switches, routers, and so on). 📝: *At any point of time, if the device is unable to connect to your network, reset the device by unplugging and plugging the cables from the PoE.*

8.3 Surge or Lightning Issues (For Connectorized devices)

Problem	Solution
Surge or Lighting Problem	In case of any lightning or surge occurrence, check for the conditions specified below: • Check the RF signals by referring to RSSI statistics and if the signal strength has been lowered considerably, replace the Surge Arrestor. • Unscrew the N-Type connector at the top and visually inspect the Surge Arrestor for electrical burns. If any, replace it.

8.4 Setup and Configuration Issues

Problem	Solution
Device Reboots Continuously	One of the reason for the device to reboot continuously is that the radio card is not properly placed in the mini-PCI slot. When you power on the device and you do not see the "**WIRELESS NETWORK1 PASSED**" in the POST message in the Serial Console, please contact Proxim's support site at http://my.proxim.com.
Lost Telnet or SNMP Password	Perform Operational Mode procedure. This procedure resets system and network parameters, but does not affect the image of the device. The default HTTP, Telnet, and SNMP username is **admin** and password is **public**.
Device Responds Slowly	If the device takes a long time to respond, it could mean that: • No DHCP server is available. • The IP address of the device is already in use. Verify that the IP address is assigned only to the device you are using. Do this by switching off the device and then pinging the IP address. If there is a response to the ping, another device in the network is using the same IP address. If the device uses a static IP address, switching to DHCP mode could solve this problem. • The network traffic is more.
Incorrect Device IP Address	• The default IP address assignment mode is Static and the default IP address of the device is 169.254.128.132. • If the IP address assignment mode is set to Dynamic, then the DHCP Server will assign an IP address automatically to the device. If the DHCP server is not available on your network, then the fall back IP address (169.254.128.132) of the device is used. • Use ScanTool, to find the current IP address of the device. Once you have the current IP address, use Web Interface or CLI Interface to change the device IP settings, if necessary. • If you are using static IP address assignment, and cannot access the device over Ethernet, refer to Initializing the IP Address using CLI. • Perform Operational Mode procedure. This will reset the device to static mode.

Problem	Solution
HTTP Interface or Telnet Does Not Work	- Make sure you are using a compatible browser: – 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 address bar.* - Make sure you have the correct IP address of the device. Enter the device IP address in the address bar of the browser, for example **http://169.254.128.132**. - When the **Enter Network Password** window appears, enter the User Name and and Password. The default HTTP username is **admin** and password is **public**. - Use CLI, to check the IP Access Table which can restrict access to Telnet and HTTP.
Telnet CLI Does Not Work	- Make sure you have the correct IP address. Enter the device IP address in the Telnet connection dialog, from a DOS prompt: **C:\> telnet <Device IP Address>** - Use HTTP, to check the IP Access Table which can restrict access to Telnet and HTTP. - Enable Telnet in Vista or Windows 7 as it is by default disabled.
TFTP Server Does Not Work	- The TFTP server is not properly configured and running - The IP address of the TFTP server is invalid - The upload or download directory is not correctly set - The file name is not correct
Changes in Web Interface Do Not Take Effect	1. Restart your Web browser. 2. Log on to the device again and make changes. 3. Reboot the device. 4. Click **COMMIT** for the changes to take effect. 5. Wait until the device reboots before accessing the device again.
Imbalance in the throughputs of the aSymmetric Uplink & Downlink, if NIC cards of different vendors are used	Use NIC cards of the same vendor
At the SU during 'commit', a Pop up with message "Failed to apply WORP link profile Configuration" is observed, though the configuration is valid.	Wait for few seconds and re-perform the 'commit' operation.

8.5 Application Specific Troubleshooting

Problem	Solution
RADIUS Authentication Server Services unavailable	If RADIUS Authentication is enabled on the device, then make sure that your network's RADIUS servers are operational. Otherwise, clients will not be able to log on to the device. There are several reasons for the authentication server's services to be unavailable. To make it available, • Make sure you have the proper RADIUS authentication server information setup configured on the device. Check the RADIUS Authentication Server's Shared Secret and Destination Port number (default is 1812; for RADIUS Accounting, the default is 1813). • Make sure the RADIUS authentication server RAS setup matches the device.
TFTP Server	If a TFTP server is not configured and running, you will not be able to download and upload images and configuration files to or from the device. Remember that the TFTP server need not be local, as long as you have a valid TFTP IP address. Note that you do not need a TFTP server running unless you want to transfer files to or from the device. After the TFTP server is installed: • Check to see that TFTP is configured to point to the directory containing the device Image. • Make sure you have the proper TFTP server IP Address, the proper device image file name, and that the TFTP server is connected. • Make sure the TFTP server is configured to both Transmit and Receive files (on the TFTP server's **Security** tab), with no automatic shutdown or time-out (on the **Auto Close** tab).

8.6 Wireless Link Issues

Given below are the possible reasons for a wireless link not getting established and the relevant observations.

Reason(s)	Observation
Mismatch in network name	• The Wireless Interface Statistics (In Octets, In Non-Unicast Packets) are incremented in BSU/End Point A and SU/End Point B. • The WORP counters are not affected. • The remote device is not listed in the Site Survey.
Incorrect or invalid configured BSU/End Point A name	• The Wireless Interface Statistics (In Octets, In Non-Unicast Packets) are incremented in SU/End Point B. • The WORP counters are not affected. • The remote device is not listed in the Site Survey.
Mismatch in network secret	• The Wireless Interface Statistics (In Octets, In Non-Unicast Packets) are incremented in BSU/End Point A and SU/End Point B. • The WORP counters are incremented (Req for Serv, Reg Req, Auth Req, Reg Attempts, Reg LastReason: Incorrect Parameter) on both ends.

Reason(s)	Observation
Encryption set to **No Encryption** in BSU/End Point A and **AES Encryption** in SU/End Point B	• The Wireless Interface Statistics (In Octets, In Non-Unicast Packets) are incremented in BSU/End Point A; No decrypt errors are observed in SU/End Point B. • In SU/End Point B, the WORP counters (Announcements, Req for Serv, Reg Attempts, Reg incomplete, Reg timeout, Reg Last Reason: Timeout) are incremented. In BSU/End Point A, no WORP counters are incremented except announcements. • The remote device is not listed in the Site Survey.
Encryption set to **AES Encryption** in BSU/End Point A and **No Encryption** in SU/End Point B	• The Wireless Statistics counters and WORP counters are not incremented in SU/End Point B. • The remote device is not listed in the Site Survey.
Encryption set to **AES Encryption** in both BSU/End Point A and SU/End Point B. A mismatch in Encryption key	• The Wireless Interface Statistics (In Octets, In Non-Unicast Packets) are incremented only in SU/End Point B. • The remote device is not listed in the Site Survey.
BSU exceeds the maximum SU limit	• The Wireless Interface Statistics (In Octets, In Non-Unicast Packets) are incremented in SU/End Point B but fails to authenticate. • The WORP counters (Announcements, Req for Serv, Reg Attempts, Reg Incompletes, Reg Timeouts, Reg Last Reason: Timeout) are incremented in SU/End Point B. • The remote device is listed in the Site Survey.
Interference issues due to wider beam width of the antenna	• **MP-835-CPE-10, MP-835-CPE-25, MP-835-CPE-50, MP-835-CPE-100, MP-825-CPE-50, MP-825-CPE-100, MP-825-SUR-50^{+}, MP-825-SUR-100 and QB-826-EPR/LNK-100 uses a wider beam width antenna (up to 38 ^{o}) with a gain of 15dBi. Due to its wider beam width, it may pick up more interfering signals and may report large number of errors compared to other Tsunami products. Wireless interference may also lead to:** – SNR value fluctuations between the Antenna (A1/A2) ports – DDRS operation at lower data rates – Higher number of PHY errors which may result in false RADAR detection in DFS bands • **To overcome these issues, use a spectrum analyzer and switch to a noise-free channel.**
With multiple link profiles, the wireless network performance is getting affected.	The overall performance of the wireless network gets affected when using multiple link profiles and atleast one of the subscriber is operating with a lower data rate. • For example, consider a wireless network with a BSU and 5 SU profiles. Each SU is transmitting data at a data rate as tabulated below. As SU1 is operating at a lower data rate (6.5 Mbps), the entire performance of the network gets affected.

<table>
<tr><th>Reason(s)</th><th>Observation</th></tr>
<tr><td></td><td>
<table>
<tr><th>SU Profile(s)</th><th>Data Rate</th><th>Throughput</th></tr>
<tr><td>SU1</td><td>6.5 Mbps</td><td rowspan="5">Aggregated throughput can be a maximum of 13 Mbps</td></tr>
<tr><td>SU2</td><td>39 Mbps</td></tr>
<tr><td>SU3</td><td>78 Mbps</td></tr>
<tr><td>SU4</td><td>130 Mbps</td></tr>
<tr><td>SU5</td><td>78 Mbps</td></tr>
</table>
<p>In order to optimize the network performance, apply QoS.
Given below is an example on how the network performance can be improved by applying QoS. QoS is applied for SU1 with the following configuration:</p>
<ul>
<li>PIR based on the ToS value 96</li>
<li>SFC with MIR/CIR= 1Mbps; Priority = 3; Latency/Jitter=10ms</li>
</ul>
<p>Subscribers SU2...SU5 use the default QoS configuration.</p>
<table>
<tr><th>Profiles</th><th>Data Rate</th><th>Throughput</th></tr>
<tr><td>SU1</td><td>6.5 Mbps</td><td rowspan="5">With QoS applied for SU1, expected throughput is 26 Mbps</td></tr>
<tr><td>SU2</td><td>39 Mbps</td></tr>
<tr><td>SU3</td><td>78 Mbps</td></tr>
<tr><td>SU4</td><td>130 Mbps</td></tr>
<tr><td>SU5</td><td>78 Mbps</td></tr>
</table>
<p><i>: Given above is just an example and values might vary from case-to-case.</i></p>
</td></tr>
</table>

8.7 Wired (Ethernet) Interface Validation

Problem	Solution
Wired (Ethernet) Interface Validation	Run iperf commands • Use iperf commands with –w option as 202k. The throughput is expected to be equal in both directions and should be comparable from laptop to laptop or desktop to desktop performance If the above throughput value is not in the expected range, • Check speed and duplex settings between the device and Personal Computer or switch or router connected • Make sure the connection established is of same speed and full duplex is as expected (10 or 100 or 1000) • With auto negotiation, if you notice this issue, then try manually setting the speed and duplex • Update the Ethernet driver in the Personal Computer to the latest one

8.8 Wireless Interface Validation

Problem	Solution
Wireless Interface Validation	**Run iperf commands** (You can run Embedded iperf commands only through Telnet.) • iperf –s –w 202k (command for iperf server) • Iperf –c ipaddress –w 202k –t time Period –I <intermediateResultInterval> –P <4 or 6> (command to run iperf client) – Ipaddress -> of the SU/End Point B or BSU/End Point A device where the iperf server is running – P -> No of pairs (Streams) • Use –d option to run bidirectional throughput • Use –r option to run unidirectional throughput one after another without changing the server and SU ends If the expected throughput is not achieved, then check the following: • **Antenna Alignment** – Note whether the antenna ports are balanced – SNR/RSSI provided for Local and Remote in the BSU/SU Link Statistics page or by using “aad” command – Signal difference of <=5 dBm is considered as balanced and recommended – If the chains are not balanced, then look at the alignment and connectors of RF cables, used between antenna and device – If in RMA (Returned from Customer), check the RF cable to radio port connectivity – Avoid nearby metal surfaces, if you are using Omni antenna • **Data Streams** – Select “Single” stream instead of “Dual” stream mode – DDRS - with single stream data rate or with Auto mode Dual stream data rates can be used only when the signal in both antenna ports is balanced. • **Antenna Port Selection** – For devices with 3x3 MIMO radio, make sure you are either enabling all antenna ports for 3x3 MIMO or using A1 and A3 antenna ports for 2x2 MIMO mode – For devices with 2x2 MIMO radio, use A1 and A2 antenna ports – For using single stream, it is mandatory to select antenna port A1 – Enabling all antenna port will not cause any issue even if it is not in use. • **Bad Channel** – Check for CRC errors, PHY errors, WORP Retries and WORP Failures in Monitor Interface Statistics page. If this count increments steadily (Refreshing the web page is required) then • Either change the channel and check for a better channel • Use Wi-Spy or similar tool and check the environment for better channel
Wireless Interface Validation	• **Data Rate Issues** – Ensure same data rates are selected if you are using fixed data rate between BSU/SU and End Point A/End Point B to have predictable throughput and link – Alternatively, use DDRS with Auto mode enabled

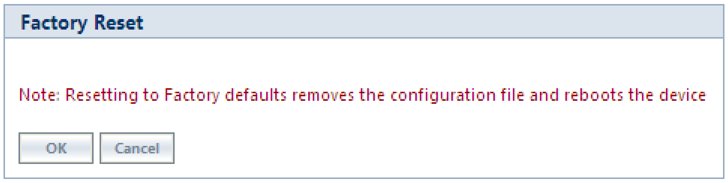
Problem	Solution
	• **Performance and Stability Issues** – Check the distance between two co-locating devices. The distance between two co-locating devices should be minimum 3 meters, in order to achieve good throughput and maintain link stability. The operating adjacent channel should maintain 5MHz spacing if managed by a single administrator. – When DDRS is disabled, check the Minimum Required SNR for the current data rate by navigating to **MONITOR** --> **WORP Statistics** --> **Interface 1** --> **Link Statistics Page** --> **Click here for Local SNR-Table**. If the current SNR is not meeting the minimum required SNR criteria for the current data rate, then accordingly reduce the data rate. – If SNR is more than the maximum optimal SNR limit (**MONITOR** --> **WORP Statistics** --> **Interface 1** --> **Link Statistics Page** --> **Click here for Local SNR-Table**) then it causes radio receiver saturation thus impacting the performance of the link. To overcome this situation, set the TPC appropriately or enable ATPC to adjust the signal level automatically. Also, enabling DDRS can help in choosing right data rate automatically. – To measure and diagnose any performance issues in the wireless link, use the **Radio Link Test Tool**. To use this tool, navigate to **MONITOR** --> **WORP Statistics** --> **Interface 1** --> **Link Statistics Page** --> **Details** -->**Click** icon. For detailed description of this tool, refer Radio Link Test Tool

8.9 Recovery Procedures

Recovery Procedure is used to restore the device to its factory default operating state. Depending on the device state, the recovery procedures can be classified under two modes:

1. **Operational Mode**: Device is up and in running state.
2. **Bootloader Mode**: Device operating image is deleted.

8.9.1 Operational Mode

S.No	Scenario	Recovery Procedure
1	Restore the device to its factory default configuration while accessing it through web interface	In the web interface, navigate to **MANAGEMENT > Reset to Factory**. The **Factory Reset** screen appears:  Factory Reset Note: Resetting to Factory defaults removes the configuration file and reboots the device In the screen, click **OK**. The device now reboots and comes with: • **IP Address**: 169.254.128.132 • **Username**: admin • **Password**: public For Reload procedure using ScanTool specific to MP-835 device series, refer **Reset/Reload Procedure**

<table>
<tr><th>S.No</th><th>Scenario</th><th>Recovery Procedure</th></tr>
<tr><td>2</td><td>The device is not accessible for reasons such as user has forgotten the web interface login password, Management VLAN Id is changed, wrong VLAN configuration.</td><td>Press and hold the Reload button (<i>use a pin or the end of a paper clip)</i> on the POE injector for a time frame as mentioned in the following table:
<table>
<tr><th>Device</th><th>Timings</th></tr>
<tr><td>MP-8200-BSU-G; MP-8100-SUA
MP-8150-SUR; MP-8150-SUR-100
MP-8250-BS9-G; MP-8250-BS1-G
MP-8200-BSU;MP-8250-BS9;MP-8250-BS1
MP-820-BSU-100; MP-822-BSU-100; MP-825-BS3-100
MP-8200-SUA; MP-8250-SUR
MP-825-CPE-50; MP-825-CPE-100;
MP-835-CPE-10, MP-835-CPE-25, MP-835-CPE-50, MP-835-CPE-100, MP-820-SUA-50^{+}; MP-820-SUA-100
MP-822-SUA-100;
MP-825-SUR-50^{+}; MP-825-SUR-100
QB-8200-EPA-G / LNK-G
QB-8250-EPR / LNK-G
QB-8200-EPA / LNK
QB-8250-EPR / LNK
QB-825-EPR/LNK-50^{+}
QB-825-EPR/LNK-100
QB-835-EPR/LNK-25
QB-835-EPR/LNK-50
QB-826-EPR/LNK-100</td><td>5 to 6 seconds</td></tr>
</table>
<ul>
<li><i>To use this procedure, use a PoE injector with Reload functionality.</i></li>
<li><i>The device operating image will get deleted, if you press the button for more than the above mentioned time.</i></li>
<li><i>The timings mentioned above are valid from the time the device is powered UP (that is during POST).</i></li>
</ul>
The device now reboots and comes with: <b>IP Address</b>: <b>169.254.128.132</b>; <b>Username</b>: <b>admin</b>; and <b>Password</b>: <b>public</b>
For Reload procedure using ScanTool specific to MP-820 / 830 series devices, refer <b>Reset/Reload Procedure</b></td></tr>
</table>

8.9.2 Bootloader Mode

S.No	Scenario	Recovery Procedure

1	a) The device operating image is corrupted for reasons such as power interruption while upgrading
	*(For only
	MP-820-BSU-100;
	MP-822-BSU-100;
	MP-820-SUA-50$^+$;
	MP-820-SUA-100;
	MP-822-SUA-100;
	MP-825-BS3-100;
	MP-825-SUR-50$^+$;
	MP-825-SUR-100;
	devices).*
		• After powering-up the device, press and hold the Reload button on the PoE injector (use a pin or the end of a paper clip) for first 15 seconds and then release the button between 15-30 seconds. By doing so, the operating image will get deleted.
		:
		• *No reload via Ethernet cross cable.*
		• *It is not applicable to MP-835-CPE-10, MP-835-CPE-25, MP-835-CPE-50, MP-835-CPE-100, MP-825-CPE-50 and MP-825-CPE-100, QB-835-EPR/LNK-25, QB-835-EPR/LNK-50 and QB-826-EPR/LNK-100 devices.*
		After deleting the operating image, refer Using the ScanTool and Using the Bootloader CLI sections to load the firmware onto the device.
		For Reload procedure using ScanTool specific to MP-820 / 830 series devices, refer **Reset/Reload Procedure**

	b) The device operating image is corrupted for reasons such as power interruption while upgrading *(For all devices)*.	Do one of the following: • While powering the device, press and hold the Reload button on the PoE injector (*use a pin or the end of a paper clip)* for 15 seconds. By doing so, the operating image will get deleted. • Use a 4-pair (Gigabit) cross over Ethernet cable between the PoE and the device. By doing so, the reload functionality gets activated and forcibly deletes the operating image. • If you are having serial access to the device during POST, press **SHIFT+u** to enter into forced user mode of the bootloader. From the Bootloader prompt, enter the command **firmware_delete**. After deleting the operating image, refer Using the ScanTool and Using the Bootloader CLI sections to load the firmware onto the device.
2	The device is not accessible for reasons such as user has forgotten the web interface login password, Management VLAN Id is changed, and wrong VLAN configuration. And, you do not have a reload capable PoE but Serial access is possible	If you are having serial access to the device during POST, press **SHIFT+u** to enter into forced user mode of the bootloader. From the Bootloader prompt, enter the command **config_delete**. This command will also delete the Upgrade License file. Next, issue the command **reboot**. The device now reboots and comes with: **IP Address**: **169.254.128.132**; **Username**: **admin**; and **Password**: **public**

8.9.3 Load a New Image

Follow one of the procedures below to load a new image to the device:

- Using the ScanTool
- Using the Bootloader CLI

: *A new image cannot be downloaded using Bootloader CLI onto MP-835-CPE-10, MP-835-CPE-25, MP-835-CPE-50, MP-835-CPE-100, MP-825-CPE-50, MP-825-CPE-100 and QB-826-EPR/LNK-100 as it does not provide a serial interface.*

8.9.3.1 Using the ScanTool

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

ScanTool automatically detects the device that does not have a valid software image. The **TFTP Server** and **Image File Name** parameters are enabled in the ScanTool's ***Change*** screen so that you can download a new image to the device. (These fields are disabled, if ScanTool detects a software image on the device). See Initialization.

Preparing to Download the Device Image

Before starting the download process, you need to know the device IP Address, Subnet Mask, the TFTP Server IP Address, and the Image file name. Make sure the TFTP server is running and properly configured to point to the folder containing the image to be downloaded.

Download Procedure

Follow these steps to download a software image to the device by using ScanTool:

1. Download the latest software from http://my.proxim.com, and copy it to the default directory of the TFTP server.
2. Launch Proxim's ScanTool.
3. Highlight the entry for the device that you want to update and click **Change**.
4. Set **IP Address Type** to **Static**.

: *You need to assign static IP information temporarily to the device since its DHCP client functionality is not available when no image is installed on the device.*

5. Now enter the IP address, Subnet mask, Default-gateway, Server - IP address and the image filename.
6. Click OK. The device will reboot and the download starts automatically.
7. Click OK when prompted to return to the Scan List screen after the device has been updated successfully.
8. Click Cancel to close the ScanTool.

After the download process is completed, the device will reboot and initialize. After successful initialization, the device is ready to be configured.

8.9.3.2 Using the Bootloader CLI

To download the new device image, you will need an Ethernet connection to the computer on which the TFTP server resides. This can be any computer on the LAN or connected to the device with an Ethernet cable.

You must also connect the device to a computer with a standard serial cable and use a terminal client. From the terminal, enter the CLI commands to set the IP address of the device and to download the device image.

Preparing to Download the device image

Before starting, you need to know the device IP Address, Subnet Mask, the TFTP Server IP Address, and the device image file name. Make sure the TFTP server is running and configured to point to the default directory containing the image to be downloaded.

Download Procedure

1. Download the latest software from http://my.proxim.com, and copy it to the default directory of the TFTP server.
2. Connect the device serial port to your computer's serial port.
3. Open your terminal emulator program and set the following connection properties:
   - **Com Port:** COM1, COM2 and so on, depending on your computer
   - **Baud Rate:** 115200
   - **Data Bits:** 8
   - **Stop Bits:** 1
   - **Flow Control:** None
   - **Parity:** None
4. Under **File > Properties > Settings > ASCII Setup**, enable the **Send line ends with line feeds** option.

   Terminal Emulator program sends a line return at the end of each line of code.

   The terminal display shows Power On Self Tests (POST) activity. After approximately 30 seconds, a message indicates: **Starting ScanTool interface, press any key to enter CLI 5".** After this message appears, press any key. Now the bootloader prompt appears as below:

   ```
   Bootloader=>
   ```
5. Enter the following commands:

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

   Example:
   Bootloader=> show
   Bootloader=> set ipaddr 169.254.128.132
   Bootloader=> set serverip 169.254.128.133
   Bootloader=> set filename image_proxim.sei
   Bootloader=> set gatewayip 169.254.128.133
   Bootloader=> set netmask 255.255.255.0
   Bootloader=> set ipaddrtype static
   Bootloader=> show
   Bootloader=> reboot
   ```

   The device will reboot and then download the image file. When the download process is complete, configure the device.

8.9.4 Setting IP Address using Serial Port

If the ScanTool fails to scan the device and users knows the login credentials then you can set the IP address for the device using serial port.

8.9.4.1 Hardware and Software Requirements

- Standard serial (RS-232) cable
- ASCII Terminal software

8.9.4.2 Attach the Serial Port Cable

1. Connect one end of the serial cable to the device and the other end to a serial port on your computer.
2. Power on the computer and the device.

8.9.4.3 Initializing the IP Address using CLI

After connecting the cable to the serial port, you can use the CLI to communicate with the device. CLI supports the most-generic terminal emulation programs. In addition, many web sites offer shareware or commercial terminal programs that you can download. Once the IP address has been assigned, you can use the HTTP interface or the Telnet to complete the configuration.

Follow these steps to assign an IP address to the device:

1. Open your terminal emulation program and set the following connection properties:
   - **Com Port**: COM1, COM2, and so on depending on your computer
   - **Baud Rate**: 115200
   - **Data Bits**: 8
   - **Stop Bits**: 1
   - **Flow Control**: None
   - **Parity**: None

   The terminal display shows Power On Self Tests (POST) activity, and then displays the software version. It prompts you to enter the CLI username and password. The commands to enter the username and password are as follows:

   ```
   #################################################|
   # +-++-++-++-++-++-+
   # |p||r||o||x||i||m|
   # +-++-++-++-++-++-+
   # Version: 1.0.0 B208100
   # Architecture: MIPS 7660
   # Creation: 10-Aug-2009 (IST) 08:16:14 PM
   #################################################|
   Username: admin
   Password:
   ```

   This process may take up to 90 seconds.

2. Enter the CLI Username and password. By default username is **admin** and password is **public**. The terminal displays a welcome message and then the CLI Prompt. Enter ‘show ip’ as shown below:

   ```
   System Name> show ip

   The following Ethernet IP information is displayed:

   // Ethernet IP CONFIGURATION //
   INDEX 1
   IP Address: 10.0.0.1
   Mask: 255.255.255.0
   Address Type: static
   ```

```
// IP Gateway Configuration //
Gateway IP Address: 169.254.128.1
```

3. Change the IP address and other network values using the following CLI commands (use your own IP address and Subnet mask).

```
System Name> enable
System Name# configure
System Name(config)#network
System Name(config-net)# ip
System Name(config-net-ip)# ethernet-ip-table
System Name(config-net-ip-etherip)# rowedit 1 ipaddress <ipaddress>
System Name(config-net-ip-etherip)# rowedit 1 mask <subnet mask>
System Name(config-net-ip-etherip)# rowedit 1 address-type <Address Type>
System Name(config-net-ip)# default-gateway <IP Gateway>
System Name(config-net-ip-etherip)#exit
System Name(config-net-ip)#exit
System Name(config-net)#exit
System Name(config)# commit 1
System Name(config)# reboot 1
```

4. After the device reboots, verify the new IP address by reconnecting to the CLI. Alternatively, you can ping the device from a network computer to confirm that the new IP address has taken effect.

   When a proper IP address is set, use HTTP interface or Telnet to configure the rest of the operating parameters of the device.

8.10 Spectrum Analyzer

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

8.10.1 Avoiding Interference

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

- Change the channel to a frequency that has no or least interference.
- Try changing the antenna polarization.
- A small beam antenna looks only in one particular direction. Because of the higher gain of such an antenna, lowering the output power or adding extra attenuation might be required to stay legal. This solution cannot help when the source of interference is right behind the remote site.
- Adjusting the antenna angle/height can help to reduce the interference.

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

8.10.2 Conclusion

A spectrum analyzer can be a great help to identify whether interference might be causing link problems on the device. Before checking for interference, the link should be verified by testing in an isolated environment, to make sure that the hardware works and your configurations are correct. The path analysis, cabling and antennas should be checked as well.

- Base Announces should increase continuously.

- Registration Requests and Authentication Requests should be divisible by 3. WORP is designed in a way that each registration sequence starts with 3 identical requests. It is not a problem if, once in a while, one of those requests is missing. Missing requests frequently is to be avoided.
- Monitor / Per Station (Information per connected remote partner): Check that the received signal level (RSL) is the same on both sides. This should be the case if output power is the same. Two different RSLs indicate a broken transmitter or receiver. A significant difference between Local Noise and Remote Noise could indicate a source of interference near the site with the highest noise. Normally, noise is about –80 dBm at 36 Mbps. This number can vary from situation to situation, of course, also in a healthy environment.

8.11 Miscellaneous

8.11.1 Unable to Retrieve Event Logs through HTTPS

If using Internet Explorer 7 and are not able to retrieve event logs through HTTPS, do the following:

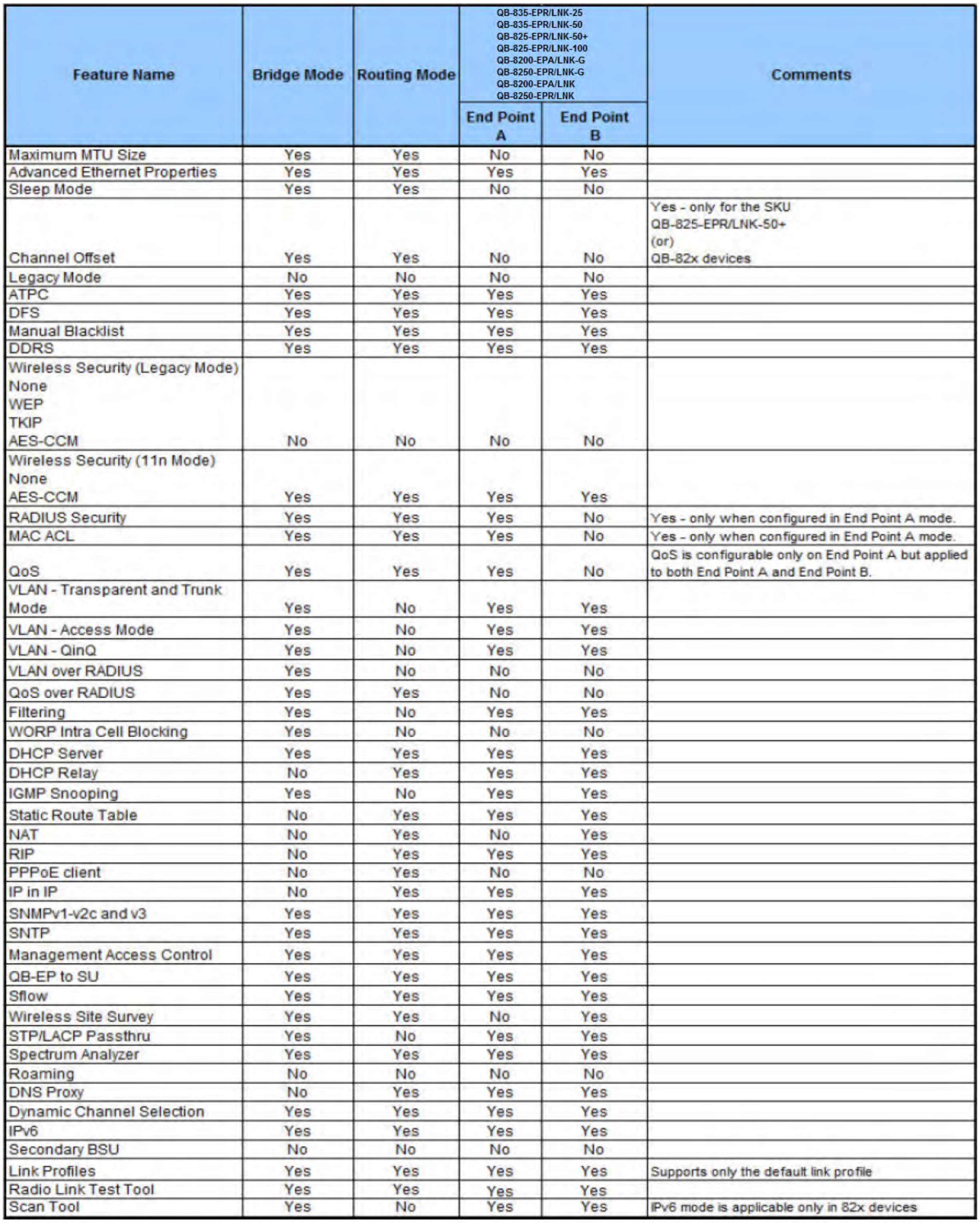
1. Open Internet Explorer
2. Navigate to **Tool** > **Internet Options** > **Advanced**
3. Go to **Security** and uncheck/unselect **Do not save encrypted pages to disk**

Alternatively, use Mozilla Firefox 3.5 or later.

Feature Applicability

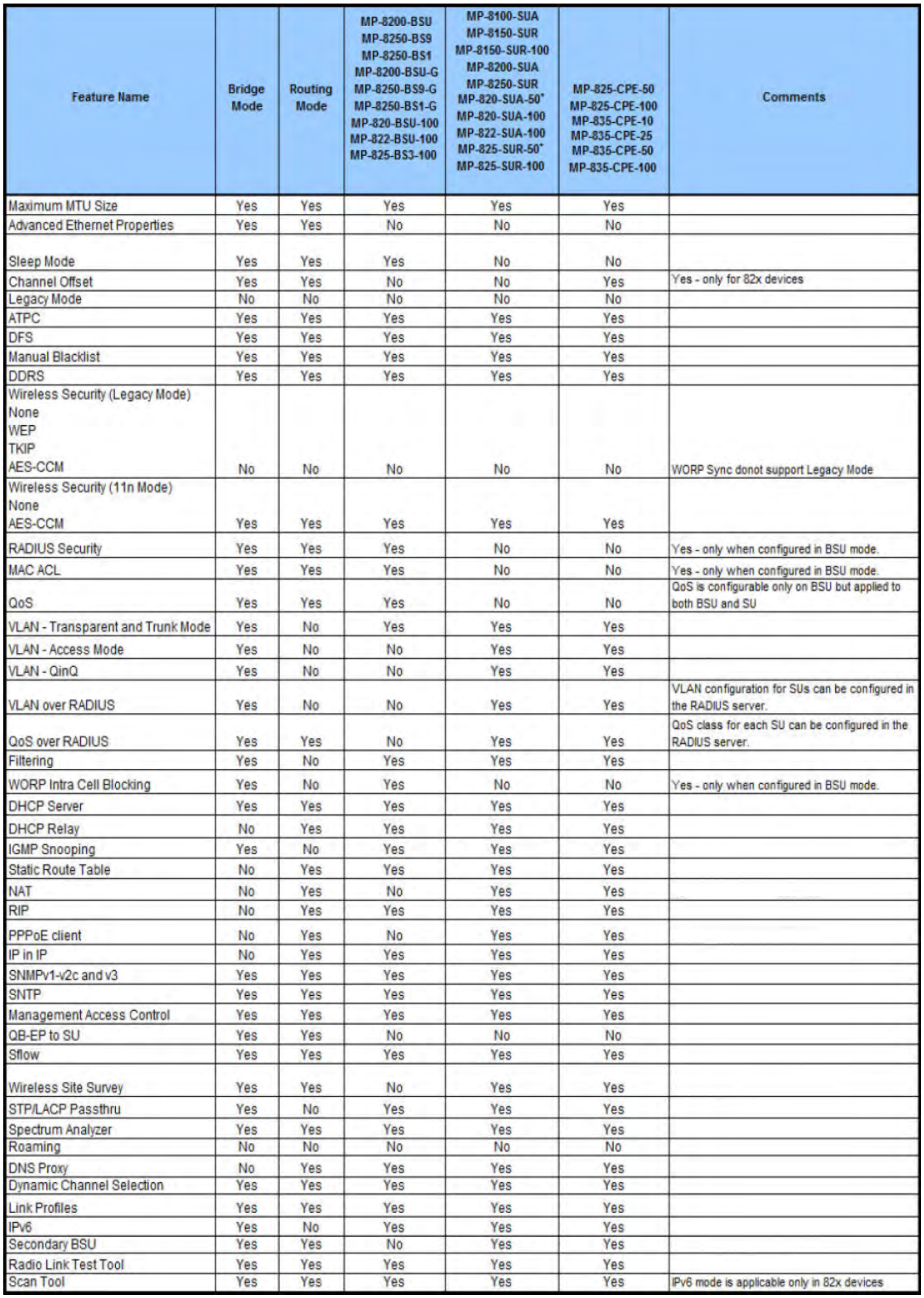
A

Given below are the feature(s) applicable to the respective point-to-point devices:



Feature Name	Bridge Mode	Routing Mode	QB-835-EPR/LNK-25 QB-835-EPR/LNK-50 QB-825-EPR/LNK-50+ QB-825-EPR/LNK-100 QB-8200-EPA/LNK-G QB-8250-EPR/LNK-G QB-8200-EPA/LNK QB-8250-EPR/LNK		Comments
			End Point A	End Point B	
Maximum MTU Size	Yes	Yes	No	No	
Advanced Ethernet Properties	Yes	Yes	Yes	Yes	
Sleep Mode	Yes	Yes	No	No	
Channel Offset	Yes	Yes	No	No	Yes - only for the SKU QB-825-EPR/LNK-50+ (or) QB-82x devices
Legacy Mode	No	No	No	No	
ATPC	Yes	Yes	Yes	Yes	
DFS	Yes	Yes	Yes	Yes	
Manual Blacklist	Yes	Yes	Yes	Yes	
DDRS	Yes	Yes	Yes	Yes	
Wireless Security (Legacy Mode) None WEP TKIP AES-CCM	No	No	No	No	
Wireless Security (11n Mode) None AES-CCM	Yes	Yes	Yes	Yes	
RADIUS Security	Yes	Yes	Yes	No	Yes - only when configured in End Point A mode.
MAC ACL	Yes	Yes	Yes	No	Yes - only when configured in End Point A mode.
QoS	Yes	Yes	Yes	No	QoS is configurable only on End Point A but applied to both End Point A and End Point B.
VLAN - Transparent and Trunk Mode	Yes	No	Yes	Yes	
VLAN - Access Mode	Yes	No	Yes	Yes	
VLAN - QinQ	Yes	No	Yes	Yes	
VLAN over RADIUS	Yes	No	No	No	
QoS over RADIUS	Yes	Yes	No	No	
Filtering	Yes	No	Yes	Yes	
WORP Intra Cell Blocking	Yes	No	No	No	
DHCP Server	Yes	Yes	Yes	Yes	
DHCP Relay	No	Yes	Yes	Yes	
IGMP Snooping	Yes	No	Yes	Yes	
Static Route Table	No	Yes	Yes	Yes	
NAT	No	Yes	No	Yes	
RIP	No	Yes	Yes	Yes	
PPPoE client	No	Yes	No	No	
IP in IP	No	Yes	Yes	Yes	
SNMPv1-v2c and v3	Yes	Yes	Yes	Yes	
SNTP	Yes	Yes	Yes	Yes	
Management Access Control	Yes	Yes	Yes	Yes	
QB-EP to SU	Yes	Yes	Yes	Yes	
Sflow	Yes	Yes	Yes	Yes	
Wireless Site Survey	Yes	Yes	No	Yes	
STP/LACP Passthru	Yes	No	Yes	Yes	
Spectrum Analyzer	Yes	Yes	Yes	Yes	
Roaming	No	No	No	No	
DNS Proxy	No	Yes	Yes	Yes	
Dynamic Channel Selection	Yes	Yes	Yes	Yes	
IPv6	Yes	Yes	Yes	Yes	
Secondary BSU	No	No	No	No	
Link Profiles	Yes	Yes	Yes	Yes	Supports only the default link profile
Radio Link Test Tool	Yes	Yes	Yes	Yes	
Scan Tool	Yes	No	Yes	Yes	IPv6 mode is applicable only in 82x devices

Given below are the feature(s) applicable to the respective point-to-multipoint devices:



Feature Name	Bridge Mode	Routing Mode	MP-8200-BSU MP-8250-BS9 MP-8250-BS1 MP-8200-BSU-G MP-8250-BS9-G MP-8250-BS1-G MP-820-BSU-100 MP-822-BSU-100 MP-825-BS3-100	MP-8100-SUA MP-8150-SUR MP-8150-SUR-100 MP-8200-SUA MP-8250-SUR MP-820-SUA-50* MP-820-SUA-100 MP-822-SUA-100 MP-825-SUR-50* MP-825-SUR-100	MP-825-CPE-50 MP-825-CPE-100 MP-835-CPE-10 MP-835-CPE-25 MP-835-CPE-50 MP-835-CPE-100	Comments
Maximum MTU Size	Yes	Yes	Yes	Yes	Yes	
Advanced Ethernet Properties	Yes	Yes	No	No	No	
Sleep Mode	Yes	Yes	Yes	No	No	
Channel Offset	Yes	Yes	No	No	Yes	Yes - only for 82x devices
Legacy Mode	No	No	No	No	No	
ATPC	Yes	Yes	Yes	Yes	Yes	
DFS	Yes	Yes	Yes	Yes	Yes	
Manual Blacklist	Yes	Yes	Yes	Yes	Yes	
DDRS	Yes	Yes	Yes	Yes	Yes	
Wireless Security (Legacy Mode) None WEP TKIP AES-CCM	No	No	No	No	No	WORP Sync donot support Legacy Mode
Wireless Security (11n Mode) None AES-CCM	Yes	Yes	Yes	Yes	Yes	
RADIUS Security	Yes	Yes	Yes	No	No	Yes - only when configured in BSU mode.
MAC ACL	Yes	Yes	Yes	No	No	Yes - only when configured in BSU mode.
QoS	Yes	Yes	Yes	No	No	QoS is configurable only on BSU but applied to both BSU and SU
VLAN - Transparent and Trunk Mode	Yes	No	Yes	Yes	Yes	
VLAN - Access Mode	Yes	No	No	Yes	Yes	
VLAN - QinQ	Yes	No	No	Yes	Yes	
VLAN over RADIUS	Yes	No	No	Yes	Yes	VLAN configuration for SUs can be configured in the RADIUS server.
QoS over RADIUS	Yes	Yes	No	Yes	Yes	QoS class for each SU can be configured in the RADIUS server.
Filtering	Yes	No	Yes	Yes	Yes	
WORP Intra Cell Blocking	Yes	No	Yes	No	No	Yes - only when configured in BSU mode.
DHCP Server	Yes	Yes	Yes	Yes	Yes	
DHCP Relay	No	Yes	Yes	Yes	Yes	
IGMP Snooping	Yes	No	Yes	Yes	Yes	
Static Route Table	No	Yes	Yes	Yes	Yes	
NAT	No	Yes	No	Yes	Yes	
RIP	No	Yes	Yes	Yes	Yes	
PPPoE client	No	Yes	No	Yes	Yes	
IP in IP	No	Yes	Yes	Yes	Yes	
SNMPv1-v2c and v3	Yes	Yes	Yes	Yes	Yes	
SNTP	Yes	Yes	Yes	Yes	Yes	
Management Access Control	Yes	Yes	Yes	Yes	Yes	
QB-EP to SU	Yes	Yes	No	No	No	
Sflow	Yes	Yes	Yes	Yes	Yes	
Wireless Site Survey	Yes	Yes	No	Yes	Yes	
STP/LACP Passthru	Yes	No	Yes	Yes	Yes	
Spectrum Analyzer	Yes	Yes	Yes	Yes	Yes	
Roaming	No	No	No	No	No	
DNS Proxy	No	Yes	Yes	Yes	Yes	
Dynamic Channel Selection	Yes	Yes	Yes	Yes	Yes	
Link Profiles	Yes	Yes	Yes	Yes	Yes	
IPv6	Yes	No	Yes	Yes	Yes	
Secondary BSU	Yes	Yes	No	Yes	Yes	
Radio Link Test Tool	Yes	Yes	Yes	Yes	Yes	
Scan Tool	Yes	Yes	Yes	Yes	Yes	IPv6 mode is applicable only in 82x devices

B

Parameters Requiring Reboot

Given below are the parameters that require the device to reboot.

Parameter(s)	Web Page(s)	Applicable Device Mode*
System Configuration		
Frequency Domain	BASIC CONFIGURATION ADVANCED CONFIGURATION -> System	All
Network Mode	ADVANCED CONFIGURATION -> System	All
Maximum MTU	ADVANCED CONFIGURATION -> System	All
Radio Mode	BASIC CONFIGURATION ADVANCED CONFIGURATION -> System	All
Controller Status	ADVANCED CONFIGURATION -> System	All Applicable only to • MP-820-BSU-100 • MP-822-BSU-100 • MP-825-BS3-100 • MP-820-SUA-50^{+} • MP-820-SUA-100 • MP-822-SUA-100 • MP-825-SUR-50^{+} • MP-825-SUR-100 • MP-825-CPE-50 • MP-825-CPE-100 • MP-835-CPE-10 • MP-835-CPE-25 • MP-835-CPE-50 • MP-835-CPE-100 • QB-825-EPR/LNK-50^{+} • QB-825-EPR/LNK-100 • QB-835-EPR/LNK-25 • QB-835-EPR/LNK-50 • QB-826-EPR/LNK-100
IP Configuration (Bridge Mode)		
Ethernet	BASIC CONFIGURATION ADVANCED CONFIGURATION -> Network -> IP Configuration	All
Default Gateway IP Address		All
DNS		All

Parameter(s)	Web Page(s)	Applicable Device Mode*
IP Configuration (Routing Mode)		
Ethernet	BASIC CONFIGURATION ADVANCED CONFIGURATION -> Network -> IP Configuration	All
Wireless		All
Wireless (With PPPoE)		SU Mode
Default Gateway IP Address		All
DNS (Primary and Secondary Address)		All
NAT		
Status	ADVANCED CONFIGURATION -> Network -> NAT	SU Mode / End Mode B mode
Dynamic Start Port	ADVANCED CONFIGURATION -> Network -> NAT	SU Mode / End Mode B mode
Dynamic End Port	ADVANCED CONFIGURATION -> Network -> NAT	SU Mode / End Mode B mode
PPPoE		
Status	ADVANCED CONFIGURATION -> Network -> PPPoE Client	SU Mode
Ethernet Interface Properties		
Admin Status	ADVANCED CONFIGURATION -> Network -> Ethernet	All
Wireless Interface Properties		
Legacy Mode	ADVANCED CONFIGURATION > Wireless > Interface 1 > Properties > 'Basic' Tab	All
Sync Status	ADVANCED CONFIGURATION > Wireless > Interface 1 > Properties > 'Sync' Tab	BSU Mode Applicable to the devices • MP-8200-BSU-G • MP-8250-BS9-G • MP-8250-BS1-G • MP-8200-BSU • MP-8250-BS9 • MP-8250-BS1 • MP-820-BSU-100 • MP-822-BSU-100 • MP-825-BS3-100
Upgrade Firmware and Configuration		
Upgrade Firmware	MANAGEMENT -> File Management -> Upgrade Firmware	All
Upgrade Configuration	MANAGEMENT -> File Management -> Upgrade Configuration	All

Parameter(s)	Web Page(s)	Applicable Device Mode*
Upgrade License	MANAGEMENT -> File Management -> Upgrade License	Applicable only to, • MP-820-SUA • MP-822-SUA • MP-825-SUR • MP-825-CPE • MP-835-CPE • MP-8100-SUA • MP-8150-SUR • MP-8150-SUR-100 • MP-8200-BSU-G • MP-8200-BSU • MP-8200-SUA • MP-8250-BS9-G • MP-8250-BS1-G • MP-8250-BS9 • MP-8250-BS1 • MP-825-BS3-100 • MP-820-BSU-100 • MP-822-BSU-100 • MP-8250-SUR
HTTP / HTTPS		
Admin Password	MANAGEMENT -> Services -> HTTP / HTTPS	All
Monitor Password		All
HTTP		All
HTTP Port		All
HTTPS		All
SNMP (If SNMP v1-v2c is enabled)		
SNMP	MANAGEMENT -> Services -> SNMP	All
Version		All
Read Password		All
Read / Write Password		All
SNMP Trap Host Table		All
SNMP (If SNMP v3 is enabled)		

Parameter(s)	Web Page(s)	Applicable Device Mode*
SNMP	MANAGEMENT -> Services -> SNMP	All
Version		All
Security Level		All
Priv Protocol		All
Priv Password		All
Auth Protocol		All
Auth Password		All
SNMP Trap Host Table		All
Telnet / SSH		
Admin Password	MANAGEMENT -> Services -> Telnet / SSH	All
Monitor Password		All
Telnet		All
Telnet Port		All
Telnet Sessions		All
SSH		All
SSH Port		All
SSH Sessions		All
Management Access Control		
Access Table Status	MANAGEMENT -> Access Control	All
Management Access Control Table		All
Reset to Factory	MANAGEMENT -> Reset to Factory	All
Convert QB to MP	MANAGEMENT -> Convert QB to MP	Applicable only to • QB-8200-EPA-G/LNK-G • QB-8200-EPA/LNK • QB-825-EPR/LNK -50^{+} • QB-825-EPR/LNK -100 • QB-835-EPR/LNK -25 • QB-835-EPR/LNK -50 • QB-826-EPR/LNK-100

* **BSU**: Refers to a Base Station
SU Mode: Refers to both SU and CPE
End Point A Mode: Refers to a device in End Point A mode
End Point B Mode: Refers to a device in End Point B mode

C Frequency Domains and Channels

Introduction

The Tsunami® point-to-point and point-to-multipoint products are available in two SKUs: United States (US) and rest of the World (WD) markets. Depending on the SKU, the device is hard programmed at factory per the regulatory domain. Regulatory domain controls the list of frequency domains that are available in that SKU. Further each frequency domain will define the country specific regulatory rules and frequency bands. The frequency domains can be easily configured using the Web Interface as it is a drop down list with all the available domains. The following table lists all the Tsunami® 800 and 8000 Series products with the applicable frequency domains and their corresponding ENUM values, SKUs supported and licensed frequency bands.

US Frequency Domains

Point to Multipoint Devices								
Product(s)				MP-8100-SUA	MP-8150-SUR MP-8150-SUR-100	MP-8200-BSU-G MP-8200-BSU MP-8200-SUA MP-8250-BS9 / BS1-G MP-8250-BS9 / BS1 MP-8250-SUR		MP-820-SUA-50+ MP-820-SUA-100 MP-825-CPE-50 MP-825-CPE-100 MP-835-CPE-10 MP-835-CPE-25 MP-835-CPE-50 MP-835-CPE-100 MP-825-SUR-50+ MP-825-SUR-100 MP-825-BS3-100 MP-820-BSU-100
				US	US	US (For Products manufactured prior 1st June 2016)	US (For Products manufactured after 1st June 2016)	US
	Licensed Bands (in GHz)			2.4, 4.9, 5.0	5.0	4.9, 5.0	4.9, 5.0	4.9 L mask 5.0
Frequency Domains	United States 5 GHz - US*	ENUM Values	1			✓		✓
	United States 5.8 GHz - US*		2	✓	✓	✓	✓	✓
	United States 2.4 GHz - US*		3	✓				
	US2 (5.3 and 5.8 GHz) - US*		22	✓	✓	✓		✓
	United States 4.9 GHz		28			✓	✓	✓
	US3 (5.2 and 5.8 GHz) - US*		38	✓	✓	✓	✓	✓
	US4 (4.9 and 5 GHz) - US*		44			✓	✓ **	✓
	US1 (5.3 and 5.4 GHz) - US*		45					✓

* Applicable to US SKU only
# US SKU is not applicable to QB-8150-LNK-12
** For US4, 5.3 and 5.4 GHz bands are not available.

Point to Point Devices				
Product(s)		QB-8200-EPA-G/LNK-G QB-8250-EPR-G/LNK-G QB-8200-EPA/LNK QB-8250-EPR/LNK		QB-825-EPR/LNK-100 QB-825-EPR/LNK-50 QB-835-EPR/LNK-25 QB-835-EPR/LNK-50
		US (For Products prior 1st June 2016)	US (For Products after 1st June 2016)	US
Licensed Bands (in GHz)		4.9, 5.0	4.9, 5.0	4.9 L mask 5.0
Frequency Domains	ENUM Values			
United States 5 GHz - US*	1	✓		✓
United States 5.8 GHz - US*	2	✓	✓	✓
United States 2.4 GHz - US*	3			
US2 (5.3 and 5.8 GHz) - US*	22	✓		✓
United States 4.9 GHz	28	✓	✓	✓
US3 (5.2 and 5.8 GHz) - US*	38	✓	✓	✓
US4 (4.9 and 5 GHz) - US*	44	✓	✓ **	✓
US1 (5.3 and 5.4 GHz) - US*	45			✓

* Applicable to US SKU only
# US SKU is not applicable to QB-8150-LNK-12
** For US4, 5.3 and 5.4 GHz bands are not available.

World Frequency Domains

Point to Multipoint Devices							
Product(s)				MP-8100-SUA	MP-8150-SUR MP-8150-SUR-100	MP-8200-BSU-G MP-8200-SUA MP-8250-BS9 / BS1-G MP-8250-SUR MP-820-SUA-50^{+} MP-820-BSU-100 MP-8200-BSU MP-8250-BS9 MP-8250-BS1	MP-825-SUR-50^{+} MP-825-CPE-50 MP-825-CPE-100 MP-835-CPE-10 MP-835-CPE-25 MP-835-CPE-50 MP-835-CPE-100 MP-825-BS3-100
				WD	WD	WD	WD
Licensed Bands (in GHz)				2.4, 4.9, 5.0	4.9, 5.0	4.9, 5.0	4.9 L mask 5.0
Frequency Domains	World 5 GHz	ENUM Values	4	✓	✓	✓	✓
	World 4.9 GHz		5	✓	✓	✓	✓
	World 2.4 GHz		6	✓			
	World 2.3 GHz		7	✓			
	World 2.5 GHz		8	✓			
	Canada 5 GHz		9	✓	✓	✓	✓
	WD Europe 5.8 GHz		10	✓	✓	✓	✓
	WD Europe 5.4 GHz		11	✓	✓	✓	✓
	WD-Europe 2.4 GHz		12	✓			
	Russia 5 GHz		13	✓	✓	✓	✓
	Taiwan 5 GHz		14	✓	✓	✓	✓
	WD United States 5 GHz		1	✓	✓	✓	✓
	Canada 5.8 GHz		16	✓	✓	✓	✓
	World 6.4 GHz		17				
	WD UK 5.8 GHz		20	✓	✓	✓	✓
	World 5.9 GHz		21	✓	✓	✓	✓
	India 5.8 GHz		23	✓	✓	✓	✓
	Brazil 5.4 GHz		24	✓	✓	✓	✓
	Brazil 5.8 GHz		25	✓	✓	✓	✓
	Australia 5.4 GHz		26	✓	✓	✓	✓
	Australia 5.8 GHz		27	✓	✓	✓	✓
	WD United States 4.9 GHz		28			✓	✓
	Canada 4.9 GHz		30			✓	✓
	WD Japan 4.9 GHz		19			✓	
	Legacy 5GHz		32	✓	✓	✓	✓
	WD Japan 5.6 GHz		33			✓	✓
	WD United States 5.8		2			✓	✓
	World 5.8 GHz		35	✓	✓	✓	✓
	Indonesia 5.7 GHz		36	✓	✓	✓	✓
	Egypt 5.8 GHz		39	✓	✓	✓	✓

Point to Point Devices						
Product(s)				QB-8200-EPA-G/LNK-G QB-8250-EPR-G/LNK-G QB-8200-EPA/LNK QB-8250-EPR/LNK	QB-825-EPR/LNK-50 QB-825-EPR/LNK-100 QB-835-EPR/LNK-25 QB-835-EPR/LNK-50	QB-826-EPR/LNK-100
				WD	WD	WD
Licensed Bands (in GHz)				4.9, 5.0	4.9 L mask 5.0	6.4
Frequency Domains	World 5 GHz	ENUM Values	4	✓	✓	
	World 4.9 GHz		5	✓	✓	
	World 2.4 GHz		6			
	World 2.3 GHz		7			
	World 2.5 GHz		8			
	Canada 5 GHz		9	✓	✓	
	WD-Europe 5.8 GHz		10	✓	✓	
	WD-Europe 5.4 GHz		11	✓	✓	
	WD-Europe 2.4 GHz		12			
	Russia 5 GHz		13	✓	✓	
	Taiwan 5 GHz		14	✓	✓	
	WD United States 5 GHz		1	✓	✓	
	Canada 5.8 GHz		16	✓	✓	
	World 6.4 GHz		17			✓
	World UK 5.8 GHz		20	✓	✓	
	World 5.9 GHz		21	✓	✓	
	India 5.8 GHz		23	✓	✓	
	Brazil 5.4 GHz		24	✓	✓	
	Brazil 5.8 GHz		25	✓	✓	
	Australia 5.4 GHz		26	✓	✓	
	Australia 5.8 GHz		27	✓	✓	
	WD United States 4.9 GHz		28	✓	✓	
	Canada 4.9 GHz		30	✓	✓	
	WD Japan 4.9 GHz		19	✓		
	Legacy 5 GHz		32	✓	✓	
	WD Japan 5.6 GHz		33	✓	✓	
	WD United States 5.8 GHz		2	✓	✓	
	World 5.8 GHz		35	✓	✓	
	Indonesia 5.7 GHz		36	✓	✓	
	Egypt 5.8 GHz		39	✓	✓	
	US4 (4.9 and 5 GHz)		44	✓	✓	

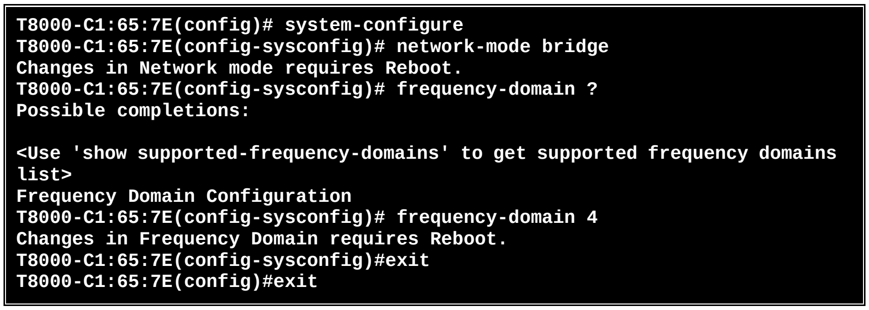
Europe Frequency Domains

Point to Multipoint Devices								
Product(s)				MP-8100-SUA	MP-8150-SUR MP-8150-SUR-100	MP-8200-BSU-G MP-8200-SUA MP-8250-BS9-G MP-8250-SUR MP-820-BSU-100 MP-8200-BSU MP-8250-BS9 MP-8250-BS1	MP-820-SUA-50^{+}	MP-825-SUR-50^{+} MP-825-CPE-50 MP-825-CPE-100 MP-835-CPE-10 MP-835-CPE-25 MP-835-CPE-50 MP-835-CPE-100 MP-825-BS3-50^{+}
				EU	EU	EU	EU	EU
Licensed Bands (in GHz)				2.4, 4.9, 5.0	4.9, 5.0	4.9, 5.0	4.9, 5.0	5.0
Frequency Domains	UK 5.8 GHz	ENUM Values	20	✓	✓	✓	✓	✓
	Europe 5.8 GHz		10	✓	✓	✓	✓	✓
	Europe 5.4 GHz		11	✓	✓	✓	✓	✓
	Europe 2.4 GHz		12	✓				

Point to Point Devices					
Product(s)				QB-8200-EPA-G/LNK-G QB-8250-EPR-G/LNK-G QB-8200-EPA/LNK QB-8250-EPR/LNK	QB-825-EPR/LNK-50^{+} QB-825-EPR/LNK-100 QB-835-EPR/LNK-25 QB-835-EPR/LNK-50
				EU	EU
Licensed Bands (in GHz)				4.9, 5.0	5.0
Frequency Domains	UK 5.8 GHz	ENUM Values	20	✓	✓
	Europe 5.8 GHz		10	✓	✓
	Europe 5.4 GHz		11	✓	✓
	Europe 2.4 GHz		12		

When the device is configured by using CLI or SNMP, care has to be taken to set the domains by using a predefined ENUM value.

Example: The CLI commands to set WORLD 5 GHz as frequency domain are as follows:



```
T8000-C1:65:7E(config)# system-configure
T8000-C1:65:7E(config-sysconfig)# network-mode bridge
Changes in Network mode requires Reboot.
T8000-C1:65:7E(config-sysconfig)# frequency-domain ?
Possible completions:

<Use 'show supported-frequency-domains' to get supported frequency domains
list>
Frequency Domain Configuration
T8000-C1:65:7E(config-sysconfig)# frequency-domain 4
Changes in Frequency Domain requires Reboot.
T8000-C1:65:7E(config-sysconfig)#exit
T8000-C1:65:7E(config)#exit
```

❗ *: All DFS countries support only 20 and 40 MHz channel bandwidths.*

Thailand Frequency Domains

Point to Multipoint Devices						
Product(s)				**MP-8250-SUR**	**MP-8250-BS9**	**MP-825-CPE-50** **MP-835-CPE-10** **MP-835-CPE-25** **MP-835-CPE-50** **MP-835-CPE-100**
				Thailand	**Thailand**	**Thailand**
	Licensed Bands (in GHz)			**5.0** **4.9**	**5.0** **4.9**	**5.0**
Frequency Domains	Thailand 5.2 GHz	**ENUM Values**	42	✓	✓	✓
	Thailand 5.6 GHz		43	✓	✓	✓

Point to Point Devices					
Product(s)				**QB-8250-EPR**	**QB-825-EPR/LNK-50^{+}** **QB-825-EPR/LNK-100** **QB-835-EPR/LNK-25** **QB-835-EPR/LNK-50**
				Thailand	**Thailand**
Licensed Bands (in GHz)				**5.0** **4.9**	**5.0**
Frequency Domains	Thailand 5.2 GHz	**ENUM Values**	42	✓	✓
	Thailand 5.6 GHz		43	✓	✓

IC(Industry Canada) 5.2 GHz Frequency Domains

Point to Multipoint Devices				
Product(s)				**MP-822-BSU-100** **MP-822-SUA-100**
				Canada
	Licensed Bands (in GHz)			**(5.150 - 5.250)**
Frequency Domains	Industry Canada 5.2 GHz	**ENUM Values**	45	✓

2.4 GHz Channels

Frequency Domain	Frequency Band (Start Frequency ~ End Frequency in MHz)	Allowed Channels (Center Frequency in GHz)				
		5 MHz	10 MHz	20 MHz	40 PLUS MHz	40 MINUS MHz
US SKU						
United States 2.4 GHz	2412 ~ 2462	1 (2412), 2 (2417)... 10 (2457), 11 (2462).	1 (2412), 2 (2417)... 10 (2457), 11 (2462).	1 (2412), 2 (2417)... 10 (2457), 11 (2462).	1 (2412), 2 (2417)... 6 (2437), 7 (2442).	5 (2432), 6 (2437)... 10 (2457), 11 (2462).
World SKU						
World 2.3 GHz	2277 ~ 2397	100 (2277), 101 (2282)... 123 (2392), 124 (2397).	100 (2277), 101 (2282)... 122 (2387), 123 (2392).	101 (2282), 102 (2287)... 121(2382), 122 (2387).	101 (2282), 102 (2287)... 117 (2362), 118 (2367).	105 (2302), 106(2307)... 121(2382), 122 (2387).
World 2.4 GHz	2412 ~ 2472	1 (2412), 2 (2417)... 12 (2467), 13 (2472).	1 (2412), 2 (2417)... 12 (2467), 13 (2472).	1 (2412), 2 (2417)... 12 (2467), 13 (2472).	1 (2412), 2 (2417)... 8 (2447), 9 (2452).	5 (2432), 6 (2437)... 12 (2467), 13 (2472).
World 2.5 GHz	2477 ~ 2507	200(2477), 201(2482)... 205 (2502), 206(2507).	200(2477), 201(2482)... 205 (2502), 206(2507).	201(2482), 202 (2487)... 204(2497), 205 (2502).	-	-
WD-Europe 2.4 GHz	2412 ~ 2472	1 (2412), 2 (2417)... 12 (2467), 13 (2472).	1 (2412), 2 (2417)... 12 (2467), 13 (2472).	1 (2412), 2 (2417)... 12 (2467), 13 (2472).	1 (2412), 2 (2417)... 8 (2447), 9 (2452).	5 (2432), 6 (2437)... 12 (2467), 13 (2472).
EU SKU						
Europe 2.4 GHz	2412 ~ 2472	1 (2412), 2 (2417)... 12 (2467), 13 (2472).	1 (2412), 2 (2417)... 12 (2467), 13 (2472).	1 (2412), 2 (2417)... 12 (2467), 13 (2472).	1 (2412), 2 (2417)... 8 (2447), 9 (2452).	5 (2432), 6 (2437)... 12 (2467), 13 (2472).

4.9 and 5 GHz Channels

Frequency Domain	Frequency Band (Start Frequency ~ End Frequency in MHz)	Allowed Channels (Center Frequency in GHz)				
		5 MHz	10 MHz	20 MHz	40 PLUS MHz	40 MINUS MHz
US SKU						
United States 5 GHz	5180 ~ 5240 (Non-DFS) 5260 ~ 5320 (DFS) 5500 ~ 5580 (DFS) 5660 ~ 5700 (DFS) 5745 ~ 5825 (non-DFS)	-	-	36(5180), 37(5185), 38(5190), 39(5195), 40(5200), 41(5205), 42(5210), 43(5215), 44(5220), 45(5225), 46(5230), 47(5235), 48(5240), 52(5260), 53(5265)... 63(5315), 64(5320). 100(5500), 101(5505)... 115(5575), 116(5580). 132(5660), 133(5665)... 139(5695), 140(5700). 149(5745), 150(5750)... 164(5820), 165(5825).	36(5180), 37(5185), 38(5190), 39(5195), 40(5200), 41(5205), 42(5210), 43(5215), 44(5220), 52(5260), 53(5265)... 59(5295), 60(5300). 100(5500), 101(5505)... 111(5555), 112(5560). 133(5665), 134(5670)... 135(5675), 136(5680). 149(5745), 150(5750)... 160(5800), 161(5805).	40(5200), 41(5205), 42(5210), 43(5215), 44(5220), 45(5225), 46(5230), 47(5235), 48(5240), 56(5280), 57(5285)... 63(5315), 64(5320). 104(5520), 105(5525)... 115(5575), 116(5580). 136(5680), 137(5685)... 139(5695), 140(5700). 153(5765), 154(5770)... 164(5820), 165(5825).
United States 5.8 GHz	5740 ~ 5830 (Non-DFS)	148(5740), 149(5745)... 165(5825), 166(5830).	149(5745), 150(5750)... 164(5820), 165(5825).	149(5745), 150(5750)... 164(5820), 165(5825).	149(5745), 150(5750)... 160(5800), 161(5805).	153(5765), 154(5770)... 164(5820), 165(5825).
United States2 (5.3, 5.8 GHz)	5260 ~ 5320 (DFS) 5745 ~ 5825 (Non-DFS)	-	-	52(5260), 53(5265)... 63(5315), 64(5320). 149(5745), 150(5750)... 164(5820), 165(5825).	52(5260), 53(5265)... 59(5295), 60(5300). 149(5745), 150(5750)... 160(5800), 161(5805).	56(5280), 57(5285)... 63(5315), 64(5320). 153(5765), 154(5770)... 164(5820), 165(5825).
United States 4.9 GHz	4942 ~ 4987 (Non-DFS)	5(4942.5), 15(4947.5)... 85(4982.5), 95(4987.5).	10(4945), 20(4950)... 80(4980), 90(4985).	20(4950), 30(4955)... 70(4975), 80(4980).	-	-

Frequency Domain	Frequency Band (Start Frequency ~ End Frequency in MHz)	Allowed Channels (Center Frequency in GHz)				
		5 MHz	10 MHz	20 MHz	40 PLUS MHz	40 MINUS MHz
United States3 (5.2, 5.8 GHz)	5180 ~ 5240 (Non-DFS) 5745 ~ 5825 (Non-DFS) *Please note that all 82x and 8xxx SKUs support this frequency.*	36(5180), 37(5185), 38(5190), 39(5195), 40(5200), 41(5205), 42(5210), 43(5215), 44(5220), 45(5225), 46(5230), 47(5235), 48(5240), 148(5740), 149(5745)... 165(5825), 166(5830).	36(5180), 37(5185), 38(5190), 39(5195), 40(5200), 41(5205), 42(5210), 43(5215), 44(5220), 45(5225), 46(5230), 47(5235), 48(5240), 149(5745), 150(5750)... 164(5820), 165(5825).	36(5180), 37(5185), 38(5190), 39(5195), 40(5200), 41(5205), 42(5210), 43(5215), 44(5220), 45(5225), 46(5230), 47(5235), 48(5240), 149(5745), 150(5750)... 164(5820), 165(5825).	36(5180), 37(5185), 38(5190), 39(5195), 40(5200), 41(5205), 42(5210), 43(5215), 44(5220), 149(5745), 150(5750)... 160(5800), 161(5805).	40(5200), 41(5205), 42(5210), 43(5215), 44(5220), 45(5225), 46(5230), 47(5235), 48(5240), 153(5765), 154(5770)... 164(5820), 165(5825).
United States4 (4.9, 5 GHz)	4950 - 4980 (Non-DFS) 5180 - 5195 (Non-DFS) 5205 - 5240 (Non-DFS) 5260 - 5295 (DFS) 5305 - 5320 (DFS) 5500 - 5580 (DFS) 5660 - 5700 (DFS) 5745 - 5825 (Non-DFS)	-	-	20 (4950), 30 (4955), 40 (4960), 50 (4965), 60 (4970), 70 (4975), 80 (4980). 36 (5180), 37 (5185), 38 (5190), 39 (5195). 41 (5205), 42 (5210).... 47 (5235), 48 (5240). 52 (5260), 53 (5265).... 58 (5290), 59 (5295). 61 (5305), 62 (5310), 63 (5315), 64 (5320). 100 (5500), 101 (5505).... 115 (5575), 116 (5580). 132 (5660), 133 (5665).... 139 (5695), 140 (5700). 149 (5745), 150 (5750).... 164 (5820), 165 (5825).	-	-
Japan SKU						
Japan 4.9 GHz	4912 ~ 4980 (Non-DFS)	182(4912.5), 183(4917.5)... 188(4942.5), 189(4947.5).	183(4915), 184(4920)... 188(4940), 189(4945).	184(4920), 188(4940), 192(4960), 196(4980).	184(4920), 192(4960).	188(4940), 196(4980).

Frequency Domain	Frequency Band (Start Frequency ~ End Frequency in MHz)	Allowed Channels (Center Frequency in GHz)				
		5 MHz	10 MHz	20 MHz	40 PLUS MHz	40 MINUS MHz

Japan 5.6 GHz	5500 ~ 5700 (DFS)	-	-	100(5500)
				104(5520)
				108(5540)
				112(5560)
				116(5580)
				120(5600)
				124(5620)
				128(5640)
				132(5660)
				136(5680)
				140(5700)
					100(5500)
					108(5540)
					116(5580)
					124(5620)
					136(5680)
						104(5520)
						112(5560)
						120(5600)
						128(5640)
						140(5700)

World SKU						
WD United States 5 GHz	5180 ~ 5240 (Non-DFS) 5260 ~ 5320 (DFS) 5500 ~ 5580 (DFS) 5660 ~ 5700 (DFS) 5745 ~ 5825 (non-DFS)	-	-	36(5180), 37(5185), 38(5190), 39(5195), 40(5200), 41(5205), 42(5210), 43(5215), 44(5220), 45(5225), 46(5230), 47(5235), 48(5240), 52(5260), 53(5265)... 63(5315), 64(5320). 100(5500), 101(5505)... 115(5575), 116(5580). 132(5660), 133(5665)... 139(5695), 140(5700). 149(5745), 150(5750)... 164(5820), 165(5825).	36(5180), 37(5185), 38(5190), 39(5195), 40(5200), 41(5205), 42(5210), 43(5215), 44(5220), 52(5260), 53(5265)... 59(5295), 60(5300). 100(5500), 101(5505)... 111(5555), 112(5560). 133(5665), 134(5670)... 135(5675), 136(5680). 149(5745), 150(5750)... 160(5800), 161(5805).	40(5200), 41(5205), 42(5210), 43(5215), 44(5220), 45(5225), 46(5230), 47(5235), 48(5240), 56(5280), 57(5285)... 63(5315), 64(5320). 104(5520), 105(5525)... 115(5575), 116(5580). 136(5680), 137(5685)... 139(5695), 140(5700). 153(5765), 154(5770)... 164(5820), 165(5825).
World 5 GHz	5155 ~ 6075 (Non-DFS) *Please note that 8200 & 82x SKUs support upto 5920 MHz frequency.*	31(5155), 32(5160)... 214(6070), 215(6075).	31(5155), 32(5160)... 214(6070), 215(6075).	32(5160), 33(5165)... 213(6065), 214(6070).	32(5160), 33(5165)... 209(6045), 210(6050).	36(5180), 37(5185)... 213(6065), 214(6070).
World 4.9 GHz	4905 ~ 4995 (Non-DFS)	181(4905), 182(4910)… 187(4935), 188(4940). 10(4945), 20(4950)… 100(4990), 110(4995).	181(4905), 182(4910)… 187(4935), 188(4940). 10(4945), 20(4950)… 100(4990), 110(4995).	182(4910), 183(4915)… 187(4935), 188(4940). 10(4945), 20(4950)… 90(4985), 100(4990).	182(4910), 183(4915)… 187(4935), 188(4940). 10(4945), 20(4950)… 50(4965), 60(4970).	186(4930), 187(4935), 188(4940), 10(4945), 20(4950)… 90(4985), 100(4990).

Frequency Domain	Frequency Band (Start Frequency ~ End Frequency in MHz)	Allowed Channels (Center Frequency in GHz)				
		5 MHz	10 MHz	20 MHz	40 PLUS MHz	40 MINUS MHz

World 5.9 GHz	5880 ~ 5920 (Non-DFS)	176(5880),
		177(5885)...
		183(5915),
		184(5920).
			176(5880),
			177(5885)...
			183(5915),
			184(5920).
				177(5885),
				178(5890)...
				182(5910),
				183(5915).
					177(5885)
					178(5890)
					179(5895)
						181(5905)
						182(5910)
						183(5915)

Canada 5 GHz	5255 ~ 5325 (DFS) 5495 ~ 5585 (DFS) 5655 ~ 5705 (DFS)	-	-	52(5260), 53(5265)... 63(5315), 64(5320). 100(5500), 101(5505)... 115(5575), 116(5580). 132(5660), 133(5665)... 139(5695), 140(5700).	52(5260), 53(5265)... 59(5295), 60(5300). 100(5500), 101(5505)... 111(5555), 112(5560). 132(5660), 133(5665)... 135(5675), 136(5680).	56(5280), 57(5285)... 63(5315), 64(5320). 104(5520), 105(5525)... 115(5575), 116(5580). 136(5680), 137(5685)... 139(5695), 140(5700).
WD-Europe 5.4 GHz	5495 ~ 5585 (DFS) 5655 ~ 5705 (DFS)	-	-	100(5500), 101(5505)... 115(5575), 116(5580). 132(5660), 133(5665)... 139(5695), 140(5700).	100(5500), 101(5505)... 111(5555), 112(5560). 132(5660), 133(5665)... 135(5675), 136(5680).	104(5520), 105(5525)... 115(5575), 116(5580). 136(5680), 137(5685)... 139(5695), 140(5700).
WD-Europe 5.8 GHz	5735 ~ 5870 (DFS)	-	-	149(5745), 150(5750)... 172(5860), 173(5865).	149(5745), 150(5750)... 168(5840), 169(5845).	153(5765), 154(5770)... 172(5860), 173(5865).
Russia 5 GHz	5155 ~ 6075 (Non-DFS) ***Please note that 8200 & 82x SKUs support upto 5920 MHz frequency.***	31(5155), 32(5160)... 214(6070), 215(6075).	31(5155), 32(5160)... 214(6070), 215(6075).	32(5160), 33(5165)... 213(6065), 214(6070).	32(5160), 33(5165)... 209(6045), 210(6050).	36(5180), 37(5185)... 213(6065), 214(6070).
Taiwan 5 GHz	5495 ~ 5705 (DFS) 5740 ~ 5810 (Non-DFS)	-	-	100(5500), 101(5505)... 139(5695), 140(5700). 149(5745), 150(5750)... 160(5800), 161(5805).	100(5500), 101(5505)... 135(5675), 136(5680). 149(5745), 150(5750)... 156(5780), 157(5785).	104(5520), 105(5525)... 139(5695), 140(5700). 153(5765), 154(5770)... 160(5800), 161(5805).

India 5.8 GHz	5830 ~ 5870 (Non-DFS)	166(5830),
		167(5835)...
		173(5865),
		174(5870).
			166(5830),
			167(5835)...
			173(5865),
			174(5870).
				167(5835),
				168(5840)...
				172(5860),
				173(5865).
					167(5835)
					168(5840)
					169(5845)
						171(5855)
						172(5860)
						173(5865)

Canada 5.8 GHz	5735 ~ 5855 (Non-DFS)	147(5735), 148(5740)... 170(5850), 171(5855).	147(5735), 148(5740)... 170(5850), 171(5855).	148(5740), 149(5745)... 169(5845), 170(5850).	148(5740), 149(5745)... 165(5825), 166(5830).	152(5760), 153(5765)... 169(5845), 170(5850).
WD U.K 5.8 GHz	5730 ~ 5790 (DFS) 5820 ~ 5845 (DFS)	-	-	147(5735), 148(5740)... 156(5780), 157(5785). 167(5835).	147(5735), 148(5740)... 152(5760), 153(5765).	151(5755), 152(5760)... 156(5780), 157(5785).

Frequency Domain	Frequency Band (Start Frequency ~ End Frequency in MHz)	Allowed Channels (Center Frequency in GHz)				
		5 MHz	10 MHz	20 MHz	40 PLUS MHz	40 MINUS MHz
Australia 5.4 GHz	5475 ~ 5595 (DFS) 5655 ~ 5720 (DFS)	-	-	96(5480), 97(5485)… 117(5585), 118(5590). 132(5660), 133(5665)… 142(5710), 143(5715).	96(5480), 97(5485)… 113(5565), 114(5570). 132(5660), 133(5665)… 138(5690), 139(5695).	100(5500), 101(5505)… 117(5585), 118(5590). 136(5680), 137(5685)… 142(5710), 143(5715).
Australia 5.8 GHz	5730 ~ 5845 (Non-DFS)	146(5730), 147(5735)… 168(5840), 169(5845).	146(5730), 147(5735)... 148(5740), 169(5845).	147(5735), 148(5740)… 167(5835), 168(5840).	147(5735), 148(5740)... 163(5815), 164(5820).	151(5755), 152(5760)… 167(5835), 168(5840).
Brazil 5.4 GHz	5475 ~ 5720 (DFS)	-	-	96(5480), 97(5485)… 142(5710), 143(5715).	96(5480), 97(5485)… 138(5690), 139(5695).	100(5500), 101(5505)… 142(5710), 143(5715).
Brazil 5.8 GHz	5730 ~ 5845 (Non-DFS)	146(5730), 147(5735)... 168(5840), 169(5845).	146(5730), 147(5735)... 168(5840), 169(5845).	147(5735), 148(5740)... 167(5835), 168(5840).	147(5735), 148(5740)... 163(5815), 164(5820).	151(5755), 152(5760)... 167(5835), 168(5840).
Canada 4.9 GHz	4945 ~ 4985 (Non-DFS)	10(4945), 20(4950)... 80(4980), 90(4985).	10(4945), 20(4950)... 80(4980), 90(4985).	20(4950), 30(4955)... 70(4975), 80(4980).	20(4950), 30(4955), 40(4960).	60(4970), 70(4975), 80(4980).
Egypt 5.8 GHz	5.725 ~ 5.85(DFS)	NA	146(5730), 147(5735)... 168(5840), 169(5845).	147(5735), 148(5740)... 167(5835), 168(5840).	NA	NA
Legacy 5GHz	5150 ~ 6080 (Non-DFS) *Please note that 8200 & 82x SKUs support upto 5920 MHz frequency.*	30(5150), 31(5155)... 215(6075), 216(6080).	30(5150), 32(5160)... 214(6070), 216(6080).	30(5150), 34(5170)... 210(6050), 216(6070).	-	-

WD Japan 4.9	4912 ~ 4980 (Non-DFS)
	Please note that 8100 SKUs does not support this frequency.
		182(4912.5),
		183(4917.5)...
		188(4942.5),
		189(4947.5).
			183(4915),
			184(4920)...
			188(4940),
			189(4945).
				184(4920),
				188(4940),
				192(4960),
				196(4980).
					184(4920)
					192(4960)
						188(4940)
						196(4980)

WD-Japan 5.6	5500 ~ 5700 (DFS)	-	-	100(5500)
				104(5520)
				108(5540)
				112(5560)
				116(5580)
				120(5600)
				124(5620)
				128(5640)
				132(5660)
				136(5680)
				140(5700)
					100(5500)
					108(5540)
					116(5580)
					124(5620)
					136(5680)
						104(5520)
						112(5560)
						120(5600)
						128(5640)
						140(5700)

WD United States 4.9 GHz	4942 ~ 4987 (Non-DFS)	5(4942.5), 15(4947.5)... 85(4982.5), 95(4987.5),	10(4945), 20(4950)... 80(4980), 90(4985).	20(4950), 30(4955)... 70(4975), 80(4980).	-	-

Frequency Domain	Frequency Band (Start Frequency ~ End Frequency in MHz)	Allowed Channels (Center Frequency in GHz)				
		5 MHz	10 MHz	20 MHz	40 PLUS MHz	40 MINUS MHz
WD United States 5.8 GHz	5740 ~ 5830 (Non-DFS)	148(5740), 149(5745)... 165(5825), 166(5830).	149(5745), 150(5750)... 164(5820), 165(5825).	149(5745), 150(5750)... 164(5820), 165(5825).	149(5745), 150(5750)... 160(5800), 161(5805).	153(5765), 154(5770)... 164(5820), 165(5825).
World 5.8 GHz	5720 ~ 5855 (Non-DFS)	144(5720), 145(5725)... 170(5850), 171(5855).	144(5720), 145(5725)... 170(5850), 171(5855).	145(5725), 146(5730)... 169(5845), 170(5850).	145(5725), 146(5730)... 165(5825), 166(5830).	149(5745), 150(5750)... 169(5845), 170(5850).
Indonesia 5.7 GHz	5730 ~ 5820 (Non-DFS)	146(5730), 147(5735)... 163(5815), 164(5820).	146(5730), 147(5735)... 163(5815), 164(5820).	147(5735), 148(5740)... 162(5810), 163(5815).	--	--
Thailand 5.2 GHz	5170 ~ 5330 (Non-DFS)	35(5170), 36(5180)..... 64(5320), 65(5330).	35(5170), 36(5180)..... 64(5320), 65(5330).	36(5180), 37(5185)... 63(5315), 64(5320).	36(5180), 37(5185)... 59(5295), 60(5300).	40(5200), 41(5205).... 63(5315), 64(5320).
Thailand 5.6 GHz	5490 ~ 5835 (Non-DFS)	99(5490), 100(5500)... 165(5825), 166(5830).	99(5490), 100(5500)... 165(5825), 166(5830).	100(5500) 101(5505)... 164(5820), 165(5825).	100(5500) 101(5505)... 160(5800), 161(5805).	104(5520), 105(5525)... 164(5820), 165(5825).
Industry Canada (IC) 5.2 GHz	5125 ~ 5250(Non-DFS)	31(5155), 32(5160), 33(5165), 34(5170), 35(5175), 36(5180), 37(5185), 38(5190), 39(5195), 40(5200), 41(5205), 42(5210), 43(5215), 44(5220), 45(5225), 46(5230), 47(5235), 48(5240), 49(5245).	31(5155), 32(5160), 33(5165), 34(5170), 35(5175), 36(5180), 37(5185), 38(5190), 39(5195), 40(5200), 41(5205), 42(5210), 43(5215), 44(5220), 45(5225), 46(5230), 47(5235), 48(5240), 49(5245).	32(5160), 33(5165), 34(5170), 35(5175), 36(5180), 37(5185), 38(5190), 39(5195), 40(5200), 41(5205), 42(5210), 43(5215), 44(5220), 45(5225), 46(5230), 47(5235), 48(5240).	32(5160), 33(5165), 34(5170), 35(5175), 36(5180), 37(5185), 38(5190), 39(5195), 40(5200), 41(5205), 42(5210), 43(5215), 44(5220).	36(5180), 37(5185), 38(5190), 39(5195), 40(5200), 41(5205), 42(5210), 43(5215), 44(5220), 45(5225), 46(5230), 47(5235), 48(5240).

Frequency Domain	Frequency Band (Start Frequency ~ End Frequency in MHz)	Allowed Channels (Center Frequency in GHz)				
		5 MHz	10 MHz	20 MHz	40 PLUS MHz	40 MINUS MHz
EU SKU						
U.K 5.8 GHz	5730 ~ 5790 (DFS) 5820 ~ 5845 (DFS)	-	-	147(5735), 148(5740)... 156(5780), 157(5785). 167(5835)	147(5735), 148(5740)... 152(5760), 153(5765).	151(5755), 152(5760)... 156(5780), 157(5785).
Europe 5.8 GHz	5735 ~ 5870 (DFS)	-	-	149(5745), 150(5750)... 172(5860), 173(5865).	149(5745), 150(5750)... 168(5840), 169(5845).	153(5765), 154(5770)... 172(5860), 173(5865).
Europe 5.4 GHz	5495 ~ 5585 (DFS) 5655 ~ 5705 (DFS)	-	-	100(5500), 101(5505)... 115(5575), 116(5580). 132(5660), 133(5665)... 139(5695), 140(5700).	100(5500), 101(5505)... 111(5555), 112(5560). 132(5660), 133(5665)... 135(5675), 136(5680).	104(5520), 105(5525)... 115(5575), 116(5580). 136(5680), 137(5685)... 139(5695), 140(5700).

6.4 GHz Channels

Frequency Domain	Frequency Band (Start Frequency ~ End Frequency in MHz)	Allowed Channels (Center Frequency)				
		5 MHz	10 MHz	20 MHz	40 PLUS MHz	40 MINUS MHz
World 6.4 GHz	5905 ~ 6420	181 (5905), 182 (5910)... 283 (6415), 284 (6420).	181 (5905), 182 (5910)... 283 (6415), 284 (6420).	182 (5910), 183 (5915)... 282 (6410), 283 (6415).	182 (5910), 183 (5915)... 278 (6390), 279 (6395).	186 (5930) 187 (5935)... 282 (6410), 283 (6415).

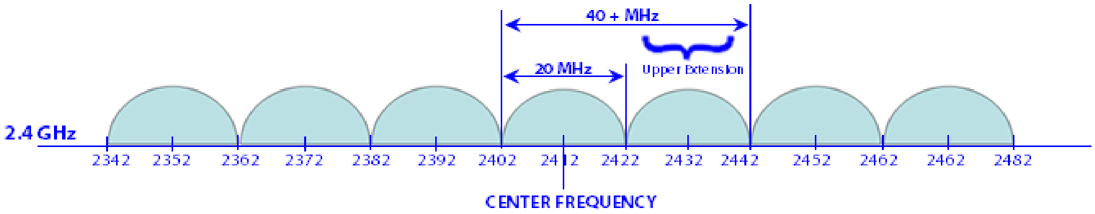
: *The center frequency listed in the above tables are based on channel offset set to '0'. If channel offset is set to any value other than '0' then the center frequency will be shifted accordingly. You can set the channel offset ranging from -2 to +2 MHz in MP-835-CPE-10, MP-835-CPE-25, MP-835-CPE-50, MP-835-CPE-100, MP-825-CPE-50, MP-825-CPE-100, MP-820-SUA-50*$^{+}$*, MP-820-SUA-100, MP-822-SUA-100, MP-825-SUR-50*$^{+}$*, MP-825-SUR-100 and QB-826-EPR/LNK-100.*

Details for 40MHz Bandwidth

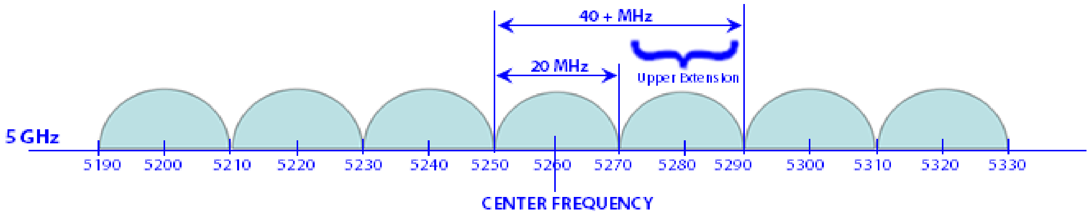
While choosing 40MHz bandwidth, you can select 40 PLUS (Upper Extension) or 40 MINUS (Lower Extension). 40 PLUS means the center frequency calculation is done for 20MHz and add another 20MHz to the top edge of 20MHz. 40 MINUS means the center frequency calculation is done for 20MHz and add another 20MHz to the bottom edge of 20MHz.

For 40 PLUS

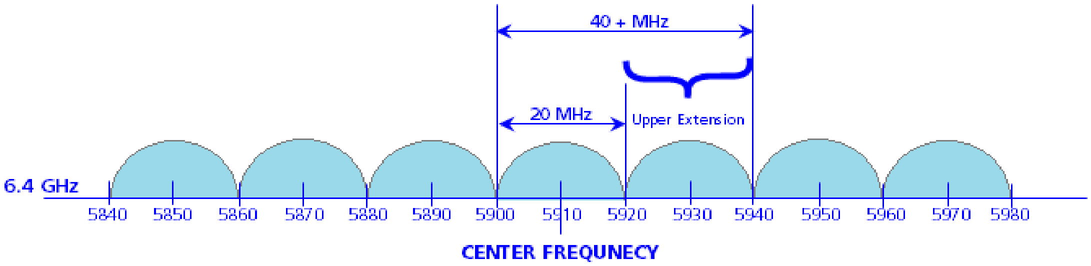
- 2.4GHz ->
  - Channel 1 = 2412 MHz
  - Bandwidth starts from 2403 MHz and ends at 2442 MHz



- 5GHz ->
  - Channel 52 = 5260 MHz
  - Bandwidth starts from 5251 MHz and ends at 5290 MHz

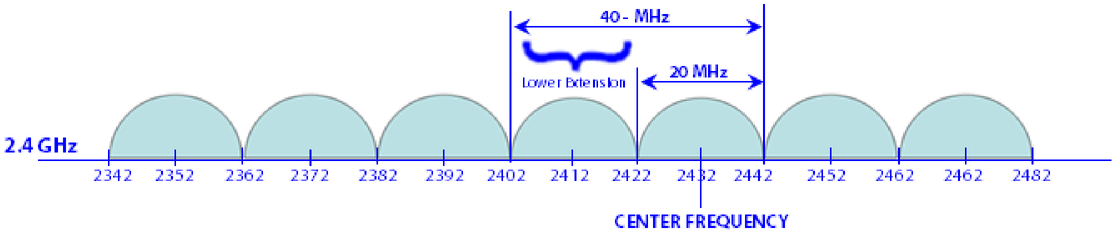


- 6.4GHz ->
  - Channel 181 = 5910 MHz
  - Bandwidth starts from 5901 MHz and ends at 5940 MHz

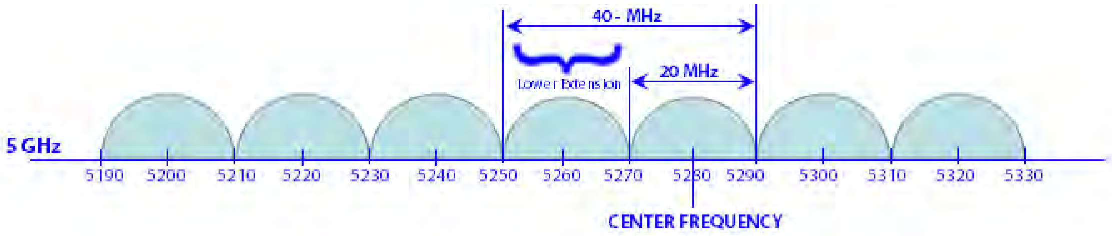


For 40 MINUS

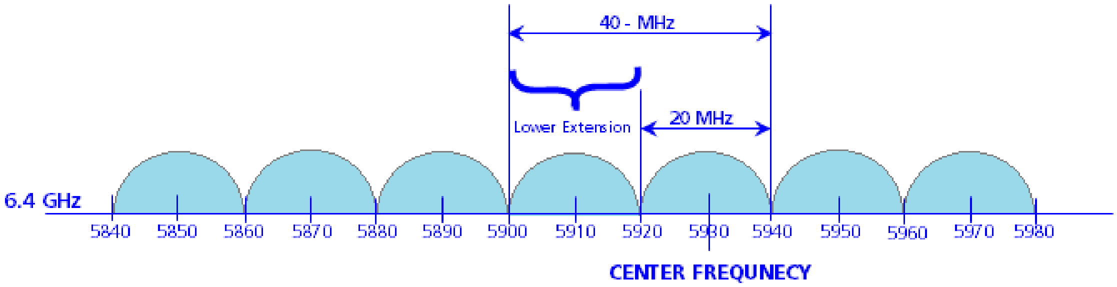
- 2.4GHz ->
  - Channel 5 = 2432 MHz
  - Bandwidth starts from 2403 MHz and ends at 2442 MHz



- 5GHz ->
  - Channel 56 = 5280 MHz
  - Bandwidth starts from 5251 MHz and ends at 5290 MHz



- 6.4GHz ->
  - Channel 186 = 5930 MHz
  - Bandwidth starts from 5901 MHz and ends at 5940 MHz



LACP - Device Management

D

Tsunami Quickbridge® devices that are part of the LACP link cannot be managed through the switches, so it is recommended to use the second Ethernet port for management.

:

- *When using second Ethernet port for management, ensure to disable Auto Shutdown for Ethernet2. See* Auto Shutdown*).*
- ***STP/LACP Frames** should be set to passthru. See* Filtering (Bridge Only)

: Whenever the Ethernet port1 is connected to CTM2 device and the Ethernet port2 is connected to PC via a passive PoE (Without the AC Power plugged in, Part No: PD-4401). Proxim recommends the usage of PD-4401 for passive PoE, as the other PoEs cannot guarentee the desired Ethernet Sync functionality

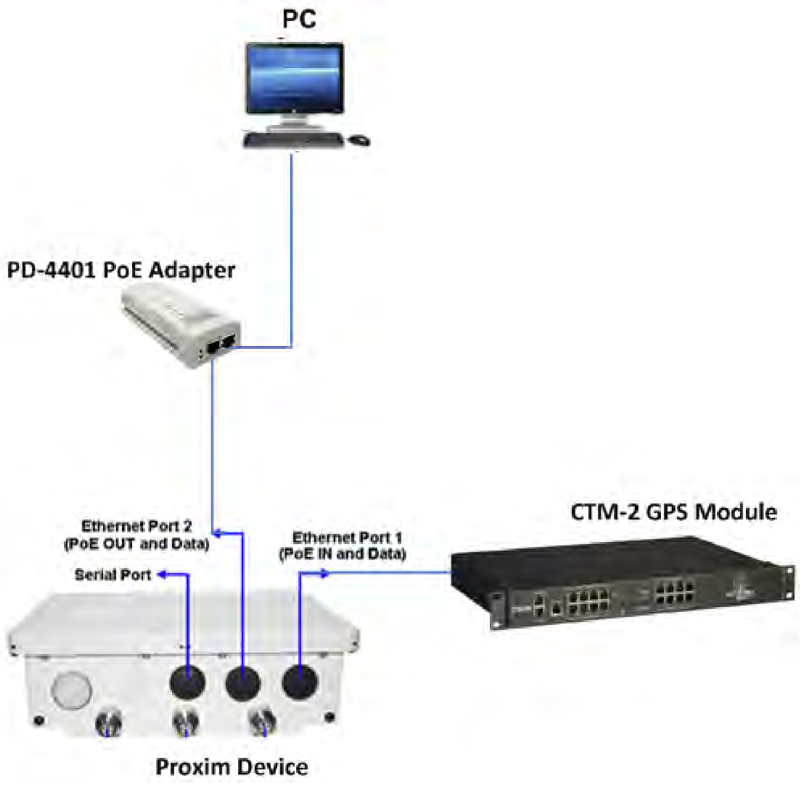


Figure D-1 Ethernet Port2 of 8xxx device connected to a PC via a Passive PoE (Proxim recommends PoE Adapter with Part number PD-4401 to be used as Passive PoE)

In this chapter, we have chosen the following two examples to explain the device management in the LACP link, by using the second Ethernet port.

Example1

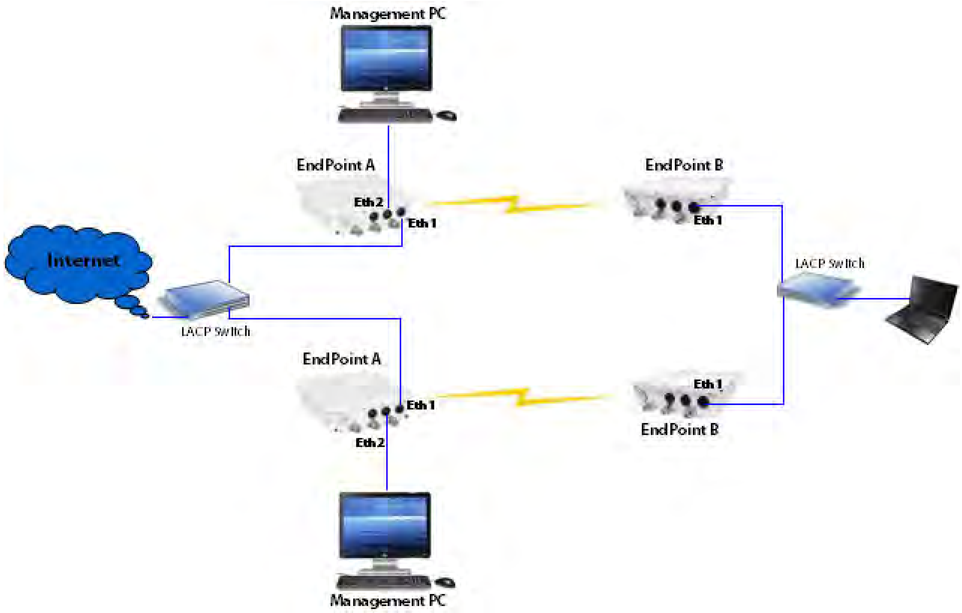


Figure D-2 Device Management with No VLAN

In this example, we have considered a network with two QuickBridge links each supporting LACP mode. In this setup, VLAN is not configured on both LACP switches and devices.

The Ethernet1 of all the devices is connected to the LACP port and is used for data transfer.

To manage the devices, use a dedicated management Personal Computer per QuickBridge link. Use Ethernet2 port of the device to connect the Personal Computer.

: In Fail Over Mode (if one of the link goes down), the remote device of a particular link cannot be managed.

Example2

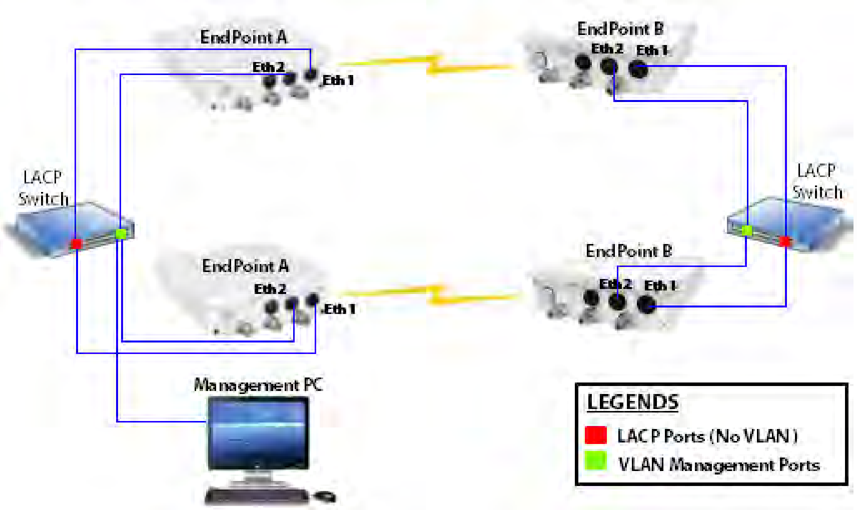


Figure D-3 Device Management with VLAN

In this example, we have considered a network with two QuickBridge links each supporting LACP mode. In this setup, Ethernet 1 of all the devices is connected to the LACP port, with no VLAN. The Ethernet 2 of all the devices is connected to the tagged VLAN management port with Spanning Tree enabled.

To manage all the devices in the QuickBridge network, use one dedicated management Personal Computer connected to the untagged VLAN port of the switch.

To manage the devices, configure same management VLAN Id on all the devices. The Ethernet 1 should be configured in transparent VLAN mode to allow data transfer. The Ethernet2 can be configured either in transparent mode or trunk mode to allow management traffic to the devices.

With Spanning Tree enabled on the LACP Switches, you will be able to manage all the QuickBridge devices, even if one of the wireless link goes down.

For VLAN configuration, refer VLAN (Bridge Mode Only).

QinQ E

The Subscribers 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 as follows:

- 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 MAN (Metropolitan Area Networks) or Intranet
- Provides customer traffic isolation at Layer 2 within a service provider network

Consider a BSU and SU network, with QinQ (**Double VLAN (Q in Q) Status**) enabled on the SU.

- **Subscriber**:
  - Based on the Ethernet VLAN configuration on the Subscriber, the data packets are tagged as follows:
    - **Access Mode**: SU double tags the packet with Access VLAN ID as inner tag and Service VLAN ID as outer tag.

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

    - **Trunk Mode**: SU expects a tagged packet (inner tag) and tags the packet with Service VLAN ID as outer tag.

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

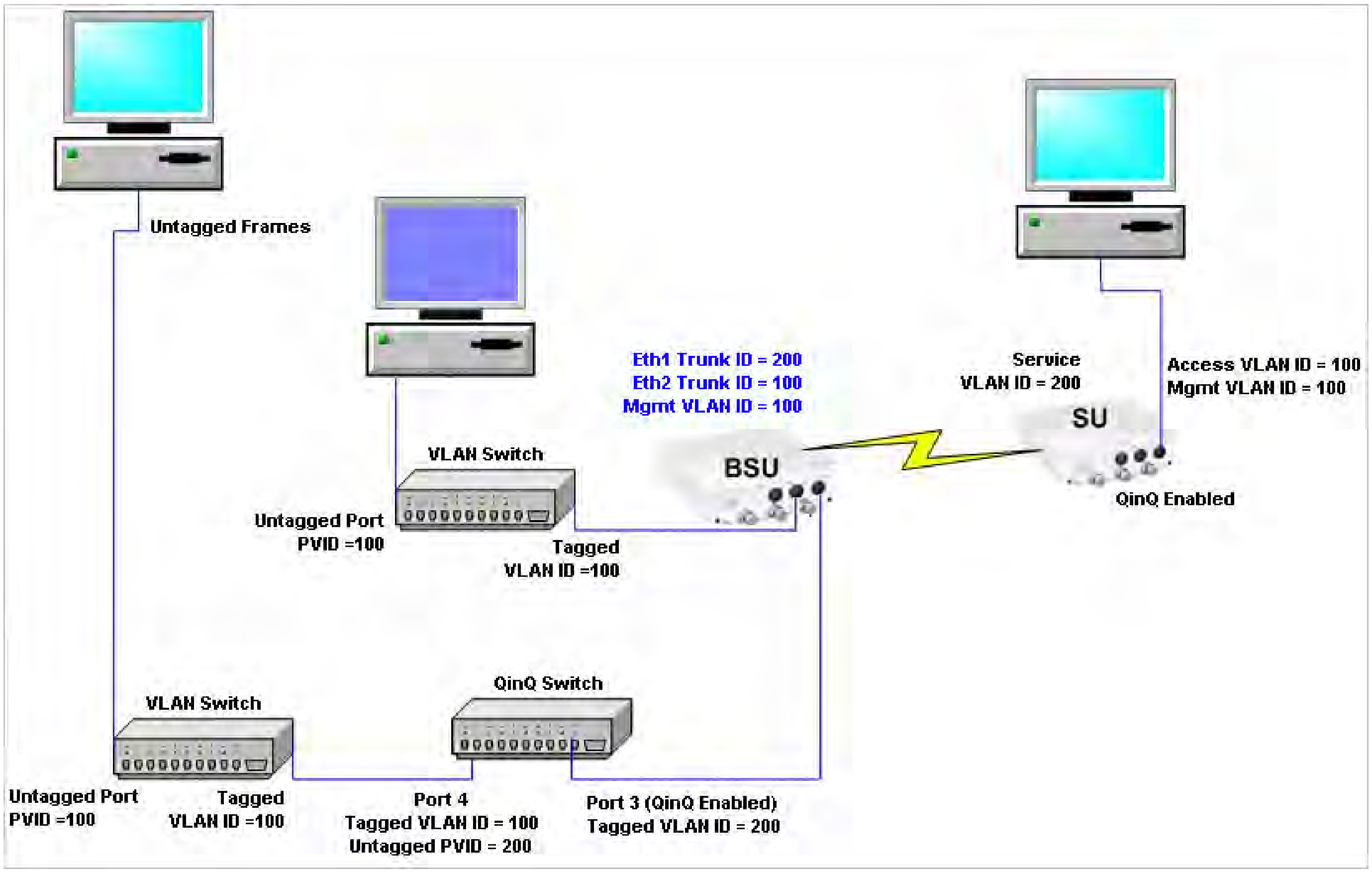
    - **Transparent Mode**: When QinQ is enabled, SU cannot be configured in the Transparent mode.
  - In case of downlink traffic, SU always expects double tagged packet from the wireless side. If the outer VLAN tag matches with Service VLAN ID then SU will untag the packet and forward to Ethernet. Based on Ethernet VLAN configuration, the data packets are handled accordingly. When the outer VLAN tag does not match the Service VLAN ID, the packet is dropped.
  - Different outer VLAN IDs can be configured for different SUs, but those VLAN IDs should also be configured on the BSU Ethernet.
- **Base Station**:
  - BSU always considers the first VLAN tag available in the packet; in case of double tagged packet it is the outer VLAN ID.
    - **Trunk Mode**: The outer tag of the packet arriving at the Ethernet side should match with the VLAN ID configured in the trunk table.
    - **Transparent Mode**: When configured in transparent mode, ensure the data packet is double tagged.
- **Device Management**
  - From the BSU Ethernet side, the BSU/SU can be managed with a single VLAN tagged packet that matches the Management VLAN ID.
  - From the SU Ethernet side, only SU can be managed with a single VLAN tagged packet that matches the Management VLAN ID; BSU cannot be managed from the SU Ethernet side.

:

- *In a QuickBridge link, Q-in-Q should be enabled either on an End Point A or an End Point B.*
- *The user configurable TPID is only used in the Service Provider VLAN tag. The Inner or customer VLAN tag should always have TPID as 0x8100.*

An Example:

The following diagram is the pictorial representation of how traffic flows in a QinQ enabled network.



The Computer behind SU can be used to manage the SU.

To manage BSU, connect another Computer to BSU Ethernet port through a VLAN switch with PVID as 100.

BSU Redundancy

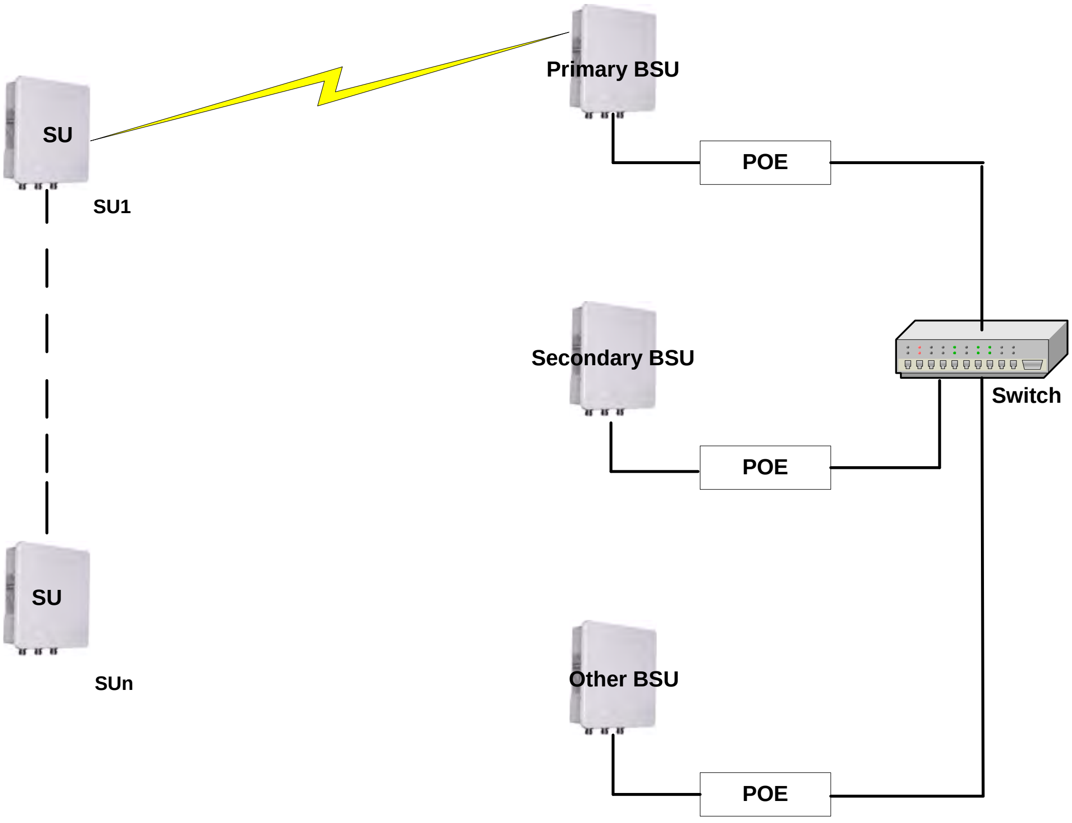
The BSU Redundancy feature can help in reducing the network outage in case of the Primary BSU failure. This feature enables the SU to keep track of the Primary and the Secondary BSU availability through a proprietary protocol. This allows the SU to switch between the Primary and the Secondary BSU depending on the link status. If both the BSUs are not available, the SU attempts to find any other BSU within its network.

Configuration Guidelines

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.
- The Primary and the Secondary BSU names should be unique.
- 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.

Example



The Primary and the Secondary BSUs are in the same L2 Broadcast domain.

Figure F-1 An Example - BSU Redundancy Feature

Log Samples for BSU Redundancy

SU - During Boot Up

- Channel 160 is set as the current channel.
- SU is trying to register with BSU: BSU1 (MAC: 00:0b:6b:b7:4c:26).
- SU received QoS Class: Unlimited Best Effort (indx: 1).
- SU registered with BSU: BSU1 (MAC: 00:0b:6b:b7:4c:26) on channel 160(0x14004A0) (SNR: A1:46 A2:0 A3:40[dB]) at WORP port[0].
- Link Profile Index: 1.
- Wireless: WORP Link Established with **Primary BSU: BSU1**
- Wireless: **SU discovered Secondary BSU:BSU2 on channel:60**
- After getting connected to the Primary BSU, the SU should discover the secondary BSU.

Primary BSU Down - Connected to Secondary BSU

- **SU unregistered from BSU: BSU1 (MAC: 00:0b:6b:b7:4c:26)**.
- Channel 60 is set as the current channel.
- **SU is trying to register with BSU: BSU2 (MAC: 00:0b:6b:b7:4b:ff)**.
- SU received QoS Class: Unlimited Best Effort (indx: 1).
- SU registered with BSU: BSU2 (MAC: 00:0b:6b:b7:4b:ff) on channel 60(0x78043C) (SNR: A1:51 A2:0 A3:49[dB]) at WORP port[0].
- kernel:Worp: Link Profile Index: 1.
- Wireless: WORP Link Established with Secondary BSU: BSU2

Connected to Other BSU

- 01:52:25 kernel:Worp: WARNING: Channel 100 is set as the current channel.
- 01:52:25 kernel:Worp: SU is trying to register with BSU: BSU3 (MAC: 00:20:a6:d3:ed:e5).
- 01:52:25 kernel:Worp: SU received QoS Class: Unlimited Best Effort (index: 1).
- 01:52:25 kernel:Worp: SU registered with BSU: BSU3 (MAC: 00:20:a6:d3:ed:e5) on channel 100(0xC80464) (SNR: A1:58 A2:0 A3:54[dB]) at WORP port[0].
- 01:52:25 kernel:Worp: Link Profile Index: 1.
- 01:52:25: Wireless: WORP Link Established with Other BSU: BSU3
- 01:54:35: Wireless: **SU discovered Secondary BSU:BSU2 on channel:60**
- 01:54:35: Wireless: **SU discovered Primary BSU:BSU1 on channel:160**
- SU should discover both the Primary and the Secondary BSU, and connect to the Primary BSU after the switch time interval.

BSU Switch Time Interval - 15 Minutes

- 1Wireless: WORP Link Established with Secondary BSU: BSU2
- **00:08:34:** Wireless: SU discovered Primary BSU:BSU1 on channel:160
- 00:23:34 kernel:Worp: SU unregistered from BSU: BSU2 (MAC: 00:0b:6b:b7:4b:ff).
- 00:23:34 kernel:Worp: WARNING: Channel 0 is set as the current channel.
- 00:23:35 kernel:Worp: SU is trying to register with BSU: BSU1 (MAC: 00:0b:6b:b7:4c:26).
- 00:23:35 kernel:Worp: SU received QoS Class: Unlimited Best Effort (indx: 1).

- 00:23:35 kernel:Worp: SU registered with BSU: BSU1 (MAC: 00:0b:6b:b7:4c:26) on channel 160(0x14004A0) (SNR: A1:43 A2:0 A3:36[dB]) at WORP port[0].
- 00:23:35 kernel:Worp: Link Profile Index: 1.
- **00:23:35: Wireless: WORP Link Established with Primary BSU: BSU1**
- 00:24:34: Wireless: SU discovered Secondary BSU:BSU2 on channel:60

Connect to Primary BSU

- 01:59:25: Wireless: **WORP Link Established with Other BSU: BSU3**
- 02:02:25 kernel:Worp: SU unregistered from BSU: BSU3 (MAC: 00:20:a6:d3:ed:e5)..
- 02:02:25: Wireless: **SU discovered Secondary BSU:BSU2 on channel:60**
- 02:02:25: Wireless: **SU discovered Primary BSU:BSU1 on channel:160**
- 02:02:25 kernel:Worp: SU is trying to register with BSU: BSU2 (MAC: 00:0b:6b:b7:4b:ff).
- 02:02:25 kernel:Worp: SU received QoS Class: Unlimited Best Effort (indx: 1).
- 02:02:25 kernel:Worp: SU registered with BSU: BSU2 (MAC: 00:0b:6b:b7:4b:ff) on channel 60(0x78043C) (SNR: A1:37 A2:0 A3:35[dB]) at WORP port[0].
- 02:02:25: Wireless: WORP Link Established with Secondary BSU: BSU2
- 02:04:25 kernel:Worp: SU unregistered from BSU: BSU2 (MAC: 00:0b:6b:b7:4b:ff).
- 02:04:25 kernel:Worp: SU is trying to register with BSU: BSU1 (MAC: 00:0b:6b:b7:4c:26).
- 02:04:25 kernel:Worp: **SU registered with BSU: BSU1** (MAC: 00:0b:6b:b7:4c:26) on channel 160(0x14004A0) (SNR: A1:46 A2:0 A3:42[dB]) at WORP port[0].
- 02:05:25: Wireless: SU discovered Secondary BSU:BSU2 on channel:60
- 02:04:25: Wireless: WORP Link Established with Primary BSU: BSU1

No Response Message

- 03:32:25 kernel:Worp: WARNING: Channel 0 is set as the current channel.
- 03:32:25 kernel:Worp: SU is trying to register with BSU: BSU1 (MAC: 00:0b:6b:b7:4c:26).
- 03:32:25 kernel:Worp: SU received QoS Class: Unlimited Best Effort (indx: 1).
- 03:32:25 kernel:Worp: SU registered with BSU: BSU1 (MAC: 00:0b:6b:b7:4c:26) on channel 160(0x14004A0) (SNR: A1:45 A2:0 A3:42[dB]) at WORP port[0].
- 03:32:25 kernel:Worp: Link Profile Index: 1.
- 03:32:25: Wireless: WORP Link Established with Primary BSU: BSU1
- 03:33:25: Wireless: **SU discovered Secondary BSU:BSU2 on channel:60**
- 03:40:43: Wireless: Secondary BSU: BSU2 not Available

Bootloader CLI and ScanTool G

Bootloader CLI

The Bootloader CLI is a minimal subset of the normal CLI that is used to perform initial configuration of the device. The Bootloader CLI is available when the device embedded software is not running.

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

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

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

The Bootloader CLI supports the following commands:

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

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

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

If the Bootloader fails to load the firmware from flash, it tries to get the firmware from the network. While trying to get firmware from the network, the device should be powered on using Ethernet 1 interface of the device. The default configuration of the Bootloader parameters are as follows:

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

To Load the Firmware from the Network

- Use the **show** command to view the parameters and their values, and use the **set** command to set the parameter value.

To Load the Firmware by using Dynamic IP Parameters

1. Set the ipaddrtype to dynamic
2. Run the BOOTP and TFTP Servers followed by device reboot

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

To Load the Firmware by using Static IP Parameters

1. Use the **set** command to set the IP parameters like 'ipaddr', 'serverip', 'filename' and also set the parameter 'ipaddrtype' to static.
2. Run the TFTP Server followed by device reboot.

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

ScanTool

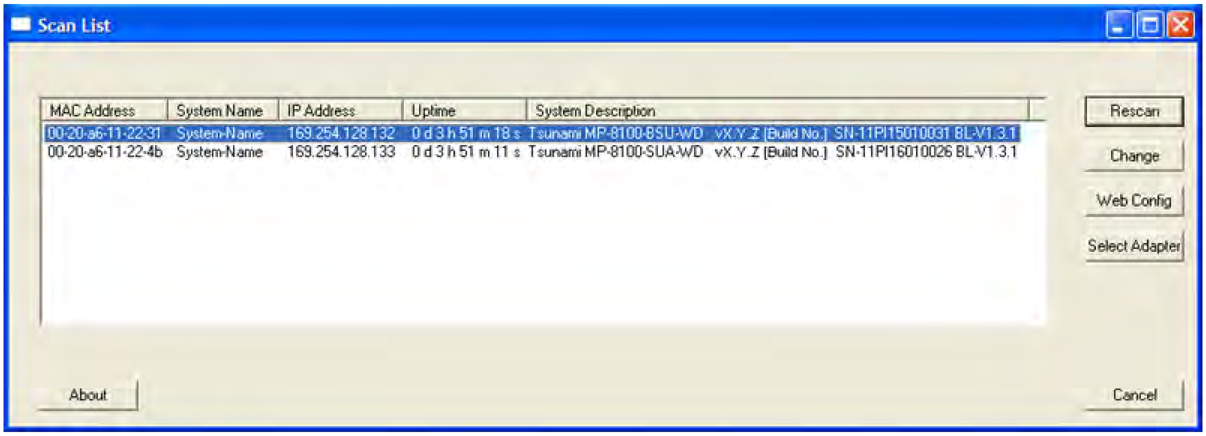
If you want to access the device with ScanTool, then the host running the ScanTool should also be in the same network as the device. The ScanTool broadcast requests are discarded by the routers if the device and the host running the ScanTool are in different network. This means that the ScanTool cannot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

: In bootloader mode, Scan Tool will support only IPv4.

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

For example:

MP-8100-BSU-WD	- Description of the device
vX.Y.Z	- Firmware Version
SN-11PI15010031	- Serial Number
BL-v1.3.1	- Bootloader version



MAC Address	System Name	IP Address	Uptime	System Description
00-20-a6-11-22-31	System-Name	169.254.128.132	0 d 3 h 51 m 18 s	Tsunami MP-8100-BSU-WD vX.Y.Z [Build No.] SN-11PI15010031 BL-V1.3.1
00-20-a6-11-22-4b	System-Name	169.254.128.133	0 d 3 h 51 m 11 s	Tsunami MP-8100-SUA-WD vX.Y.Z [Build No.] SN-11PI16010026 BL-V1.3.1

Figure G-1 Scan Tool View of a Device in Bootloader Mode (An Example)

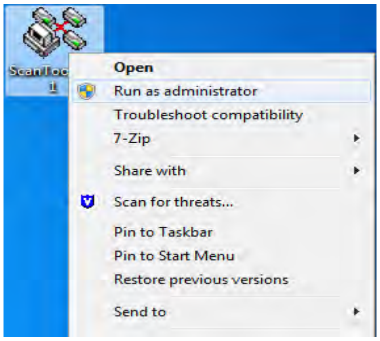
Reset/Reload Procedure

Pre-requisites

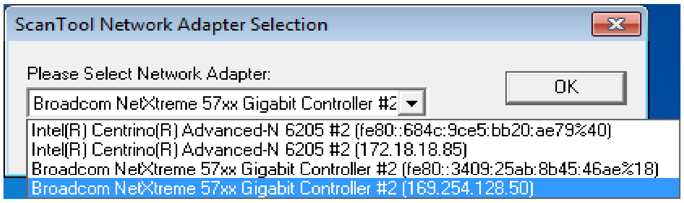
- Download ScanTool v3.1.1 or above from http://my.proxim.com
- To view the Reload/Reset button on the ScanTool window, the operating system in the PC must be Windows 07/08.
- Ensure that the Windows Firewall is turned off before the ScanTool is launched.
- Ensure that the ScanTool is **Run as Administrator**.
- Device must be connected directly to the PC over Ethernet.
- User must be able to turn on & off the power supply, during the device reload/reset procedure.

Step-by-Step instructions to perform Reload/Reset operation on a device using ScanTool application

1. Right click the **ScanTool** Application and then click **Run as Administrator**.



2. Choose a Network Adapter to which the device is connected and then click **OK**.

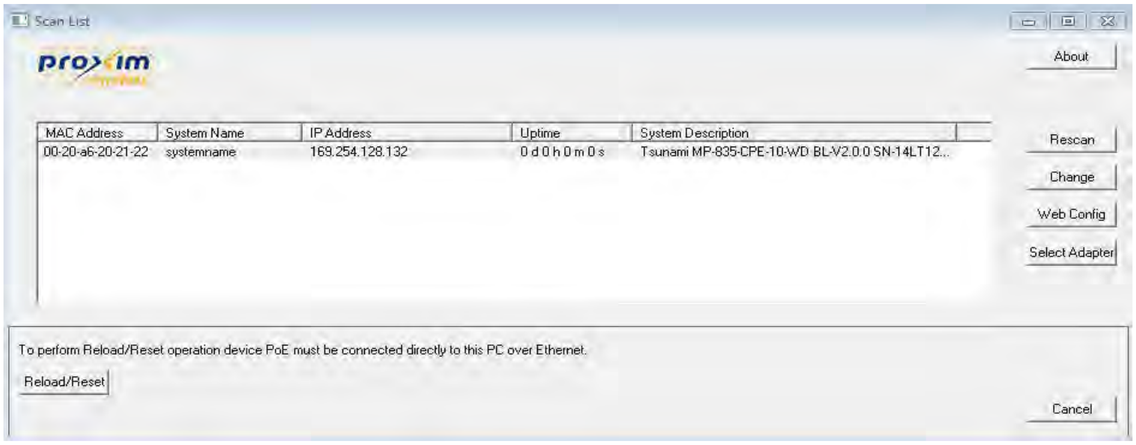

ScanTool Network Adapter Selection

Please Select Network Adapter:

Broadcom NetXtreme 57xx Gigabit Controller #2

```
Intel(R) Centrino(R) Advanced-N 6205 #2 (fe80::684c:9ce5:bb20:ae79%40)
Intel(R) Centrino(R) Advanced-N 6205 #2 (172.18.18.85)
Broadcom NetXtreme 57xx Gigabit Controller #2 (fe80::3409:25ab:8b45:46ae%18)
Broadcom NetXtreme 57xx Gigabit Controller #2 (169.254.128.50)
```

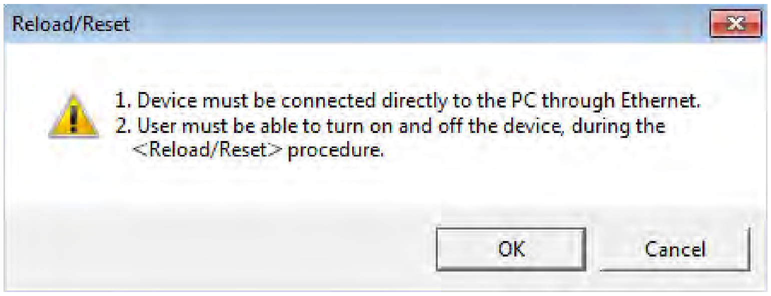
3. Click **Reload/Reset** button, at the bottom-left corner of the window.


Scan List

MAC Address	System Name	IP Address	Uptime	System Description
00-20-a6-20-21-22	systemname	169.254.128.132	0 d 0 h 0 m 0 s	Tsunami MP-835-CPE-10-WD BL-V2.0.0 SN-14LT12...

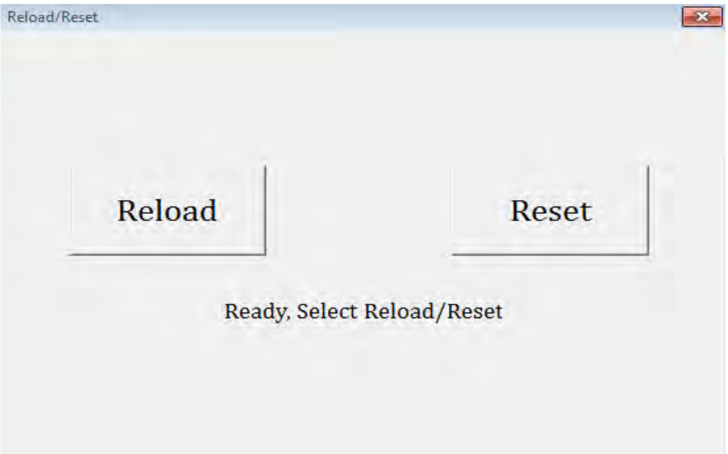
To perform Reload/Reset operation device PoE must be connected directly to this PC over Ethernet.

4. Click **OK**, on the dialog box.



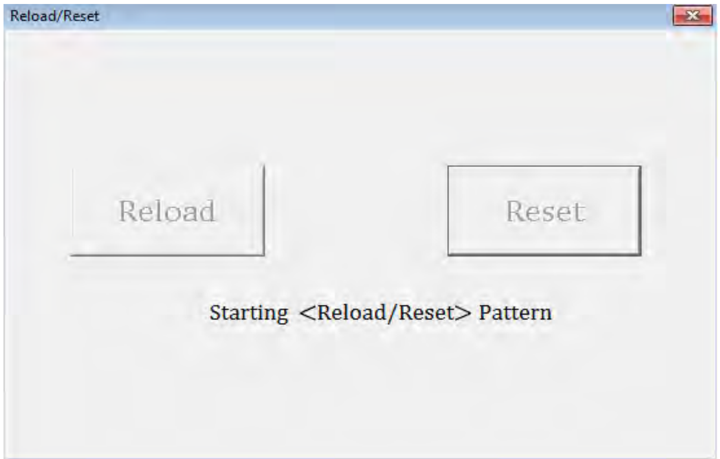
1. Device must be connected directly to the PC through Ethernet.
2. User must be able to turn on and off the device, during the <Reload/Reset> procedure.

5. Click the **Reset/Reload** button, as per the requirement.



Ready, Select Reload/Reset

6. Reload/Reset pattern is initialized.

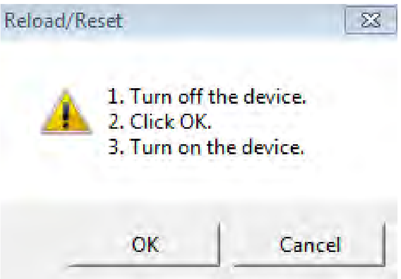


Starting <Reload/Reset> Pattern

: The message on the screenshots consists of either Reload or Reset as per the operation selected.

7. Perform the following steps:
   a. Switch off the power supply to the device by unplugging the RJ45 cable from the **PWR LAN-OUT** port on the **PoE Adapter**.
   b. Click **OK** on the dialog box.

c. Switch on the power supply to the device by re-plugging the RJ45 cable at the **PWR LAN-OUT** port on the **PoE Adapter**.

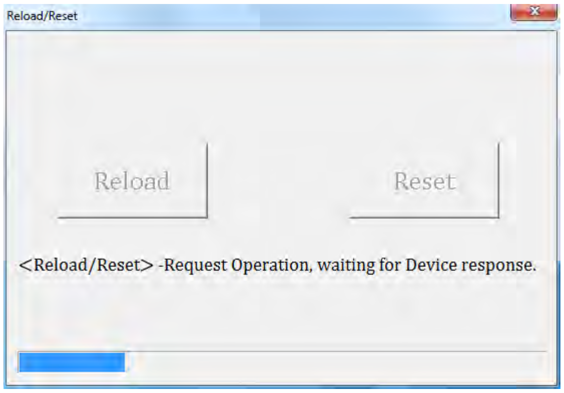


1. Turn off the device.
2. Click OK.
3. Turn on the device.

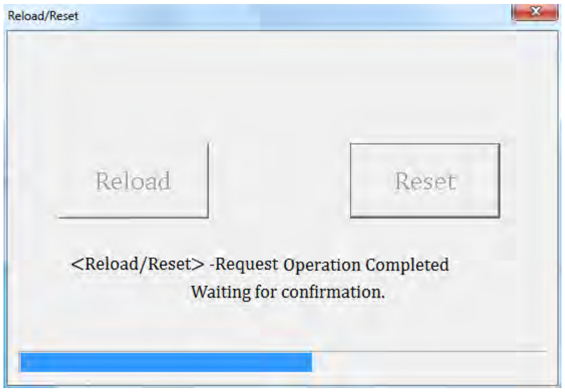
:

- *It can be noted that the steps a,b & c together constitute the "Power recycle" process.*
- *During Reload operation, ensure that the BOOTP and TFTP servers are properly configured and started.*
- *Unintentional press on the release-latch of the Ethernet cables during the Reload/Reset process unplugs the cable and results in failure of the Reload/Reset operation.*

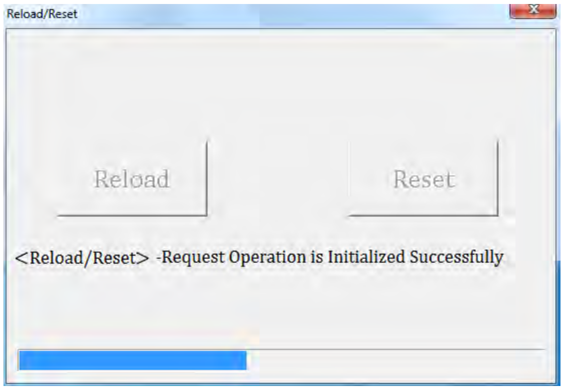
8. During the progress of the Reload/Reset-Request operation, various messages are displayed on the dialog box as given below:



<Reload/Reset> -Request Operation, waiting for Device response.

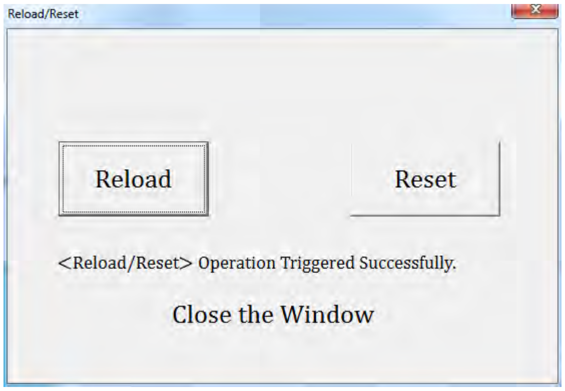


<Reload/Reset> -Request Operation Completed
Waiting for confirmation.



<Reload/Reset> -Request Operation is Initialized Successfully

9. Reload/Reset operation is started successfully.



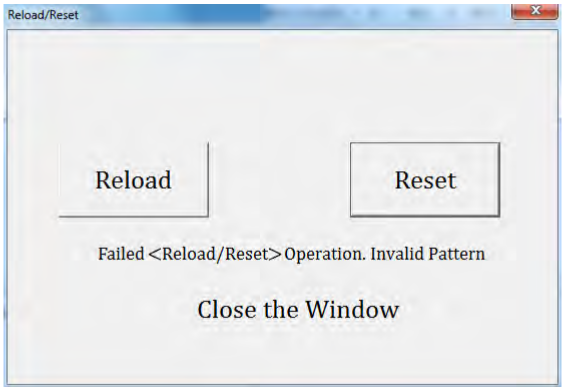
<Reload/Reset> Operation Triggered Successfully.

: *It is recommended to close the dialog box, as soon as the Reload/Reset operation is completed.*

The Reload/Reset operation has been triggered successfully. A new firmware is loaded on to the device with Reload operation, or else the device configuration is restored to the factory default settings with Reset operation.

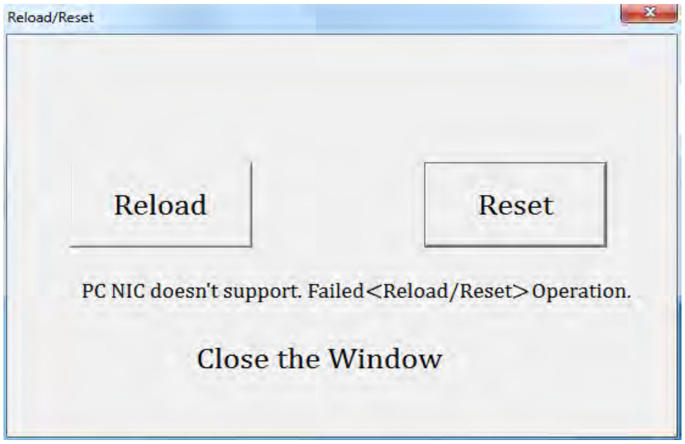
Troubleshooting the Reset/Reload Operation Failure

1. Reload/Reset operation fails
   a. If the LAN-IN cable gets unplugged during the power recycle process.



Failed <Reload/Reset> Operation. Invalid Pattern

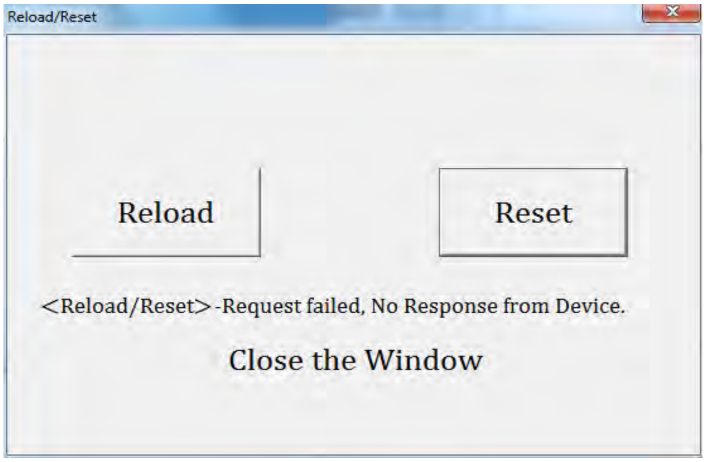
   b. If the LAN-IN cable is inserted in a NIC port, which is incompatible with the ScanTool application.



PC NIC doesn't support. Failed<Reload/Reset>Operation.

c. If the dialog box appears as given below

1. Check the connectivity issues of the Ethernet cable from the LAN port to the PC.
2. Check the Firewall status. If the Windows Firewall is turned on, perform the following steps:
   a. Under **Windows Firewall**, click **Allow a program for Windows Firewall**.
   b. Click **Change Settings** and then click **Allow another program**.
   c. View the **Add a Program** dialog box.
   d. Select the **ScanTool** program from the list and then click **Add**.
   e. Select the **Home/Work (Private)**, **Public** checkboxes and then click **OK**.



<Reload/Reset>-Request failed, No Response from Device.

Close the Window

H

SNR Information

Given below are the SNR values for the following devices:

- MP-8100-SUA
- MP-8150-SUR
- MP-8150-SUR-100

MCS Index	Modulation	No of Streams	2.4 GHz												
			5 MHz			10 MHz			20 MHz			40 MHz			
			Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate		Min SNR	Max SNR
												Full	Short		
MCS0	BPSK 1/2	Single	1.6	10	86	3.3	10	86	6.5	12	86	13.5	15	26	80
MCS1	QPSK 1/2	Single	3.3	15	86	6.5	16	86	13	21	86	27	30	26	80
MCS2	QPSK 3/4	Single	4.9	21	84	9.7	21	84	19.5	21	84	40.5	45	26	79
MCS3	16 QAM 1/2	Single	6.5	23	82	13	23	82	26	23	82	54	60	30	77
MCS4	16 QAM 3/4	Single	9.7	26	80	19.5	26	80	39	25	80	81	90	33	77
MCS5	64 QAM 2/3	Single	13	29	79	26	29	79	52	27	78	108	120	37	76
MCS6	64 QAM 3/4	Single	14.6	30	79	29.3	31	78	58.5	30	77	121.5	135	40	75
MCS7	64 QAM 5/6	Single	16.2	32	78	32.5	32	78	65	32	77	135	150	42	75
MCS8	BPSK 1/2	Dual	3.3	12	86	6.5	14	86	13	14	86	27	30	16	80
MCS9	QPSK 1/2	Dual	6.5	20	84	13	21	84	26	21	84	54	60	26	80
MCS10	QPSK 3/4	Dual	9.7	22	82	19.5	23	82	39	22	82	81	90	28	79
MCS11	16 QAM 1/2	Dual	13	23	80	26	23	80	52	24	80	108	120	32	77
MCS12	16 QAM 3/4	Dual	19.5	27	80	39	27	80	78	30	78	162	180	35	77
MCS13	64 QAM 2/3	Dual	26	30	79	52	30	79	104	34	78	216	240	37	76
MCS14	64 QAM 3/4	Dual	29.3	36	78	58.5	35	77	117	37	77	243	270	43	75
MCS15	64 QAM 5/6	Dual	32.5	39	78	65	38	77	130	39	76	270	300	45	75

MCS Index	Modulation	No of Streams	5 GHz												
			5 MHz			10 MHz			20 MHz			40 MHz			
			Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate		Min SNR	Max SNR
												Full	Short		
MCS0	BPSK 1/2	Single	1.6	6	86	3.3	7	86	6.5	6	86	13.5	15	9	80
MCS1	QPSK 1/2	Single	3.3	8	86	6.5	8	86	13	9	86	27	30	11	80
MCS2	QPSK 3/4	Single	4.9	10	84	9.7	13	84	19.5	11	84	40.5	45	15	79
MCS3	16 QAM 1/2	Single	6.5	14	82	13	16	82	26	14	82	54	60	16	77

MCS Index	Modulation	No of Streams	5 GHz												
			5 MHz			10 MHz			20 MHz			40 MHz			
			Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate		Min SNR	Max SNR
												Full	Short		
MCS4	16 QAM 3/4	Single	9.7	17	80	19.5	20	80	39	18	80	81	90	20	77
MCS5	64 QAM 2/3	Single	13	22	79	26	24	79	52	22	78	108	120	24	76
MCS6	64 QAM 3/4	Single	14.6	25	79	29.3	26	78	58.5	25	77	121.5	135	27	75
MCS7	64 QAM 5/6	Single	16.2	28	78	32.5	29	78	65	28	77	135	150	30	75
MCS8	BPSK 1/2	Dual	3.3	8	86	6.5	9	86	13	9	86	27	30	9	80
MCS9	QPSK 1/2	Dual	6.5	12	84	13	12	84	26	12	84	54	60	13	80
MCS10	QPSK 3/4	Dual	9.7	14	82	19.5	15	82	39	14	82	81	90	17	79
MCS11	16 QAM 1/2	Dual	13	16	80	26	16	80	52	16	80	108	120	22	77
MCS12	16 QAM 3/4	Dual	19.5	20	80	39	21	80	78	20	78	162	180	25	77
MCS13	64 QAM 2/3	Dual	26	25	79	52	26	79	104	26	78	216	240	27	76
MCS14	64 QAM 3/4	Dual	29.3	29	78	58.5	29	77	117	29	77	243	270	30	75
MCS15	64 QAM 5/6	Dual	32.5	30	78	65	30	77	130	30	76	270	300	33	75

Given below are the SNR values for the following device(s) in legacy mode:

- MP-8100-SUA
- MP-8150-SUR
- MP-8150-SUR-100

Modulation	2.4 GHz									5 GHz					
	5 MHz			10 MHz			20 MHz			5 MHz		10 MHz		20 MHz	
	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Min SNR	Max SNR	Min SNR	Max SNR	Min SNR	Max SNR
BPSK 1/2	1.5	10	84	3	10	84	6	13	84	8	84	8	84	7	81
BPSK 3/4	2.25	10	84	4.5	11	84	9	13	84	9	84	9	84	8	81
QPSK 1/2	3	12	84	6	11	84	12	15	84	10	82	10	82	9	81
QPSK 3/4	4.5	14	84	9	13	84	18	15	84	12	82	11	82	12	81
16QAM 1/2	6	17	82	12	17	80	24	22	80	16	82	16	82	15	80
16QAM 3/4	9	20	82	18	23	78	36	25	73	18	82	18	80	18	80
64QAM 2/3	12	27	81	24	29	76	48	28	73	24	80	24	80	24	78
64QAM 3/4	13.5	29	80	27	30	74	54	29	72	27	80	27	80	27	76

Given below are the SNR values for the following devices:

- MP-8200-BSU-G
- MP-8250-BS9-G
- MP-8250-BS1-G
- MP-8200-BSU
- MP-8250-BS9
- MP-8250-BS1
- MP-8200-SUA
- MP-8250-SUR
- QB-8200-EPA-G/LNK-G
- QB-8250-EPR-G/LNK-G
- QB-8200-EPA/LNK
- QB-8250-EPR/LNK

MCS Index	Modulation	No of Streams	4.900 - 5.925 GHz													
			5 MHz			10 MHz			20 MHz			40 MHz			
			Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate		Min SNR	Max SNR
												Full	Short		
MCS0	BPSK 1/2	Single	1.6	7	50	3.3	7	50	6.5	7	50	13.5	15	9	50
MCS1	QPSK 1/2	Single	3.3	9	50	6.5	10	50	13	11	50	27	30	10	50
MCS2	QPSK 3/4	Single	4.9	11	50	9.7	13	50	19.5	13	50	40.5	45	14	50
MCS3	16 QAM 1/2	Single	6.5	15	50	13	16	50	26	16	50	54	60	16	50
MCS4	16 QAM 3/4	Single	9.7	19	50	19.5	20	50	39	20	50	81	90	20	50
MCS5	64 QAM 2/3	Single	13	23	50	26	24	50	52	24	50	108	120	24	50
MCS6	64 QAM 3/4	Single	14.6	25	50	29.3	26	50	58.5	26	50	121.5	135	27	50
MCS7	64 QAM 5/6	Single	16.2	28	50	32.5	29	50	65	29	50	135	150	29	50
MCS8	BPSK 1/2	Dual	3.3	8	50	6.5	9	50	13	9	50	27	30	10	50
MCS9	QPSK 1/2	Dual	6.5	12	50	13	12	50	26	12	50	54	60	13	50
MCS10	QPSK 3/4	Dual	9.7	15	50	19.5	15	50	39	15	50	81	90	16	50
MCS11	16 QAM 1/2	Dual	13	18	50	26	18	50	52	18	50	108	120	20	50
MCS12	16 QAM 3/4	Dual	19.5	20	50	39	21	50	78	21	50	162	180	24	50
MCS13	64 QAM 2/3	Dual	26	25	50	52	26	50	104	26	50	216	240	27	50
MCS14	64 QAM 3/4	Dual	29.3	29	50	58.5	29	50	117	29	50	243	270	30	50
MCS15	64 QAM 5/6	Dual	32.5	30	50	65	30	50	130	30	50	270	300	33	50

Given below are the SNR values for the following device(s) in legacy mode:

- MP-8200-BSU-G
- MP-8250-BS9-G
- MP-8250-BS1-G
- MP-8200-BSU
- MP-8250-BS9
- MP-8250-BS1
- MP-8200-SUA
- MP-8250-SUR
- QB-8200-EPA-G/LNK-G
- QB-8250-EPR-G/LNK-G
- QB-8200-EPA/LNK
- QB-8250-EPR/LNK

Modulation	4.900 - 5.925 GHz								
	5 MHz			10 MHz			20 MHz		
	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR
BPSK 1/2	1.5	7	80	3	7	80	6	8	79
BPSK 3/4	2.25	8	80	4.5	9	79	9	9	77
QPSK 1/2	3	10	79	6	10	77	12	10	76
QPSK 3/4	4.5	12	78	9	12	76	18	12	74
16QAM 1/2	6	16	77	12	16	74	24	16	73
16QAM 3/4	9	20	76	18	20	72	36	21	72
64QAM 2/3	12	25	74	24	24	70	48	25	69
64QAM 3/4	13.5	27	73	27	27	68	54	27	68

Given below are the SNR values for the following devices:

- MP-820-SUA-50$^+$
- MP-820-SUA-100
- MP-822-SUA-100
- MP-825-SUR-50$^+$
- MP-825-SUR-100
- MP-825-CPE-50
- MP-825-CPE-100
- MP-835-CPE-10
- MP-835-CPE-25
- MP-835-CPE-50
- MP-835-CPE-100
- MP-820-BSU-100
- MP-822-BSU-100

- MP-825-BS3-50+
- QB-825-EPR/LNK-50+
- QB-825-EPR/LNK-100
- QB-835-EPR/LNK-25
- QB-835-EPR/LNK-50

MCS Index	Modulation	No of Streams	5 GHz											
			5 MHz			10 MHz			20 MHz			40 MHz		
			Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR
MCS0	BPSK 1/2	Single	1.6	9	50	3.3	9	50	6.5	9	50	13.5	9	50
MCS1	QPSK 1/2	Single	3.3	10	50	6.5	10	50	13	12	50	27	11	50
MCS2	QPSK 3/4	Single	4.9	13	50	9.7	13	50	19.5	13	50	40.5	15	50
MCS3	16 QAM 1/2	Single	6.5	17	50	13	17	50	26	16	50	54	16	50
MCS4	16 QAM 3/4	Single	9.7	20	50	19.5	21	50	39	22	50	81	24	50
MCS5	64 QAM 2/3	Single	13.0	24	50	26	25	50	52	25	50	108	28	50
MCS6	64 QAM 3/4	Single	14.6	26	50	29.3	27	50	58.5	27	50	121.5	29	50
MCS7	64 QAM 5/6	Single	16.2	30	50	32.5	29	50	65	30	50	135	30	50
MCS8	BPSK 1/2	Dual	3.3	10	50	6.5	10	50	13	10	50	27	10	50
MCS9	QPSK 1/2	Dual	6.5	13	50	13	12	50	26	12	50	54	13	50
MCS10	QPSK 3/4	Dual	9.7	15	50	19.5	16	50	39	15	50	81	17	50
MCS11	16 QAM 1/2	Dual	13.0	18	50	26	19	50	52	17	50	108	22	50
MCS12	16 QAM 3/4	Dual	19.5	23	50	39	23	50	78	23	50	162	25	50
MCS13	64 QAM 2/3	Dual	26.0	27	50	52	26	50	104	27	50	216	27	50
MCS14	64 QAM 3/4	Dual	29.3	29	50	58.5	29	50	117	30	50	243	30	50
MCS15	64 QAM 5/6	Dual	32.5	31	50	65	30	50	130	31	50	270	33	50

: Short GI - 400 nSec is not valid for the 82x devices.

Given below are the SNR values for the following device in legacy mode:

- MP-820-SUA-50^+
- MP-820-SUA-100
- MP-822-SUA-100
- MP-825-SUR-50^+
- MP-825-SUR-100
- MP-825-CPE-50
- MP-835-CPE-10
- MP-835-CPE-25
- MP-835-CPE-50
- MP-835-CPE-100
- MP-825-CPE-100
- QB-825-EPR/LNK-50+
- QB-825-EPR/LNK-100
- QB-835-EPR/LNK-25
- QB-835-EPR/LNK-50
- MP-820-BSU-100
- MP-822-BSU-100
- MP-825-BS3-50+

Modulation	5 GHz					
	10 MHz			20 MHz		
	Data Rate	Min SNR	Max SNR	Data Rate	Min SNR	Max SNR
BPSK 1/2	3	8	50	6	8	50
BPSK 3/4	4.5	9	50	9	9	50
QPSK 1/2	6	11	50	12	12	50
QPSK 3/4	9	12	50	18	13	50
16QAM 1/2	12	16	50	24	16	50
16QAM 3/4	18	21	50	36	21	50
64QAM 2/3	24	24	50	48	25	50
64QAM 3/4	27	28	50	54	28	50

Configuration File Cross-loading across the Products

Proxim portfolio comprises different product lines and SKUs which differ in features and capabilities depending on the hardware platform and the country setting or licensing used in them. This document describes the process to successfully apply the configuration file on a device(s) and about the software checks run while applying the configuration file on a device(s).

The user can apply a configuration file retrieved from a (Source) device to another compatible (Target) device. In order to successfully apply the configuration file, the following criteria should be met.

1. The Hardware Inventory Component ID should be same for both the source device and the target device.

Hardware Inventory Component ID	Products
2000	AP-800; AP-8000
2001	MP-8100-BSU; MP-8100-SUA; MP-8150-SUR MP-8150-SUR-100 MP-8160-BSU; MP-8160-SUA; MP-8160-BS9 MP-8200-BSU; MP-8200-SUA; MP-8250-BS9/SUR MP-8200-BSU-G; MP-8250-BS9/BS1-G MP-8200-BSU; MP-8250-BS9/BS1 MP-820-BSU-100; MP-822-BSU-100; MP-825-BS3-100 QB-8200-EPA-G; QB-8250-EPR-G QB-8200-EPA; QB-8250-EPR QB-825-EPR/LNK-50+ QB-825-EPR/LNK-100 QB-835-EPR/LNK-25 QB-835-EPR/LNK-50 QB-8xxx-EPA; QB-8xxx-EPR
2003	MP-8150-CPE
2005	Tsunami 82x Series
2006	AP-8100

NOTE:*The configuration file can be applied only to the devices of the same family.*

- *The configuration file retrieved from an 8xx series device cannot be applied to a device from 81xx series.*
- *The configuration file of a MP-8160-BSU/MP-8160-SUA device cannot be applied to an 8100/8200 series device and vice versa even though they share the same component ID.*
- *The configuration file of a MP-8150-CPE device cannot be applied to a MP-8160-CPE device and vice versa even though they share the same component ID.*
- *The configuration file of a MP-82xx-BSx can be applied on a MP-82xx-BSx-G device where as the configuration file of MP-82xx-BSx-G cannot be applied on MP-82xx-BSx.*

2. The Regulatory Domain should be same in both the source device and the target device.The available **Regulatory Domains** are listed below:
   - WD

- US
- JP
- EU*

NOTE: *WD SKU is compatible only with the EU SKU. For example, if the configuration file retrieved from a WD SKU device is loaded on a US or JP SKU target device then the upgrade fails.*

If the above criteria are met, the configuration file can be successfully applied on the target device else an error message is thrown. Once the configuration file is loaded and the device is rebooted, the software tries to apply the new configuration file during the system boot-up process.

Sometimes, a device from a particular product series may have a different license information compared to other devices of the same series. Therefore, the start-up process validates the configuration file against the license file of the device before applying the configuration file. The configuration file is valid, if the following conditions are met:

1. The input bandwidth limit in the configuration file should be less than or equal to the input bandwidth limit in the license file.
2. The output bandwidth limit in the configuration file should be less than or equal to the output bandwidth limit in the license file.
3. The sum of the input and output bandwidth limit in the configuration file should be less than or equal to the cumulative bandwidth limit in the license file.
4. The frequency band (2.4, 4.9, and 5 G Hz) in the configuration file should match with any one of the supported frequency bands in the license file.
5. The radio operation mode (BSU/SU/AP) in the configuration file should match with any one of supported radio operating modes in the license file.
6. The number of satellites in the configuration file should be less than or equal to the number of satellites in the license file.
7. The product family (TMP/TQB/AP) value in the configuration file should match the product family value in the license file.
8. Tx/Rx antenna chain mask in the configuration file should match the Tx/Rx antenna chain mask in the license file.

NOTE: *If any one of the above conditions is not met, the configuration file will be removed by the flash control module during initialization and the device will boot-up with the last known good configuration. Before deleting the configuration file, an eventlog is generated about the violation of the license parameters. In some cases, if the last known good configuration does not exist internally, the device can reset the configuration to factory defaults and boot up.*

Abbreviations

J

A	
ACL	Access Control List
ACS	Automatic Channel Selection
AES	Advanced Encryption Standard
ALG	Application Level Gateway
ARP	Address Resolution Protocol
ATPC	Adaptive Transmit Power Control
B	
BSU	Base Station Unit
C	
CCP	Compression Control Protocol
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface
CIR	Committed Information Rate
CPE	Customer Premises Equipment
CRC	Cyclic Redundancy Check
D	
DDRS	Dynamic Data Rate Selection
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSL	Digital Subscriber Line
E	
EIRP	Equivalent Isotropically Radiated Power
EOL	End of Life
ETSI	European Telecommunications Standards Institute
F	
FCC	Federal Communications Commission

FCS	Frame Check Sequence
G	
Gbps	Gigabit Per Second
GPL	General Public License
GRE	Generic Routing Encapsulation
H	
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
I	
IANA	Internet Assigned Numbers Authority (IANA)
IC	Industry Canada
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
ISP	Internet Service Provider
ITS	Intelligent Transportation System
L	
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LCP	Link Configuration Protocol
LED	Light Emitting Diode
LGPL	Lesser General Public License
M	
MAN	Metropolitan Area Networks
Mbps	Megabits Per Second
MD5	Message-Digest algorithm
MIB	Management Information Base
MIMO	Multiple-input and multiple-output
MIR	Maximum Information Rate
MP	Multipoint
MPPE	Microsoft Point-to-Point Encryption
MSCHAP v2	Microsoft Challenge-Handshake Authentication Protocol
MTU	Maximum Transmission Unit

N	
NAPT	Network Address Port Translation
NAT	Network Address Translation
NCP	Network Control Protocol
NBD	Next Business Day
NMS	Network Management System
NOP	Non Occupancy Period
P	
PAP	Password Authentication Protocol
PC	Personal Computer
PoE	Power Over Ethernet
PPPoE	Point-to-point Protocol over Ethernet
PTMP	Point-to-multipoint
PTP	Point-to-point
PVES	ProximVision ES
Q	
QB	QuickBridge
QoS	Quality of Service
R	
RADIUS	Remote Authentication Dial In User Service
RAS	Remote Access Services
RF	Radio Frequency
RIP	Routing Information Protocol
RMA	Return Material Authorization
RLT	Radio Link Test
RSSI	Received Signal Strength Indicator
S	
SHA	Secure Hash Algorithm
SKU	Stock Keeping Unit
SNMP	Simple Network Management Protocol
SNR	Signal-to-noise Ratio
SNTP	Simple Network Time Protocol
SSH	Secure Shell

SSL	Secure Socket Layer
STP	Spanning Tree Protocol
SU	Subscriber Unit
T	
TBC	Text Based Configuration
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TPC	Transmit Power Control
TPID	Tag Protocol Identifier
TTL	Time to Live
U	
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair
V	
VLAN	Virtual Local Area Network
W	
WEP	Wired Equivalent Privacy
WORP	Wireless Outdoor Router Protocol

Lightning Protection

K

Lightning protection is used to maximize the reliability of the communications equipment by safely re-directing current from a lightning strike or a power surge traveling along the Cat 5/Cat5e/Cat 6 Ethernet cabling to the ground using the shortest path possible. Designing a proper grounding system prior to installing any communications equipment is critical to minimize the possibility of equipment damage, void warranties, and cause serious injury.

The surge arrestor (sometimes referred to as a lightning protector) can protect your sensitive electronic equipment from high-voltage surges caused by discharges and transients at the PoE.

Proxim Wireless offers superior lightning and surge protection for Tsunami® series products. Contact your reseller or distributor for more information.

Warranty and Technical Support

L

For Warranty and Technical Support Policy, please visit http://proxim.com/support.

Obtaining Technical Service and Support

If you are having trouble using the Proxim product, please read this guide and the additional documentation provided with your product. If you require additional support to resolve your issue, please be ready to provide the following information before you contact Proxim's Technical Services team:

- Product information
  - Part number and serial number of the suspected faulty device
- Trouble/error information
  - Trouble/symptom being experienced
  - Activities completed to confirm fault
  - Network information (What kind of network are you using?)
  - Circumstances that preceded or led up to the error
  - Message or alarms viewed
  - Steps taken to reproduce the problem
- ServPak information (if a Servpak customer):
  - ServPak account number
- Registration information
  - If the product is not registered, date and location where you purchased the product

: Technical Support is free for the warranty period from the date of purchase.

Support Options

Proxim eService Web Site Support

The Proxim eService Web site is available 7x24x365 at http://my.proxim.com.

On the Proxim eService Web Site, you can access the following services:

- **Product Download Page**: Provides quick links to product firmware, software, and documentation downloads.
- **Proxim TV Links**: A link to helpful video tutorials.
- **Knowledgebase**: A solution database of all the resolved problems. You can search by product, category, keywords, or phrases.
- **Live Chat**: Chat with a support technician on-line or request to call back at a later time.
- **Create a Support Request**: Create a support request with our technical support staff who will reply to you by email.
- **Case Management**: Login to check the status of your support cases, update your personal profile, or access restricted information and features.
- **Provide Feedback**: Submit a suggestion, complaint, or other feedback about the support site and our products.

Telephone Support

Contact technical support via telephone as follows:

- **USA and Canada Customers**
  - — **Phone**: +1-408-383-7700; +1-866-674-6626
  - — **Business Hours**: 24x7 live response. Tier 3 support: 8 a.m. to 5 p.m. M-F PDT (UTC/GMT -7 hrs)
- **International Customers**
  - — **Phone**: +1-408-383-7700; 0800-916475 (France); 8-800-100-9485 (Russia)
  - — **Business Hours**: 24x7 live response. Tier 3 support: 8 a.m. to 5 p.m. M-F PDT (UTC/GMT -7 hrs)

ServPak Support

To provide even greater investment protection, Proxim Wireless offers a cost-effective support program called ServPak. ServPak is a program of enhanced service support options that can be purchased as a bundle or individually, tailored to meet your specific needs. Whether your requirement is round the clock technical support or advance replacement service, we are confident that the level of support provided in every service in our portfolio will exceed your expectations.

All ServPak service bundles are sold as service contracts that provide coverage for specific products from 1 to 3 years. Servpak bundles are considered an upgrade to the standard product warranty and not an extension.

All Plans Include	ServPak Plus	ServPak Prime
24x7 Basic Technical Support	**Basic Advanced Replacement (Two business days/ International economy shipment service)**	**Priority Advanced Replacement (Next business day/ International priority shipment service)**
8x7 Advanced Technical Support		**24x7 Advanced Technical Support**
Software Maintenance		**Proxim Vision Support**
Access to Knowledge Base		

Additional Information on ServPak Options

Advanced Replacement of Hardware

In the event of a hardware failure, our guaranteed turnaround time for return to factory repair is 30 days or less. Customers who purchase this service are guaranteed replacement of refurbished or new hardware to be shipped out within one or two business days, as applicable. Options are available for shipment services depending on the customer’s support needs. Hardware is shipped on business days, Monday – Friday excluding Holidays, 8:00 AM – 3:30 PM Eastern Time.

7x24x365 Availability

Unlimited, direct access to technical support engineers 24 hours a day, 7 days a week, 365 days a year including Holidays.

8x5 Availability

Unlimited, direct access to world-class technical support engineers 8 hours a day, 5 days a week, Monday through Friday from 8:00AM - 5:00PM Pacific Standard Time.

Basic Technical Support

Customers who purchase this service can be rest assured that their call will be answered by Proxim's Tier 1 technical support and a case opened immediately to document the problem and provide initial troubleshooting to identify the solution and resolve the incident in a timely manner.

Advanced Technical Support

In addition to Proxim's world-class Tier 1 technical support, customers will be able to have their more complex issues escalated to our world-class Tier 3 technical support engineers. Our Tier 3 engineers will review specific configurations to troubleshoot intricate issues and will also provide helpful insights regarding Proxim's products and various tips from decades of collective experience in the wireless industry.

Software Maintenance

It's important to maintain and enhance security and performance of wireless equipment and Proxim makes this easy by providing a Software Maintenance program that enables customers to access new feature and functionality rich software upgrades and updates. Customers will also have full access to Proxim's vast Knowledgebase of technical bulletins, white papers and troubleshooting documents.

To purchase ServPak support services, please contact your authorized Proxim distributor. To receive more information or for questions on any of the available ServPak support options, please visit our website at http://www.proxim.com/support/servpak, call Proxim Support (For telephone numbers, see Telephone Support) or send an email to servpak@proxim.com.