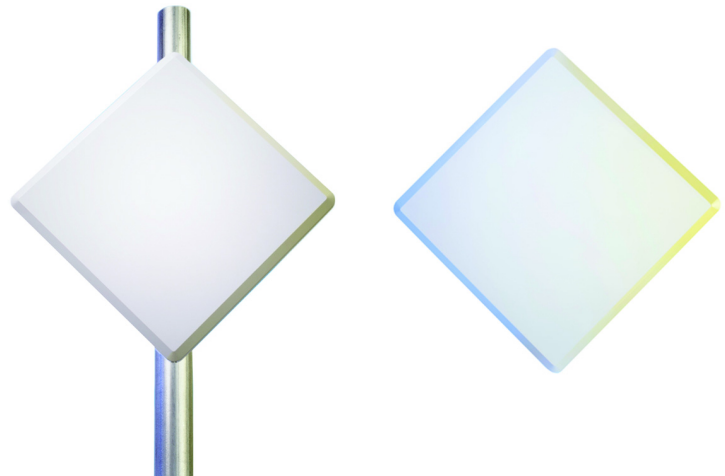




Tsunami MP.11
Model 4954-R
Installation and Management



IMPORTANT!

Before installing and using this product, see the
Safety and Regulatory Compliance Guide located on the product CD.

Copyright

©2006 Proxim Wireless Corporation, San Jose, CA. All rights reserved. Covered by one or more of the following U.S. patents: 5,231,634; 5,875,179; 6,006,090; 5,809,060; 6,075,812; 5,077,753. This manual and the software described herein are copyrighted with all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of Proxim Wireless Corporation.

Trademarks

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

Contents

1	Introduction	9
	About This Book	9
	Reference Manual	10
	Wireless Network Topologies	11
	Point-to-Point Link	11
	Point-to-Multipoint Network	11
	Management and Monitoring Capabilities	12
	Web Interface	12
	Command Line Interface	12
	SNMP Management	12
2	Installation and Initialization	14
	Hardware Overview	15
	Power-over-Ethernet	15
	Serial Connection	15
	External Antenna Connection	16
	Product Package	17
	Hardware Installation	19
	Step 1: Choose a Location	20
	Step 2: Unpack Shipping Box	21
	Step 3: Assemble the Cable	22
	Step 4: Determine Proper Mounting Orientation	23
	Step 5: Assemble Mounting Hardware	24
	Step 6: Mount the Unit	25
	Step 7: Plug in the Cables	26
	Step 8: Power on the Unit	27
	Step 9: View LEDs	27
	Step 10: Align the Antenna	28
	Antenna Alignment Commands	29
	Step 11: Tighten the Cables	30
	Step 12: Weatherproof the Connectors	31
	Step 13: Install Documentation and Software	32
	Initialization	33
	ScanTool	33
	Setting the IP Address with ScanTool	33
	Logging in to the Web Interface	35
3	System Overview	36
	Changing Basic Configuration Information	36
	Country and Related Settings	36

Transmit Power Control	37
SU Registration	38
Dynamic Data Rate Selection (DDRS)	39
Virtual Local Area Networks (VLANs)	40
Quality of Service (QoS)	41
Concepts and Definitions	41
Packet Identification Rule (PIR)	41
Service Flow Class (SFC)	42
QoS Class	44
4 Basic Management	45
Navigation	45
Rebooting and Resetting	46
Rebooting	46
Resetting Hardware	46
Soft Reset to Factory Default	46
General Configuration Settings	48
Monitoring Settings	49
Security Settings	50
Encryption	50
Passwords	50
Default Settings	51
Upgrading the Unit	53
5 System Status	54
Status	55
System Status	55
Systems Traps	55
Event Log	56
6 Configuration	57
System Parameters	57
Bridge and Routing Modes	58
Bridge Mode	58
Network Parameters	62
Change IP Parameters	62
Configure Spanning Tree Options	62
Enable or Disable Roaming	65
Roaming Overview	65
Roaming with Dynamic Data Rate Selection (DDRS) Enabled	65
Configuring Roaming	66

Enable and Configure the DHCP Server	68
Add Entries to the DHCP Server IP Pool Table	69
Edit/Delete Entries to the DHCP Server IP Pool Table Entries	69
Enable the DHCP Relay Agent (Routing Mode Only)	70
Add Entries to the DHCP Relay Agent Table	70
Edit/Delete Entries to the DHCP Relay Agent Table	71
Interface Parameters	72
Configure the Wireless Interface	72
Base Mode	72
Satellite Mode	76
Configure the Ethernet Interface	77
SNMP Parameters	78
Add Entries to the Trap Host Table	78
Edit/Delete Entries to the Trap Host Table	78
RIP Parameters	80
RIP Example	81
RIP Notes	81
Management Parameters	82
Configure Passwords	82
Configure Service Parameters	82
SNMP Configuration Settings	83
HTTP Configuration Settings	83
Telnet Configuration Settings	83
Serial Configuration Settings	84
Security Parameters	85
Configure MAC Authentication	85
Configure Encryption Parameters	86
Configure RADIUS Authentication	86
Filtering Parameters	88
Overview	88
Increasing Available Bandwidth	88
Increasing Network Security	88
Sample Use and Validation	88
Setting the ARP Filter	88
Configure Ethernet Protocol Filtering	89
Configure Static MAC Pair Filtering	90
Add Entries to the Static MAC Filter Table	91
Static MAC Filter Examples	92
Configure Storm Threshold Filtering	93
Configure Broadcast Protocol Filtering	93
Configure IP Access Table Filtering	94
Intra-Cell Blocking (Base Station Unit Only)	96

Overview	96
Intra-Cell Blocking Group Rules	96
Example of Intra-Cell Blocking Groups	96
Achieving Communication Between Two SUs	96
Enable Intra-Cell Blocking	97
Configure Intra-Cell Blocking Groups	97
Assign MAC Addresses (MAC Table)	98
Adding Entries	98
Block Traffic Between SUs (Security Gateway)	99
VLAN Parameters	100
Overview	100
VLAN Modes	100
VLAN Forwarding	100
VLAN Relaying	100
Management VLAN	100
BSU and SU in Transparent Mode	101
BSU in Trunk Mode and SU in Trunk/Access Mode	101
BSU VLAN Configuration	102
Add BSU VLAN Table Entries	103
Edit or Delete BSU VLAN Table Entries	103
Restricting Unit Management	104
Providing Access to Hosts in the Same VLAN	104
SU VLAN Configuration	104
Add SU Table Entries	104
Edit SU Table Entries	105
Typical User VLAN Configurations	106
QoS (Quality of Service) Parameters	107
QoS PIR Configuration	107
QoS SFC Configuration	108
QoS Class Configuration	110
QoS SU Configuration	114
SU Access to the Public Network (NAT)	116
Adding Entries	116
Editing Entries	117
Supported Session Protocols	117
7 Monitoring	119
Wireless	120
General Performance	120
WORP Interface Performance	120
ICMP	121
Per Station	122

Features	123
Link Test	124
Interfaces	125
IP ARP Table	126
IP Routes	127
Learn Table	128
RIP	129
RADIUS	130
QoS	131
Temperature	132
8 Commands	133
Download Files	133
Upload Files	134
Reboot the Unit	135
Reset the Unit to Factory Default	136
Set the Help Link Location	137
Downgrade to Previous Release	138
9 Procedures	139
TFTP Server Setup	140
Web Interface Image File Download	141
Configuration Backup	142
Configuration Restore	143
Soft Reset to Factory Default	144
Hard Reset to Factory Default	145
Forced Reload	146
Image File Download with the Bootloader	147
Download with ScanTool	147
Download with CLI	147
10 Troubleshooting	149
Connectivity Issues	149
Unit Does Not Boot	149
Serial Link Does Not Work	149
HyperTerminal Connection Problems	150
Ethernet Link Does Not Work	150
Cannot Use the Web Interface	150
Communication Issues	151

Two Units Are Unable to Communicate Wirelessly	151
Setup and Configuration Issues	152
Lost Password	152
The Unit Responds Slowly	152
Web Interface Does Not Work	152
Command Line Interface Does Not Work	152
TFTP Server Does Not Work	152
Online Help Is Not Available	153
Changes Do Not Take Effect	153
VLAN Operation Issues	154
Link Problems	155
General Check	155
Statistics Check	155
Analyzing the Spectrum	156
Avoiding Interference	156
Conclusion	156
A Frequency Bands and Channels	157
B Technical Specifications	158
Part Numbers	159
Base Station Unit	159
Subscriber Unit	159
Accessories	159
Outdoor Ethernet Cables	159
Power Injector	159
Regulatory Approvals and Frequency Ranges	160
Model 2454-R Regulatory Approval and Frequency Ranges	160
Model 4954-R Regulatory Approval and Frequency Ranges	160
Integrated Antenna Specifications	160
Subscriber Unit with Integrated 21-dBi Antenna	160
RF Modulation and Over-the-Air Rates	160
OFDM (Orthogonal Frequency Division Multiplexing)	160
Wireless Protocol	160
Device Interface	160
Network Architecture Type	161
Receive Sensitivity	161
Maximum Throughput	161
Latency	161
Transmit Power Settings	161
Range Information	162

Integrated Antenna	162
External Antenna	162
Notes	162
System Processor and Memory	162
Software Specification	163
Base Station and Subscriber Units	163
Base Station Unit	164
Subscriber Units	164
Security	164
Management	164
Antenna	164
Status LEDs	165
Local Configuration Support	165
Compliance and Standards	165
Safety	165
Radio Approvals	165
EMI and Susceptibility (Class B)	165
Water and Dust Proof	165
Electrical	165
PoE Power Injector	165
Outdoor Radio Unit	165
Dimensions	166
Base Station and Subscriber Unit	166
Base Station and Subscriber Unit with Type-N Connector	166
Subscriber Unit with Integrated 21-dBi Antenna Unpackaged: 12.60 in x 12.60 in x 3.50 in (320 mm x 320 mm x 18 mm) Weight 166	
Base Station and Subscriber Unit with Type-N Connector	166
Subscriber Unit with Integrated 21-dBi or 16-dBi Antenna Packaged weight: 10.1 lbs (4.6 kg)	166
Environmental	166
Operating	166
Storage	166
Packaging Contents	166
MTBF	166
Warranty	167
C Lightning Protection	168
D Technical Services and Support	169
Obtaining Technical Services and Support	169
Support Options	170
Proxim eService Web Site Support	170

Telephone Support	170
Hours of Operation	170
ServPak Support	170
E Statement of Warranty	171
Warranty Coverage	171
Repair or Replacement	171
Limitations of Warranty	171
Support Procedures	171
Other Information	172
Search Knowledgebase	172
Ask a Question or Open an Issue	172
Other Adapter Cards	172

Introduction

The Tsunami MP.11 Model 4954-R Base Station Unit and Subscriber Unit are flexible wireless outdoor routers that let you design solutions for point-to-point links and point-to-multipoint networks.

The 4954-R is part of the Tsunami MP.11 product family, which is comprised of several additional products, including the 5054-R and 2454-R Base Station Units (BSUs) and the 5012-R SUR Subscriber Unit for outdoor installation; and the 5054 Base Station (BSU), the 5054 Subscriber Unit (SU), and the 5012-SUI Subscriber Unit for indoor installation.

Some of the key features of the units are:

- The use of a highly optimized protocol for outdoor applications
- Routing and bridging capability
- Asymmetric bandwidth management
- Management through a Web Interface, a Command Line Interface (CLI), or Simple Network Management Protocol (SNMP)
- Software and configuration upgrade through file transfer (TFTP)
- Outdoor placement, close to the antenna, for significantly improved range and ease of installation
- Optional integrated antenna
- VLAN support

About This Book

Before installing and using the unit, Proxim recommends you review the following chapters of this manual:

- **Chapter 1 “Introduction” (this chapter):** Provides an overview of the content of this manual as well as wireless network topologies and combinations that can be built with the unit.
- **Chapter 2 “Installation and Initialization”:** Provides detailed installation instructions and explains how to access the unit for configuration and maintenance.
- **Chapter 3 “System Overview”:** Provides a high-level overview of configuration processes and features.
- **Chapter 4 “Basic Management”:** Explains the most common settings used to manage the unit.
- **Chapter 5 “System Status”:** Depicts the Web Interface’s “Status” options, including System Status and Event Logs.
- **Chapter 6 “Configuration”:** Depicts the Web Interface’s “Configure” options in a hierarchical manner, so you can easily find details about each item.
- **Chapter 7 “Monitoring”:** Depicts the Web Interface’s “Monitor” options in a hierarchical manner, so you can easily find details about each item.
- **Chapter 8 “Commands”:** Depicts the Web Interface’s “Commands” options in a hierarchical manner, so you can easily find details about each item.
- **Chapter 9 “Procedures”:** Provides a set of procedures, including TFTP Server Setup, Configuration Backup, Restore, and Download, Forced Reload, and Reset to Factory Defaults.
- **Chapter 10 “Troubleshooting”:** Helps you to isolate and solve problems with your radio unit.

The appendixes contain supplementary information you may not need immediately, including Country Code Tables and Technical Support information.

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

Reference Manual

As a companion to the *Installation and Management* manual, the *Tsunami MP.11 Reference Manual* provides the following supplemental information:

- **Command Line Interface:** Documents the text-based configuration utility's keyboard commands and parameters.
- **Event Log Error Messages:** Documents the error messages that you may see in your Event Log.
- **Alarm Traps:** Documents the alarm traps that can be set.
- **Microsoft Windows IAS Radius Server Configuration:** Provides information to assist you in setting up the IAS Radius Server.
- **Addition of Units to a Routed Network:** Describes how to add more units to your routed network.
- **Glossary:** Describes terms used in the Tsunami MP.11 documentation and in the wireless industry.

Wireless Network Topologies

The unit can be used in various network topologies and combinations. The required equipment depends upon the wireless network topology you want to build. Make sure all required equipment is available before installing the unit.

The 4954-R is designed for outdoor placement. One model of the SU is equipped with an integrated antenna. For all other models, you can connect the unit to an outdoor antenna. See the *Tsunami MP.11 Antenna Installation Guide* for details.

WARNING: To connect the unit to an outdoor antenna, consult the appropriate manufacturers' documentation for additional regulatory information, safety instructions, and installation requirements.

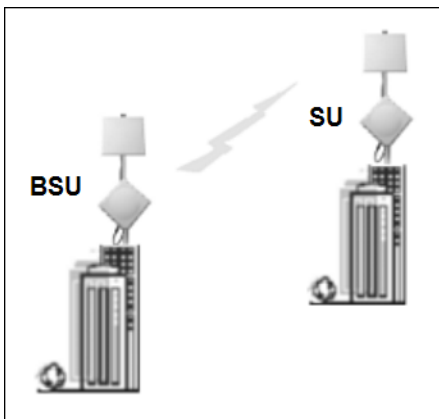
You can set up the following types of topologies:

- Point-to-Point Link
- Point-to-Multipoint Network

Each unit is set up as either a Base Station Unit (BSU) or a Subscriber Unit (SU). A link between two locations always consists of a BSU and an SU. A BSU can, depending upon its configuration, connect to one or more SUs. An SU, however, can connect only to one BSU.

Point-to-Point Link

With a BSU and an SU, it is easy to set up a wireless point-to-point link as depicted in the following figure.

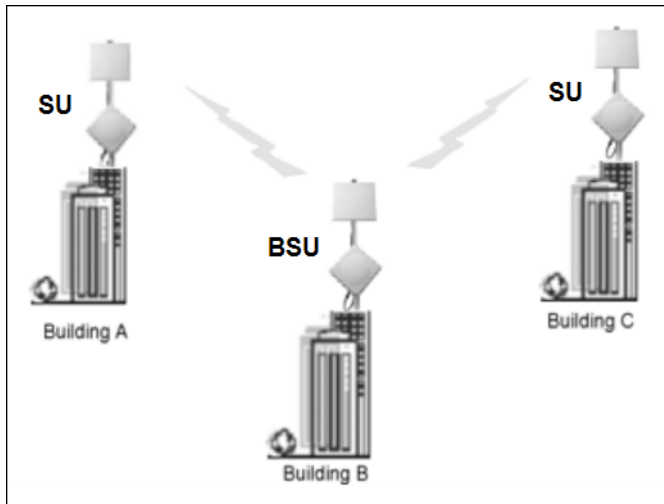


A point-to-point link lets you set up a connection between two locations as an alternative to:

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

Point-to-Multipoint Network

If you want to connect more than two buildings, you can set up a single point-to-multipoint network with a single BSU and multiple SUs, as depicted in the following figure.



Up to 250 SUs can be connected to a BSU. If a BSU already has 250 SU, a new SU cannot be connected to the BSU. In this figure, the system is designed as follows:

- The central building **B** is equipped with a BSU, connected to either an omni-directional, or a wide angle antenna.
- The two other buildings **A** and **C** are both equipped with an SU connected to a directional antenna.

Management and Monitoring Capabilities

There are several management and monitoring interfaces available to the network administrator to configure and manage the unit:

- [Web Interface](#)
- [Command Line Interface](#)
- [SNMP Management](#)

Web Interface

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

Command Line Interface

The Command Line Interface (CLI) is a text-based configuration utility that supports a set of keyboard commands and parameters to configure and manage the unit. You enter command statements, composed of CLI commands and their associated parameters. You can issue commands from the keyboard for real-time control or from scripts that automate configuration. See the *Tsunami MP.11 Reference Manual* for more information about the Command Line Interface.

SNMP Management

In addition to the Web interface and the CLI, you also can manage and configure your unit using the Simple Network Management Protocol (SNMP). Note that this requires an SNMP manager program (sometimes called MIB browser) or a Network Manager program using SNMP, such as HP OpenView or Castelrock's SNMPc. The units support several Management Information Base (MIB) files that describe the parameters that can be viewed and configured using SNMP:

- mib802.mib
- orinoco.mib

- rfc1213.mib
- rfc1493.mib
- rfc1643.mib

Proxim provides these MIB files on the CD included with your unit. You must compile one or more of these MIB files into your SNMP program's database before you can manage your unit using SNMP. See the documentation that came with your SNMP manager for instructions about how to compile MIBs.

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

The enterprise MIB (orinoco.mib) defines the read and read/write objects you can view or configure using SNMP. These objects correspond to most of the settings and statistics that are available with the other management interfaces. See the enterprise MIB for more information; the MIB can be opened with any text editor, such as Microsoft Word, Notepad, and WordPad. See [SNMP Parameters](#).

IMPORTANT!

Using a serial connection, you can access the unit through a terminal emulation program such as HyperTerminal. (See "HyperTerminal Connection Properties" in the *Tsunami MP.11 Reference Manual*.)

For all other modes of connection, you will need the IP address of the unit in order to use the Web Interface, SNMP, or the CLI. See [Setting the IP Address with ScanTool](#) for more information.

Installation and Initialization

This chapter describes the steps required to install and mount the unit, and to align the antenna. An antenna cable is required only when you use the external antenna option. Note that the unit must have either the integrated antenna or must be connected to an external antenna for its operation. The installation procedure does not include the mounting and connection of antennas. See the *Tsunami MP.11 Antenna Installation Guide* for this information.

If you are already familiar with this type of product, you can use the *Quick Install Guide* for streamlined installation procedures.

See the following sections:

- [Hardware Overview](#)
- [Product Package](#)
- [Hardware Installation](#)
 - [Step 1: Choose a Location](#)
 - [Step 2: Unpack Shipping Box](#)
 - [Step 3: Assemble the Cable](#)
 - [Step 4: Determine Proper Mounting Orientation](#)
 - [Step 5: Assemble Mounting Hardware](#)
 - [Step 6: Mount the Unit](#)
 - [Step 7: Plug in the Cables](#)
 - [Step 8: Power on the Unit](#)
 - [Step 9: View LEDs](#)
 - [Step 10: Align the Antenna](#)
 - [Step 11: Tighten the Cables](#)
 - [Step 12: Weatherproof the Connectors](#)
 - [Step 13: Install Documentation and Software](#)
- [Initialization](#)
 - [ScanTool](#)
 - [Setting the IP Address with ScanTool](#)
- [Logging in to the Web Interface](#)

Hardware Overview

The 4954-R unit contains a state-of-the-art wireless radio, an optional high-gain performance flat-panel antenna, and Power-over-Ethernet (the sole means of power for the unit). For further protection, the unit has internal, built-in surge protection.

Power-over-Ethernet

The unit is equipped with a Power-over-Ethernet (PoE) module. Using PoE, you can provide electricity and wired connectivity to the unit over a single Category 5 cable. Although the power injector that is supplied with the unit is 802.3af-compatible, standard 802.3af-compliant power modules will not properly power the units. Always use the supplied power injector.

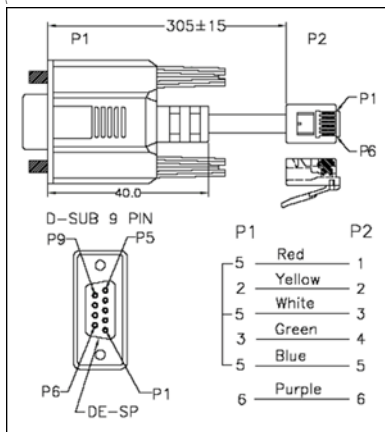
- The PoE integrated module provides –48 VDC over a standard Cat5 Ethernet cable.
- Maximum power supplied to the unit is 20 Watts (when the unit is heating or cooling); the units typically draw less than 7.5 Watts.
- The unit only accepts power on the “extra pairs”, not on the data pairs according the configuration for “midshipman” power injection, see the IEEE 802.3af standard.

Between 0 and 55° Celsius internal temperature, the unit does not need to regulate its temperature, so the power draw is generally lower in this temperature range. When the internal temperature gets close to the limits, the unit starts to heat/cool itself and the power draw increases. Powering while cold triggers a special self-heat mode where the unit is inoperable until the temperature is above 0° deg Celsius. This is signaled by a solid red LED on the Ethernet connector. Once the internal temperature is above 0 degrees Celsius, the unit boots normally.

Recommended Cable	
Function	Power (DC) and Ethernet connection
Type	Cat5, UV-shielded and outdoor-rated
Impedance	100 ohms
Recommended cables	4 UTP, 24 AWG, UL rated
Maximum Distance	330 feet / 100 meters
Connector type, unit end	RJ45 female, weatherized using weatherproof connector
Connector type, power & Ethernet adapter end	RJ45

Serial Connection

The serial connection is made with an RJ11 to DB9 connector (also referred to as a “dongle”). Connect the RJ11 end to the unit and connect the serial (DB9) end to your PC to assist you in aligning the antenna and to issue CLI commands. See the following figure:



The connections are as follows:

D-Shell	RJ11
1	NC
2	2
3	4
4	NC
5	1 + 3 + 5
6	6
7	NC
8	NC
9	NC

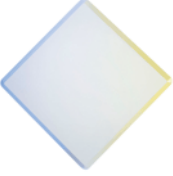




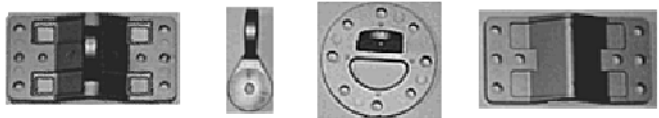
External Antenna Connection























One model of the SU has an integrated antenna; all other models have an external antenna connector (N-type) and no integrated antenna. For more information about external antennas, see the *Antenna Installation Guide*.

Product Package

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

NOTE: Unless noted in this table, cables are not supplied with the unit.

BS / SS with external antenna connector	
RJ45 to DB9 serial connector (supplied with BS only) (1 ea.)	
Installation CD	
Power Injector and Cord	
Cable Termination Kit	<p>Kit includes the following:</p>  <p>a. RJ45 connectors (2) b. Sealing caps (2) c. Sealing nut d. Lock nut e. Grounding screws</p>
Mounting Kit	<p>Kit includes the following:</p>  <p>a. Mounting clamp for wall/pole b. Extension arm c. Mounting plate to enclosure d. Mounting clamp for pole mounting</p>

<p>Mounting Hardware</p>	<p>The following mounting hardware, included with the mounting kit:</p> <table border="0"> <thead> <tr> <th><u>Quantity</u></th> <th><u>Description</u></th> <th></th> </tr> </thead> <tbody> <tr> <td>6 ea.</td> <td>Plain washer #5/16</td> <td></td> </tr> <tr> <td>2 ea.</td> <td>Hex Cap Screw NC 5/16-18 x 35</td> <td></td> </tr> <tr> <td>2 ea.</td> <td>Nut NC 5/16-18</td> <td></td> </tr> <tr> <td>4 ea.</td> <td>Helical Spring Lock Washer #1/4</td> <td></td> </tr> <tr> <td>4 ea.</td> <td>Helical Spring Lock Washer #1/16</td> <td></td> </tr> <tr> <td>2 ea.</td> <td>Hex Cap Screw NC 5/16-18 x 80</td> <td></td> </tr> <tr> <td>4 ea.</td> <td>68764, Screw, Machine, Pan, Philips, 1/4"-20, 5/8"L</td> <td></td> </tr> </tbody> </table>	<u>Quantity</u>	<u>Description</u>		6 ea.	Plain washer #5/16		2 ea.	Hex Cap Screw NC 5/16-18 x 35		2 ea.	Nut NC 5/16-18		4 ea.	Helical Spring Lock Washer #1/4		4 ea.	Helical Spring Lock Washer #1/16		2 ea.	Hex Cap Screw NC 5/16-18 x 80		4 ea.	68764, Screw, Machine, Pan, Philips, 1/4"-20, 5/8"L	
<u>Quantity</u>	<u>Description</u>																								
6 ea.	Plain washer #5/16																								
2 ea.	Hex Cap Screw NC 5/16-18 x 35																								
2 ea.	Nut NC 5/16-18																								
4 ea.	Helical Spring Lock Washer #1/4																								
4 ea.	Helical Spring Lock Washer #1/16																								
2 ea.	Hex Cap Screw NC 5/16-18 x 80																								
4 ea.	68764, Screw, Machine, Pan, Philips, 1/4"-20, 5/8"L																								
<p>Rubber Tape Strip</p>																									

Hardware Installation

This section describes the steps required to install and mount the unit, and to align the antenna. The installation procedure does not include the mounting and connection of antennas. See the documentation that accompanies the antenna and the *Tsunami MP.11 Antenna Installation Guide* for this information.

IMPORTANT:

Before installing and using this product, see *Safety and Regulatory Compliance Information on the product CD*.

NOTES:

- Be sure to read the **Release Notes** file on the product CD as it contains software version and driver information that may not have been available when this document was produced.
- Equipment is to be used with, and powered by, the power injector provided or by a power injector that meets these requirements:
 - UL-Listed/ITE (NWGQ)
 - Limited Power Source Output per UL/IEC 60950
 - CE-marked
 - Approved for Power-over-Ethernet
 - Rated output, 48 Vdc/0.42 A
 - Pinout follows 802.3af standard for mid-span devices

WARNING:

To ensure proper grounding, use the hole at the bottom point on the back of each unit and the provided grounding screws to attach a ground wire of at least 10 AWG stranded to each unit. Use proper wire grounding techniques in accordance with local electric codes.

See the following sections for installation instructions:

- [Step 1: Choose a Location](#)
- [Step 2: Unpack Shipping Box](#)
- [Step 3: Assemble the Cable](#)
- [Step 4: Determine Proper Mounting Orientation](#)
- [Step 5: Assemble Mounting Hardware](#)
- [Step 6: Mount the Unit](#)
- [Step 7: Plug in the Cables](#)
- [Step 8: Power on the Unit](#)
- [Step 9: View LEDs](#)
- [Step 10: Align the Antenna](#)
- [Step 11: Tighten the Cables](#)
- [Step 12: Weatherproof the Connectors](#)
- [Step 13: Install Documentation and Software](#)

Step 1: Choose a Location

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

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

The units are designed to directly mount to a pole. Using the supplied brackets and hardware, you can mount them to a 1.25 inch to 4.5-inch pole (outside diameter). Using just one of the pole mounting brackets, you can mount the units to a wall or other flat surface.

CAUTION: *Proxim recommends the use of a lightning arrestor at the building ingress point. You can purchase the Proxim Lightning Protector; see the documentation that comes with the unit for more information and installation instructions.*

Step 2: Unpack Shipping Box

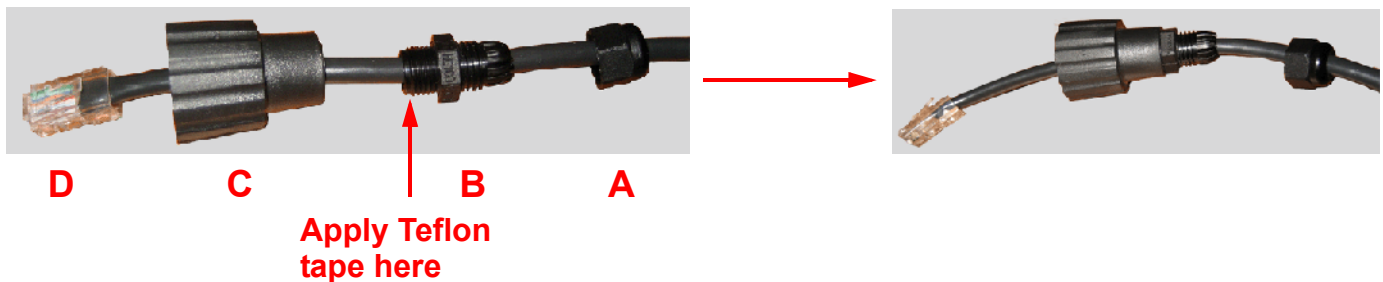
1. Unpack the unit and accessories from the shipping box.
2. Note the Ethernet and MAC addresses of the unit, as well as the serial number; these addresses may be used when configuring the unit.

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

Step 3: Assemble the Cable

You will be attaching an outdoor-rated 24 AWG CAT5 cable (diameter .114 to .250 inches/2.9 to 6.4 mm) (not provided) to the Power-over-Ethernet port on the back of the unit and waterproofing the assembly later in the installation procedure. First, you must construct the cable and assemble the waterproofing cable covers as described in the following steps. Proxim greatly simplifies this assembly process by offering pre-assembled CAT5 cable kits in 25m, 50m, and 75m lengths (part numbers 69819, 69820, and 69821, respectively).

1. Slide the sealing nut (A) over the bare end of the CAT5 cable.
2. Slide the lock nut (B) over the bare end of the CAT5 cable.
3. Slide the sealing cap (C) over the bare end of the CAT5 cable. Make sure the red rubber gasket is inside the cap.
4. Apply two wraps of 0.5" wide Teflon tape (not supplied with unit) around the threads of the lock nut (B) that will go inside the sealing cap.
5. Thread the lock nut (B) onto the sealing cap (C), and hand tighten.
6. Terminate the RJ45 connectors (D) to both ends of the CAT5 cable; test for proper wiring (cable should be a straight-through cable).

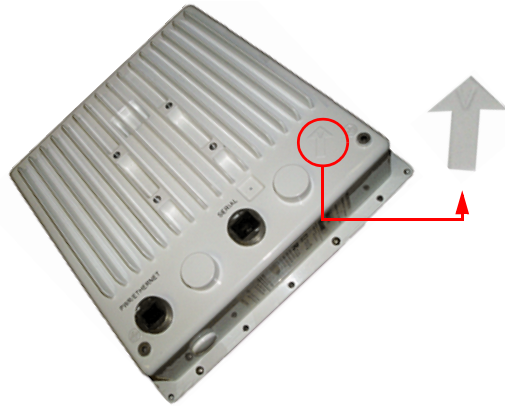


NOTE:

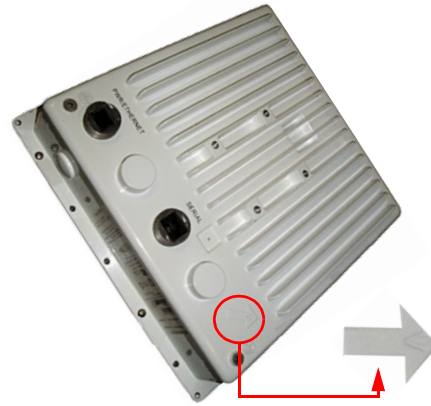
- The cable must feed through all parts of the weatherproof cap before the RJ45 is crimped on the outdoor Ethernet cable.
- The cable between the power injector and the unit must be a straight-through Ethernet cable (without crossover).
- Due to variance in CAT5 cable diameter, termination techniques of the installer, and the application of proper tightness of the connectors, it is strongly recommended that all cable connectors are secured by external weatherproofing. This process will be described in [Step 12: Weatherproof the Connectors](#).

Step 4: Determine Proper Mounting Orientation

1. Locate the arrow on the back of the unit and determine your desired mounting orientation. For *vertical polarization* using the integrated antenna, the arrow should be pointing up (perpendicular to the ground). For *horizontal polarization* using the integrated antenna, the arrow should be horizontal (parallel to the ground).



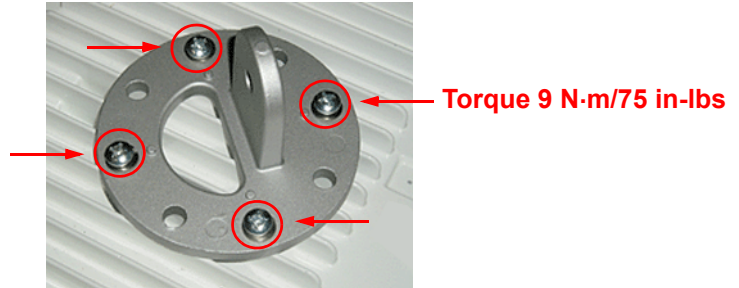
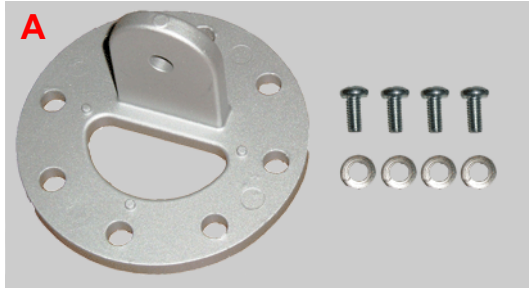
Vertical Polarization



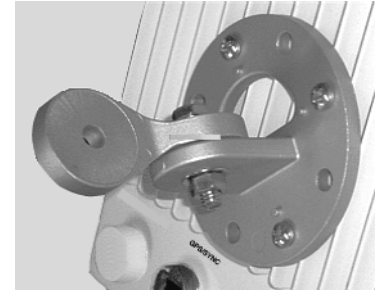
Horizontal Polarization

Step 5: Assemble Mounting Hardware

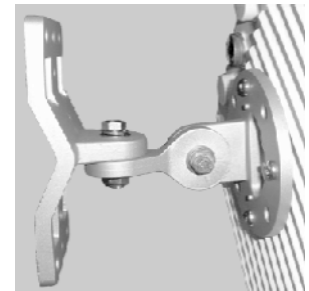
1. Attach the mounting plate (A) using the provided screws and washers (Torque 9 N-m/75 in-lbs), such that the unit's antenna will be vertically or horizontally polarized when mounted.



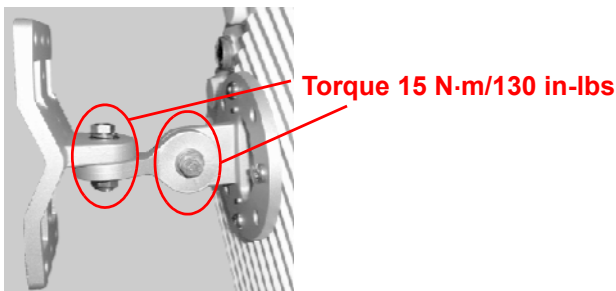
2. Attach the extension arm (B) to mounting piece (A) with the screw, nut, and washers provided, as shown below. The extension arm gives the unit more possible tilt, letting you adjust for azimuth or elevation over a larger angle.



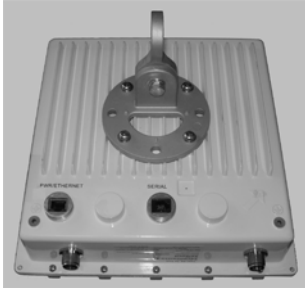
3. Attach the mounting bracket (C) to extension arm (B) with the screw, nut, and washers provided.



4. Tighten assembly (Torque 15 N-m/130 in-lbs).

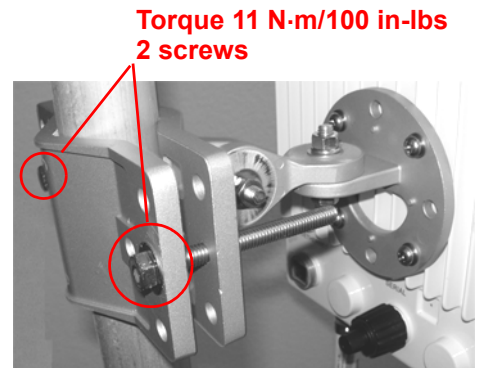
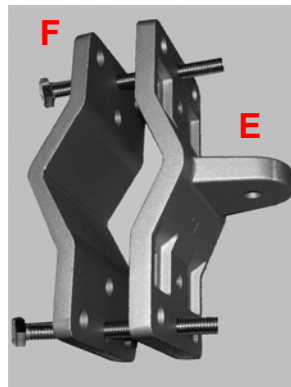
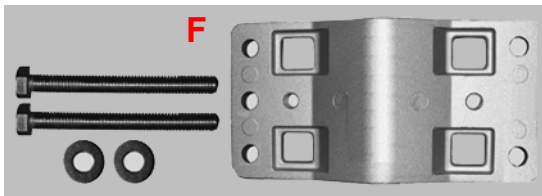


The following figure shows the full assembly attached to the unit:

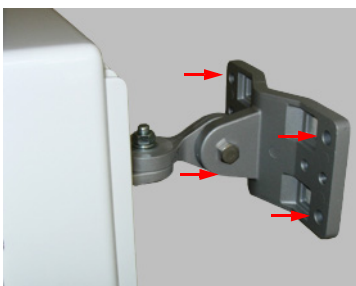


Step 6: Mount the Unit

1. To pole-mount, insert screws through bracket F and fasten around the pole to bracket E and secure (Torque 11 N·m/ 100 in-lbs).

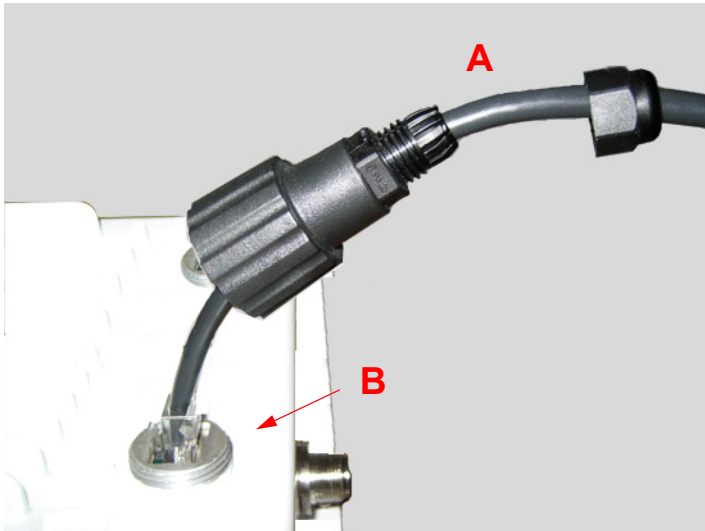


2. To wall-mount the unit, mount bracket E to a wall using 4 screws (not provided), as shown:

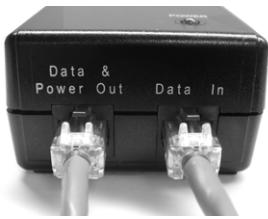


Step 7: Plug in the Cables

1. Plug one end of the CAT5 cable (A) into the RJ45 jack of the unit (B).



2. Connect the free end of the CAT5 cable to the “Data and Power Out” port on the power injector.



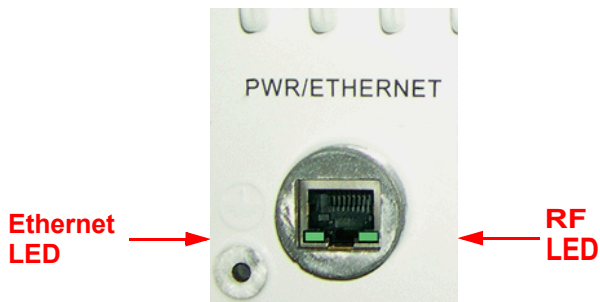
3. To connect the unit through a hub or a switch to a PC, connect a **straight-through Ethernet cable** between the network interface card in the PC and the hub, and between the hub and the RJ45 “Data In” port on the PoE adapter. To connect the unit directly to a PC, connect a **cross-over Ethernet cable** between the network interface card in the PC and the RJ45 “Data In” port on the power injector.

Step 8: Power on the Unit

Once you have connected the power injector to the Ethernet cabling and plugged the power injector cord into an AC outlet, the unit is powered on. There is no ON/OFF switch on the unit. To remove power, unplug the AC cord from the AC outlet or disconnect the RJ45 connector from the “Data and Power Out” port on the power injector.

Step 9: View LEDs

When the unit is powered on, it performs startup diagnostics. When startup is complete, the LEDs show the unit's operational state. The LEDs are present at the unit's Ethernet connector.



LEDs exhibit the following behavior:

LED State	Radio LED	Power/Ethernet LED
Red	Power is on; unit is self-heating.	—
Flashing Green	Wireless link is being established.	Power is on, Ethernet link is down.
Solid Green	Wireless link has been established.	Power is on, Ethernet link is up.

Step 10: Align the Antenna

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

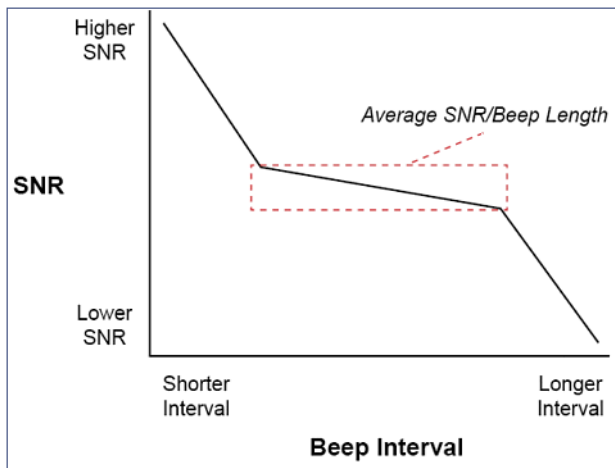
If you are installing external antennas, consult the documentation that accompanies the antenna for installation instructions. Note that you must weatherproof the antenna connectors as described in [Step 12: Weatherproof the Connectors](#).

The unit has an audible antenna alignment tool that can be activated by plugging in the supplied serial dongle (supplied with the BSU) or by issuing the CLI command for antenna alignment. The CLI command causes both audible and numerical feedback as the CLI shows the running Signal-to-Noise Ratio (SNR) values twice a second.

The output from the beeper for antenna alignment consists of short beeps with a variable interval. The interval changes with the SNR level to assist in correctly aligning the antenna. An increase in signal level is indicated by a shorter interval between beeps; a reduction in signal level results in beeps longer apart.

To allow for precise antenna alignment, small changes in SNR result in large changes in the beep period. The alignment process averages the SNR, which is represented by an average length beep. When a higher SNR is received, the beep period is made shorter, dependent upon the difference to the average. A lower SNR results in a longer period between beeps.

The first five steps around the average are represented by a large change and all following steps are a small change. This acts as if a magnifying glass is centered around the average SNR and the values next to the average are significantly different.



When the antenna is aimed, the beep intuitively represents whether the SNR is rising or falling: the higher the SNR rises, the shorter the period the beep is heard and the higher the frequency of the beep.

After the position of the antenna has been changed, SNR averaging settles at the new value and the beeping returns to the average length so the antenna can again be aimed for rising SNR.

Aiming is complete if moving in any direction results in a falling SNR value (which can be heard as longer periods between beeps).

NOTES:

- *Antenna alignment for the Base Station is useful only for a point-to-point link.*
- *The range of the average SNR has been limited to values from 5 to 43; therefore, anything over 43 always results in a short period between beeps and values below 5 always have a long period.*

- *The Antenna Alignment Display (AAD) CLI command is disabled automatically 30 minutes after it is enabled to remove the load of extra messages on the wireless interface. The default telnet timeout is 900 seconds (15 minutes). If AAD must run for the entire 30 minutes, change the default telnet timeout value to a value greater than 30 minutes (greater than 1800 seconds). This restriction is for telnet connections only and not for the serial interface. The serial interface never times out; however, the AAD command does still time out.*

Antenna Alignment Commands

- **set aad enable local**: Enables display of the local SNR. Local SNR is the SNR measured by the receiver at the near end.
- **set aad enable remote**: Enables display of the remote SNR. Remote SNR is the SNR as measured by the receiver at the far end.
- **set aad enable average**: Enables display of the average SNR. The average SNR is the average of the local and remote SNR.
- **set aad disable**: Disables Antenna Alignment Display (Ctrl-C also disables AAD).

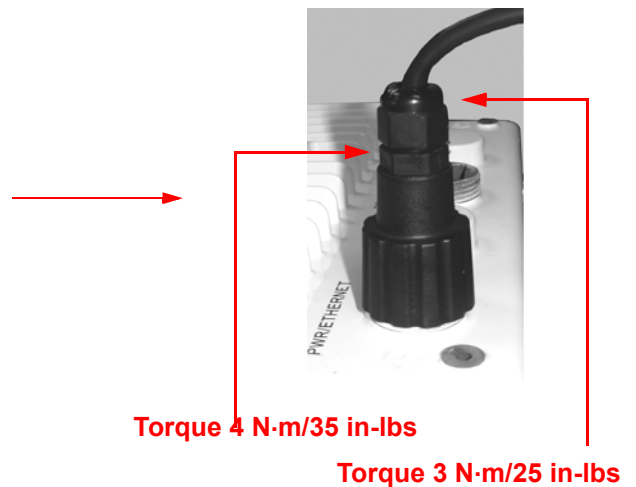
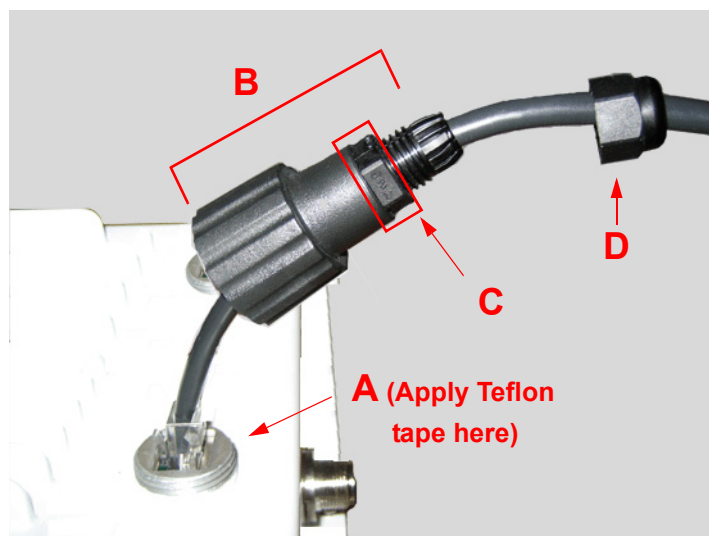
Step 11: Tighten the Cables

1. Apply two wraps of Teflon tape around the threads of the unit's RJ45 jack (A) in a clockwise direction.
2. Make sure that the red rubber gasket is still seated in the sealing cap of the sealing cap/lock nut assembly (B);
3. Slide the sealing cap/lock nut assembly (B) over the RJ45 jack (A) and thread onto enclosure. Hand tighten first, then use a pipe wrench or similar tool to tighten one more quarter turn.

CAUTION: Do not over-tighten!

4. Tighten the lock nut (C) (Torque 4 N·m/35 in-lbs).
5. Thread the sealing nut (D) onto the sealing cap/lock nut assembly (B) and tighten (Torque 3 N·m/25 in-lbs).

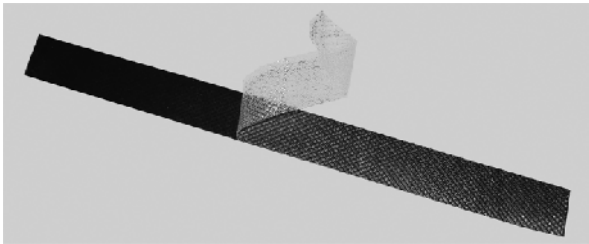
CAUTION: The lock nut (C) on the sealing cap/lock nut assembly (B) must be fully tightened over the RJ45 connector before the sealing nut (D) is fully tightened. Otherwise, the Ethernet cable may twist and damage.



Step 12: Weatherproof the Connectors

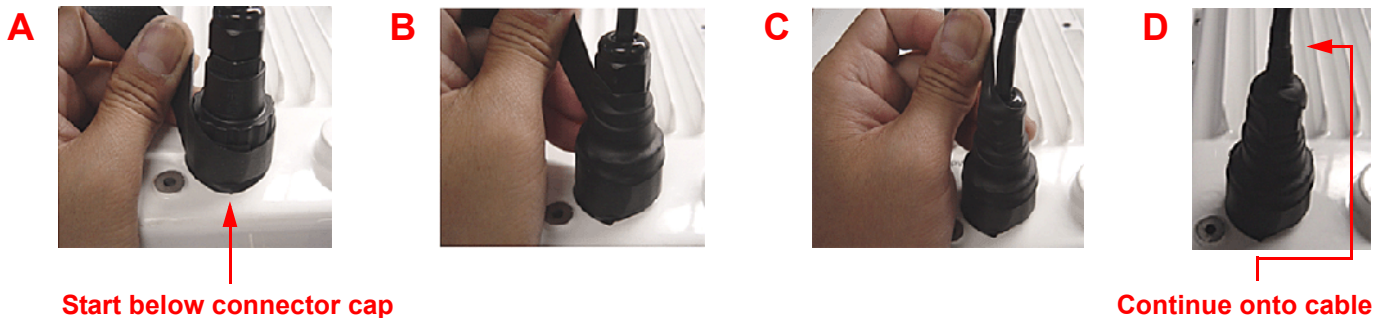
After you have fully assembled and tightened the cable, use the provided self-fusing, rubber-based tape strip and electrical tape (not provided; Proxim recommends Scotch™ Super 33+ Vinyl Electrical Tape) to seal the connection, as follows.

1. Remove the film liner from the rubber-based tape strip, and stretch the tape until it is approximately half of its original width. This activates the self-fusing action of the tape, which will set up over time to create a single, waterproof mass.



2. Stretch and wrap the tape around the connector tightly, starting below the connector cap and against the unit and wrapping in a clockwise direction. Wrap the tape once around the base of the connector cap (A). Continue to wrap the tape spirally around the connector in a clockwise direction, maintaining a 50% width overlap (B). Continue wrapping the tape spirally upward (C) until the tape extends onto the cable and you have used the entire length of tape. Seal the tape tightly against the connector and the cable (D).

NOTE: Be sure to wrap the tape in a clockwise direction; wrapping the tape in a counterclockwise direction may loosen up the connector.



3. In the same manner as described in Step 2 above, apply a layer of black electrical tape (not provided) over the rubber-based tape for further protection. Make sure the electrical tape also extends beyond the rubber-based tape to seal it.



4. Repeat the weatherproofing procedure for other connectors as appropriate.

Step 13: Install Documentation and Software

To install the documentation and software on a computer or network:

1. Place the CD in a CD-ROM drive. The installer normally starts automatically. (If the installation program does not start automatically, click **setup.exe** on the installation CD.)
2. Click the Install Software and Documentation button and follow the instructions displayed on the installer windows. The following documentation and software products are installed:

– Available from **Start > All Programs > Tsunami > MP.11 4954-R:**

- Documentation (in **Docs** subdirectory):
 - Installation and Management Guide
 - Quick Installation Guide
 - Reference Manual
 - Safety and Regulatory Guide
 - Recommended Antenna Guide
 - Antenna Installation Guide
 - Release Notes
- MP.11 4954-R Online Help
- Scan Tool (in **Scan Tool** subdirectory)
- TFTP Server (in **TFTP Server** subdirectory)

NOTE: All of these items are also available from **C:\Program Files\Tsunami\MP.11 4954-R.**

- Available from **C:\Program Files\Tsunami\MP.11 4954-R:**
- Documentation (in **Docs** folder): See list above
 - Help files (in **Help** folder; click on index.htm to access)
 - TFTP Server and Scan Tool program (in **Extras** folder)
 - MIBs (in **MIBs** folder)

Initialization

Connecting to the unit requires either:

- A direct physical connection with an Ethernet cross-over cable or with a serial RS232C cable
- A network connection

Connecting with a serial connection, allows you to configure and manage the unit with the CLI. Connecting with the other connections allows you to use of the Web Interface and SNMP in addition to the CLI.

Using a serial connection, you can access the unit through a terminal emulation program such as HyperTerminal. (See "HyperTerminal Connection Properties" in the *Tsunami MP.11 Reference Manual*.)

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

ScanTool

With ScanTool (a software utility that is included on the product installation CD), you can find out the current IP address of the unit and, if necessary, change it so that is appropriate for your network. The units are shipped with the static IP address 10.0.0.1 configured.

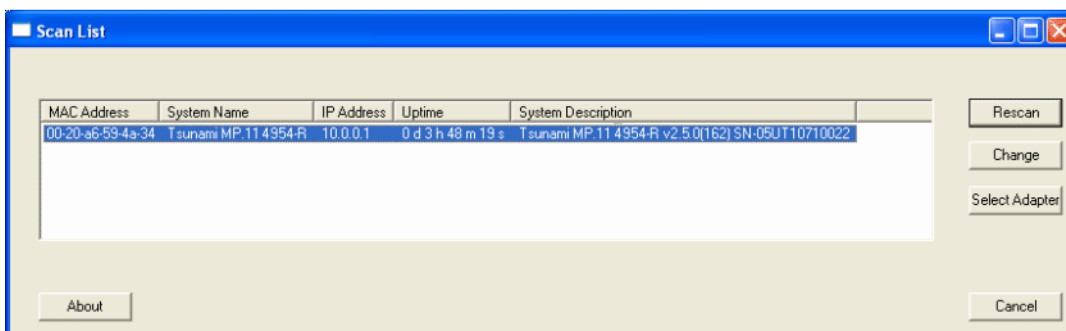
ScanTool lets you find the IP address of a Tsunami MP.11 4954-R by referencing the MAC address in a Scan List, or to assign an IP address if the correct one has not been assigned. The tool automatically detects the units installed on your network segment, regardless of IP address, and lets you configure each unit's IP settings. In addition, you can use ScanTool to download new software to a unit that does not have a valid software image installed.

Setting the IP Address with ScanTool

To discover and set/change the IP address of the unit:

1. Run ScanTool on a computer connected to the same LAN subnet as the unit, or a computer directly connected to the unit with a cross-over Ethernet cable. Double-click the **ScanTool** icon on the Windows desktop to launch the program. If the icon is not on your desktop, click **Start > All Programs > Tsunami > MP.11 4954-R > Scan Tool**.

ScanTool scans the subnet for the 4954-R unit and displays a list of the units it finds in the Scan List window (shown below). If necessary, click **Rescan** to re-scan the subnet and update the display.



You can assign a new IP address to one unit, even if more than one unit has the same (default) IP address 10.0.0.1, but the new IP address must be unique to allow use of the management interfaces.

2. Select the unit for which you want to set the IP address and click **Change**. The **Change** dialog window is displayed, as shown below.

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

Field	Value
MAC Address	00-20-a6-59-4a-34
Name	Tsunami MP.11 4954-R
IP Address Type	Static (selected)
IP Address	10.0.0.1
Subnet Mask	255.255.255.0
Gateway IP Address	10.0.0.1
TFTP Server IP Address	10.0.0.2
Image File Name	FILENAME
Read/Write Password	

- To set the IP address **manually**, ensure that **Static** is selected as the **IP Address Type** and fill in the **IP Address** and **Subnet Mask** suitable for the LAN subnet to which the unit is connected.
To set the IP address **dynamically**, ensure that **Dynamic** is selected as the **IP Address Type**. The unit will request its IP address from a DHCP server on your network.
- Enter the **Read/Write Password** (the default value is **public**) and click **OK** to confirm your changes. The respective unit reboots to make the changes effective.

NOTE: The number of asterisks displayed after you enter the password does not necessarily equal the number of characters in the actual password string. This is done for added security.

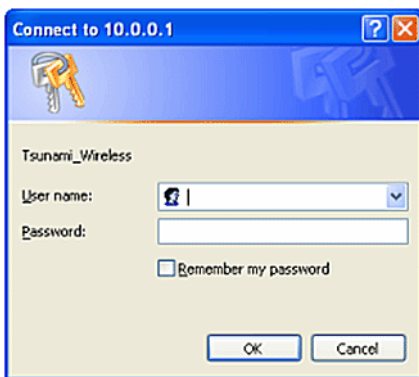
Logging in to the Web Interface

The Web Interface provides a graphical user interface through which you can easily configure and manage the unit. This section describes only how to access the Web Interface.

To use the Web Interface, you need only the IP address of the unit. (See [Setting the IP Address with ScanTool](#) for details).

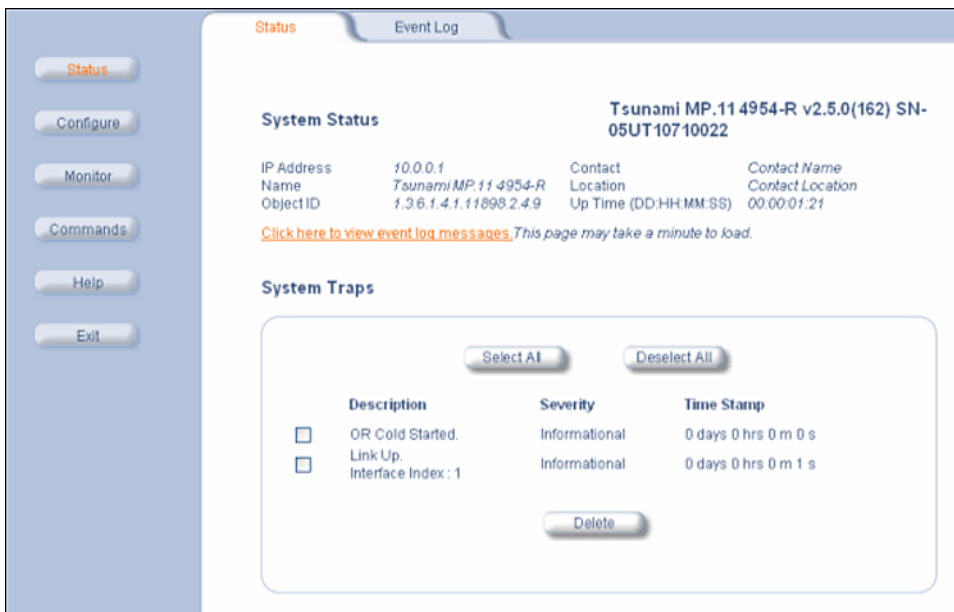
NOTE: *If the connection is slow or you are not able to connect, use the Internet Explorer Tools option to ensure you are not using a proxy server for the connection with your Web browser.*

To access the unit with a Web browser, start your Web browser and enter the IP address of the unit. The Web address must appear as **http://<ip address>** (for example, **http://10.0.0.1**). A window such as the following is displayed.



Do not fill in the **User Name**, enter only the password and click **OK**. The default password is **public**.

The **System Status** window is displayed. To find out more about the information presented in this window, see the [Status](#) chapter.



You now have access to the unit's Web Interface. The remainder of this manual describes configuring and monitoring the unit using this interface.

System Overview

This chapter provides an overview of the system. See the following sections:

- [Changing Basic Configuration Information](#)
- [SU Registration](#)
- [Dynamic Data Rate Selection \(DDRS\)](#)
- [Quality of Service \(QoS\)](#)

Changing Basic Configuration Information

To view or change basic system information, click the **Configure** button on the left side of the Web interface window, then click the **System** tab. See [System Parameters](#) for detailed information about the fields and selections in this window.

NOTE: System Name by default contains the actual model number. The following screenshot is for information only.

The screenshot displays the 'System' configuration window. On the left, there is a vertical menu with buttons for Status, Configure, Monitor, Commands, Help, and Exit. The main area is titled 'Information' and contains the following fields:

- System Name: Tsunami MP.114954-R
- Country: UNITED STATES (US) (dropdown menu)
- Location: Contact Location
- Contact Name: Contact Name
- Contact Email: name@Organization.com
- Contact Phone: Contact Phone Number
- Object ID: 1.3.6.1.4.1.11898.2.4.9
- Ethernet MAC Address: 00:20:A6:59:4A:34
- Descriptor: Tsunami MP.11 4954-R v2.5.0(162) SN-05UT10710022
- Up Time (DD:HH:MM:SS): 00:00:13:09
- Mode of Operation: Bridge (dropdown menu)
- Temperature Logging Interval: 60 Minutes (dropdown menu)

There are two notes in red text:

1. 'Note: Change in Mode of Operation requires a device reboot and appropriate changes to IP Configuration.'

2. 'NOTE: Changes in Logging Interval take effect immediately after clicking OK Button.'

At the bottom of the window are 'OK' and 'Cancel' buttons.

Country and Related Settings

The unit's **Configure System** window provides a selectable **Country** field that automatically provides the allowed bandwidth and frequencies for the selected country.

Units sold in the United States are pre-configured to scan and display only the outdoor frequencies permitted by the FCC. No other **Country** can be configured.

The Transmit Power Control (TPC) feature is always available.

Click **Configure > System**; then select the appropriate country for your regulatory domain from the **Country** drop-down box.

Continue configuring settings as desired; then click **Commands > Reboot** to save and activate the settings. Alternatively, if you want to save the configuration settings to the flash memory but not activate the settings, use the **save config** CLI command.

Transmit Power Control

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

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

You can see your unit's current output power for the selected frequency in the event log. The event log shows the selected power for all data rates, so you must look up the relevant data rate to determine the actual power level.

NOTE: *This feature only lets you decrease your output power; you cannot increase your output power beyond the maximum the radio allows for your frequency and data rate.*

See [Configure the Wireless Interface](#) to configure Transmit Power Control.

SU Registration

The list of parameters you must configure for registration of the SU on a BSU are:

- Network Name
- Base Station System Name (when used; otherwise, leave blank)
- Network Secret
- Encryption (when used)
- Frequency Channel (or Roaming)

See [System Parameters](#) to see the description of these fields and to configure them.

NOTES:

- *The frequency channel must be the same for the BSU and the SU in order to register the SU when roaming is not enabled.*
- *Channel Bandwidth and Turbo mode must be the same for the BSU and SU in order to register the SU.*
- *Roaming will automatically select a channel on the SU corresponding to the BSU channel. Roaming is the procedure in which an SU terminates the session with the current BSU and starts the registration procedure with another BSU when it finds the quality of the other BSU to be better.*

Dynamic Data Rate Selection (DDRS)

The WORP Dynamic Data Rate Selection (DDRS) lets the BSU and SUs monitor and calculate the remote average signal-to-noise ratio (SNR) and adjust the transmission data rate to an optimal value to provide the best possible throughput according to the current communication conditions and link quality during run-time.

Each frame received in the WORP protocol reports the signal and noise level in dBm at which the sender received the previous frame from the receiver, and provides the values to calculate the SNR in dB. SNR is calculated according to this formula then averaged:

$$\text{SNR [dB]} = \text{signal level [dBm]} - \text{noise level [dBm]}$$

Both the BSU and the SUs monitor the remote SNR. The BSU monitors and calculates the average remote SNR for each SU that is registered. An SU monitors and calculates the average remote SNR for the BSU.

DDRS is enabled or disabled on the BSU only. This operation requires the BSU to be rebooted. After rebooting, the BSU sends a multicast announcement to all SUs to begin the registration process. During registration, an SU is informed by the BSU whether DDRS is enabled or disabled and it sets its DDRS status accordingly.

There are two DDRS data rates that need to be configured when DDRS is enabled:

- **Default DDRS Data Rate** (*ddrsdefdatarate*): The data rate at which the BSU starts communication with all SUs to begin the registration process (the default is 6 Mbps).
- **Maximum DDRS Data Rate** (*ddrsmaxdatarate*): The maximum data rate at which the device (BSU or SU) can operate (the default is 54 Mbps).

NOTE: The default (BSU only) and maximum (BSU and SU) DDRS data rate values must be configured in the BSU and SUs separately through the CLI or the SNMP interface.

Virtual Local Area Networks (VLANs)

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

Tsunami MP.11 4954-R units are fully VLAN-ready; however, by default, VLAN support is disabled. Before enabling VLAN support (by assigning a VLAN Management ID), certain network settings should be configured and network resources such as VLAN-aware switches should be available, dependent upon the type of configuration.

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

- Manage VLAN configuration from a single window
- Define groups
- Reduce broadcast and multicast traffic to unnecessary destinations
 - Improve network performance and reduce latency
- Increase security
 - Secure network restricts members to resources on their own VLAN

VLAN tagged data is collected and distributed through a unit's Ethernet interface. The units can communicate across a VLAN-capable switch that analyzes VLAN-tagged packet headers and directs traffic to the appropriate ports when the units are working in their Transparent mode.

VLAN features can be managed via:

- The BSU's Web interface
- The Command Line Interface (see "Command Line Interface" in the *Reference Manual*)
- SNMP (see the MIBs provided on the product CD)

For more information about VLAN configuration, see [VLAN Parameters](#).

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 main priority is to guarantee a reliable and adequate transmission quality for all types of traffic under conditions of high congestion and bandwidth over-subscription.

Concepts and Definitions

The software supports QoS provisioning from the BSU only. You may define different classes of service on a BSU that can then be assigned to the SUs that are associated, or that may get associated, with that BSU.

The software provides the ability to create, edit, and delete classes of service that are specified by the following hierarchy of parameters:

- Packet Identification Rule (PIR) – up to 64 rules, including 17 predefined rules
- Service Flow class (SFC) – up to 32 SFs, including 7 predefined SFCs; up to 8 PIRs may be associated per SFC
- Priority for each rule within each SF class – 0 to 255, with 0 being lowest priority
- QoS class – up to 8 QoS classes, including 4 predefined classes; up to 4 SFCs may be associated per QoS class

Packet Identification Rule (PIR)

A Packet Identification Rule is a combination of parameters that specifies what type of traffic is allowed or disallowed. The software allows to create up to 64 different PIRs, including 17 predefined PIRs. It provides the ability to create, edit, and delete PIRs that contain none, one, or more of the following classification fields:

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

A good example is provided by the 17 predefined PIRs. Note that these rules help to identify specific traffic types:

1. All – No classification fields, all traffic matches
2. Cisco VoIP UL
 - a. Protocol Source Port Range (16,000-32,000)
 - b. IP Protocol List (17 = UDP)
3. Vonage VoIP UL
 - a. Protocol Source Port Range (8000-8001, 10000-20000)
 - b. IP Protocol List (17 = UDP)
4. Cisco VoIP DL
 - a. Protocol Destination Port Range (16,000-32,000)
 - b. IP Protocol List (17 = UDP)
5. Vonage VoIP DL

Quality of Service (QoS)

- a. Protocol Destination Port Range (8000-8001, 10000-20000)
- b. IP Protocol List (17 = UDP)
6. TCP
 - a. IP Protocol List (6)
7. UDP
 - a. IP Protocol List (17)
8. PPPoE Control
 - a. Ethertype (type 1, 0x8863)
9. PPPoE Data
 - a. Ethertype (type 1, 0x8864)
10. IP
 - a. Ethertype (type 1, 0x800)
11. ARP
 - a. Ethertype (type 1, 0x806)
12. Expedited Forwarding
 - a. IP TOS/DSCP (low=0x2D, high=0x2D, mask = 0x3F)
13. Streaming Video (IP/TV)
 - a. IP TOS/DSCP (low=0x0D, high=0x0D, mask = 0x3F)
14. 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)
15. 802.1p Voice
 - a. Ethernet Priority (low=6, high=6) (this is the equivalent of the User Priority value in the TCI (Tag Control Information) field of a VLAN tag)
16. 802.1p Video
 - a. Ethernet Priority (low=5, high=5) (this is the equivalent of the User Priority value in the TCI (Tag Control Information) field of a VLAN tag)
17. L2 Broadcast/Multicast
 - a. Ethernet Destination (dest = 0x80000000, mask = 0x80000000)

Two different VoIP rule names have been defined for each direction of traffic, Uplink (UL) and Downlink (DL), (index numbers 2 to 5). 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.

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. The software allows to create up to 32 different SFs, including seven predefined SFs. The software provides the ability to create, edit, and delete SFs that contain the following parameters and values:

- Service flow name
- Scheduling type – Best Effort (BE); Real-Time Polling Service (RtPS)
- Service Flow Direction – Downlink (DL: traffic from BSU to SU); Uplink (UL: traffic from SU to BSU)
- Maximum sustained data rate (or Maximum Information Rate, MIR) – specified in units of 1 Kbps from 8 Kbps up to the maximum rate of 108000 Kbps per SU
- Minimum reserved traffic rate (or Committed Information Rate, CIR) – specified in units of 1 Kbps from 0 Kbps up to the maximum rate of 10000 Kbps per SU

Quality of Service (QoS)

- Maximum Latency – specified in increments of 5 ms steps from a minimum of 5 ms up to a maximum of 100 ms
- Tolerable Jitter – specified in increments of 5 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 four (4), which affects the percentage of the maximum throughput of the system
- Activation state – Active; Inactive

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

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

Users are able to 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 seven predefined SFCs:

1. UL-Unlimited BE
 - a. Scheduling Type = Best Effort
 - b. Service Flow Direction = Uplink
 - c. Initialization State = Active
 - d. Maximum Sustained Data Rate = 20 Mbps
 - e. Traffic Priority = 0
2. DL-Unlimited BE (same as UL-Unlimited BE, except Service Flow Direction = Downlink)
3. UL-G711 20 ms VoIP rtPS
 - a. Schedule type = Real time Polling
 - b. Service Flow Direction = Uplink
 - c. Initialization State = Active
 - d. Maximum Sustained Data Rate = 88 Kbps
 - e. Minimum Reserved Traffic Rate = 88 Kbps
 - f. Maximum Latency = 20 milliseconds
 - g. Traffic Priority = 1
4. DL-G711 20 ms VoIP rtPS (same as UL-G711 20ms VoIP rtPS, except Service Flow Direction = Downlink)
5. UL-G729 20 ms VoIP rtPS (same as UL-G711 20ms VoIP rtPS, except Maximum Sustained Data Rate and Maximum Reserved Traffic Rate = 64 Kbps)
6. DL-G729 20 ms VoIP rtPS (same as UL-G729 20ms VoIP rtPS, except Service Flow Direction = Downlink)
7. 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

Two different VoIP Service Flow classes for each direction of traffic have been defined (index numbers 3 to 6) 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.

QoS Class

A QoS class is defined by a set of parameters that includes the PIRs and SFCs that were previously configured. The software allows creating up to eight different QoS classes, including four predefined QoS classes. Up to four 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".

The software provides the ability to 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 four 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 0-63, with priority 63 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 four 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. 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
3. 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
4. 2Mbps Video
 - a. SF class: DL-2Mbps Video
PIR: Streaming Video (IP/TV); PIR Priority: 1

Basic Management

This chapter describes basic features and functionality of the unit. In most cases, configuring these basic features is sufficient. The “Glossary” in the *Tsunami MP.11 Reference Manual* provides a brief explanation of the terms used. For CLI commands you can use for basic management, see “Command Line Interface” in the *Tsunami MP.11 Reference Manual*.

The following topics are discussed in this chapter:

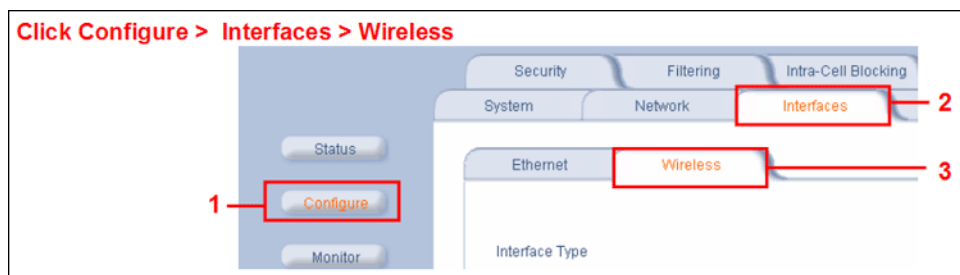
- [Navigation](#)
- [Rebooting and Resetting](#)
- [General Configuration Settings](#)
- [Monitoring Settings](#)
- [Security Settings](#)
- [Default Settings](#)
- [Upgrading the Unit](#)

Navigation

To use the Web Interface for configuration and management, you must access the unit. With ScanTool you can determine the unit’s current IP address. Then enter **http://<ip address>** in your Web browser (for example **http://10.0.0.1**). See [Setting the IP Address with ScanTool](#) for details.

NOTE: If you have your Security Internet Options set to **High**, you may not be able to access the Web interface successfully; a high security setting disables JavaScript, which is required for running Proxim’s Web browser interface. Adding the radio’s IP address as a Trusted site should fix this problem.

The Web Interface consists of Web page buttons and tabs. A tab can also contain sub-tabs. The following figure shows the convention used to guide you to the correct tab or sub-tab.



The Web Interface also provides online help, which is stored on your computer (see [Step 13: Install Documentation and Software](#) for details).

Rebooting and Resetting

All configuration changes require a restart unless otherwise stated. You can restart the unit with the **Reboot** command; see [Rebooting](#), below).

Most changes you make become effective only when the unit is rebooted. A reboot stores configuration information in non-volatile memory and then restarts the unit with the new values (see [Soft Reset to Factory Default](#)).

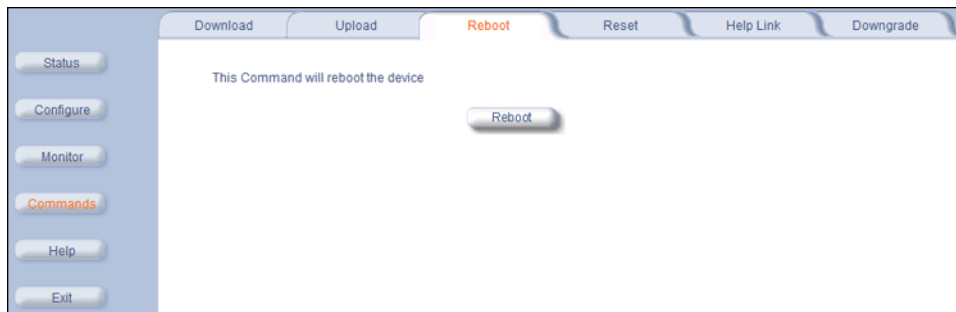
In some cases, the unit reminds you that a reboot is required for a change to take effect. You need not reboot immediately; you can reboot after you have made all your changes.

NOTE: *Saving of the unit's configuration occurs only during a controlled reboot or by specifically issuing the CLI **Save** command. If you make changes to settings without a controlled reboot (command) and you have not issued the **Save** command, a power outage would wipe out all changes since the last reboot. For example, entering static routes takes effect immediately; however, the routes are not saved until the unit has gone through a controlled reboot. Proxim strongly recommends saving your settings immediately when you finish making changes.*

Rebooting

When you reboot, the changes you have made become effective and the unit is restarted. The changes are saved automatically in non-volatile memory before the actual reboot takes place.

To reboot, click **Commands > Reboot > Reboot**. The unit restarts the embedded software. During reboot, you are redirected to a page showing a countdown timer, and you are redirected to the **Status** page after the timer counts down to 0 (zero). The CLI is disconnected during reboot. This means that a new telnet session must be started.



Resetting Hardware

If the unit does not respond for some reason and you are not able to reboot, you can restart by means of a hardware reset. This restarts the hardware and embedded software. The last saved configuration is used. Any changes that you have made since then are lost.

To reset the hardware, unplug the unit's power supply and then reconnect power to the unit.

Soft Reset to Factory Default

If necessary, you can reset the unit to the factory default settings. *This should be done only when you are experiencing problems.* Resetting to the default settings requires you to reconfigure the unit.

To reset to factory default settings:

1. Click **Commands > Reset**.
2. Click the **Reset to Factory Default** button. The device configuration parameter values are reset to their factory default values.



If you do not have access to the unit, you can use the procedure described in [Hard Reset to Factory Default](#) as an alternative.

General Configuration Settings

- **System Status:** The Status tab showing the system status is displayed automatically when you log into the Web interface. It is also the default window displayed when you click the **Status** button on the left side of the window. See [System Status](#).
- **System Configuration:** The System Configuration window lets you change the unit's *country*, *system name*, *location name*, and so on (see the window to the right). The Country selection is required to enable the correct radio parameters. The other details help distinguish this unit from other routers, and let you know whom to contact in case of problems. See [System Parameters](#) for more information.
- **IP Configuration:** The **IP Configuration** window lets you change the unit's IP parameters. These settings differ between **Routing** and **Bridge** mode. See [Network Parameters](#) for more information.
- **Interface Configuration:** The **Interface** configuration pages let you change the Ethernet and Wireless parameters. The **Wireless** tab is displayed by default when you click the **Interfaces** tab.
 - **Ethernet:** To configure the **Ethernet** interface, click **Configure > Interfaces > Ethernet**. You can set the **Configuration** parameter from this tab for the type of Ethernet transmission. The recommended setting is **auto-speed auto-duplex**. See [Configure the Ethernet Interface](#) for more information.
 - **Wireless:** To configure the **wireless** interface, click **Configure > Interfaces > Wireless**. For BSUs, the wireless interface can be placed in either **WORP Base** or **WORP Satellite** mode (selected from the **Interface Type** drop-down box). SUs can be placed only in **WORP Satellite** mode. (See [Interface Parameters](#) for more information.)
- **VLAN Configuration:** To configure BSU VLAN parameters, click the **Configure** button followed by the **VLAN** tab; the **BSU Table** tab is displayed. Click the **SUs' Table** tab to configure SU VLAN parameters. Virtual LAN (VLAN) implementation in the Tsunami MP.11 products lets the BSU and SU be used in a VLAN-aware network and processes IEEE 802.1Q VLAN-tagged packets. Network resources behind the BSU and SU can be assigned to logical groups. See [VLAN Parameters](#) for more information.

Monitoring Settings

The unit offers various facilities to monitor its operation and interfaces. Only the most significant monitoring categories are mentioned here.

- **Wireless:** To monitor the wireless interfaces, click **Monitor > Wireless**. This tab lets you monitor the general performance of the radio and the performance of the **WORP Base** or **WORP Satellite** interfaces.
- **Interfaces:** To monitor transmission details, click **Monitor > Interfaces**. The **Interfaces** tab provides detailed information about the MAC-layer performance of the wireless network and Ethernet interfaces.
- **Per Station:** Click **Monitor > Per Station** to view **Station Statistics**. On the SU, the **Per Station** page shows statistics of the BSU to which the SU is registered. On the BSU, it shows statistics of all the SU's connected to the BSU. The page's statistics refresh every 4 seconds.

Security Settings

To prevent misuse, the 4954-R provide wireless data encryption and password-protected access. *Be sure to set the encryption parameters and change the default passwords.*

In addition to Wired Equivalent Privacy (WEP), the units support Advanced Encryption Standard (AES) 128-bit encryption. Two types of the AES encryption are available. Previous releases supported only the AEC-OCB; the AES CCM protocol is now also supported.

Proxim highly recommends you change the **Network Name**, **Encryption Key**, and **Shared Secret** as soon as possible. To do so, click **Configure > Interfaces > Wireless**. The encryption key is set using the **Security** tab. For systems that will use roaming features, the **Network Name**, **Encryption Key**, and the **Shared Secret** should each be the same for all SUs that are allowed to roam as well as for all BSUs to which these SUs are allowed to roam.

Encryption

You can protect the wireless data link by using encryption. Encryption keys can be 5 (64-bit), 13 (WEP 128-bit), or 16 (AES 128-bit) characters in length. Both ends of the wireless data link must use the same parameter values.

To set the encryption parameters, click **Configure > Security > Encryption**. See [Configure Encryption Parameters](#).

Passwords

Access to the units are protected with passwords. The default password is **public**. For better security it is recommended to change the default passwords to a value (6-32 characters) known only to you.

To change the unit's HTTP, Telnet, or SNMP passwords, click **Configure > Management > Password**. See [Configure Passwords](#).

Default Settings

Feature	Default
System Name	Tsunami MP.11 4954-R
Mode of Operation	Bridge
Routing	Disabled
IP Address Assignment Type	Static
IP Address	10.0.0.1
Subnet Mask	255.255.255.0
Default Router IP Address	10.0.0.1
Default TTL	64
RIPv2	Enabled when in Routing Mode
Base Station System Name	<blank>
Network Name	OR_WORP
Frequency Channel	Channel 149, Frequency 5.745 GHz (FCC Only devices)
Transmit Power Control	0 dB
Data Rate	36 Mbps
Registration Timeout	5
Network Secret	public
Turbo Mode	Disabled
Channel Bandwidth	20 MHz
Input bandwidth limit (in Kbps)	36032
Output bandwidth limit (in Kbps)	36032
Ethernet Configuration	Auto-Speed Auto-Duplex
Serial port Baud Rate	9600
SNMP Management Interface	Enabled
Telnet Management Interface	Enabled
HTTP Management Interface	Enabled
HTTP Port	80
Telnet Port	23
Telnet Login Timeout	30
Telnet Session Timeout	900
Password	public
Maximum Satellites (per BSU)	250
MAC Authentication	Disabled
Radius Authentication	Disabled
Encryption	Disabled
Static MAC Address Filter	Disabled / No Entries
Ethernet Protocol Filtering	All Filters Disabled
DFS Priority Frequency Channel	Disabled
Announcement Period (when roaming enabled)	100 ms
Multi-Frame Bursting	Enabled
Storm Threshold	Broadcast/Multicast Unlimited
Broadcast Protocol Filtering	All Protocols Allowed

Feature	Default
Dynamic Data Rate Selection	Disabled
Roaming	Disabled
NAT	Disabled
Intra-Cell Blocking	Disabled
Antenna Alignment	Disabled
Country Selection	US-only device – US World device – GB
DHCP Server	Disabled
DHCP Relay	Disabled
Spanning Tree Protocol	Disabled
Antenna Gain (For DFS Threshold compensation)	0
Satellite Density	Large
Temperature Logging	Enabled
Temperature Logging Interval	60 minutes
VLAN Mode	BSU: Transparent Mode SU: Transparent mode when BSU in transparent mode; Trunk mode when BSU in Trunk mode
Access VLAN ID	BSU: N/A; SU: 1
Access VLAN Priority	BSU: N/A; SU: 0
Management VLAN ID	BSU: -1; SU: -1
Management VLAN Priority	BSU: 0; SU: 0
VLAN ID in Trunk VLAN Table	BSU: N/A; SU: 1

Upgrading the Unit

The units are equipped with embedded software that can be updated when new versions are released. Updating the embedded software is described in [Web Interface Image File Download](#). A TFTP server is provided on the Documentation and Software CD; the server is required to transfer the downloaded file to the unit. See [TFTP Server Setup](#).

To access all resolved problems in our solution database, or to search by product, category, keywords, or phrases, go to <http://support.proxim.com>. You can also find links to drivers, documentation, and downloads at this link.

System Status

This chapter describes viewing system status and event log information from the unit's Web Interface.

Click on the **Status** button to access system and event log information. See the following sections:

- [Status](#)
- [Event Log](#)

Help and Exit buttons also appear on each page of the Web interface; click the **Help** button to access online help; click the **Exit** button to exit the application.

For an introduction to the basics of management, see [Basic Management](#).

Status

The **Status** tab showing the system status is displayed automatically when you log into the Web Interface. It also is the default window displayed when you click the **Status** button on the left side of the window.

The **Status** tab shows the **System Status** and the **System Traps**.

The screenshot shows the 'Status' tab of the web interface. On the left is a navigation menu with buttons for Status, Configure, Monitor, Commands, Help, and Exit. The main content area has two tabs: 'Status' (active) and 'Event Log'. Under 'System Status', the device is identified as 'Tsunami MP.11 4954 v2.5.0(162) SN-04AT35580031'. A table lists system details:

IP Address	10.0.0.1	Contact	Contact Name
Name	Tsunami MP.11 Model 4954	Location	Contact Location
Object ID	1.3.6.1.4.1.11898.2.4.9	Up Time (DD:HH:MM:SS)	00:00:00:55

Below this is a link: [Click here to view event log messages.](#) This page may take a minute to load.

The 'System Traps' section contains 'Select All' and 'Deselect All' buttons, a table with two traps, and a 'Delete' button.

Description	Severity	Time Stamp
<input type="checkbox"/> OR Cold Started.	Informational	0 days 0 hrs 0 m 0 s
<input type="checkbox"/> Link Up. Interface Index : 1	Informational	0 days 0 hrs 0 m 1 s

System Status

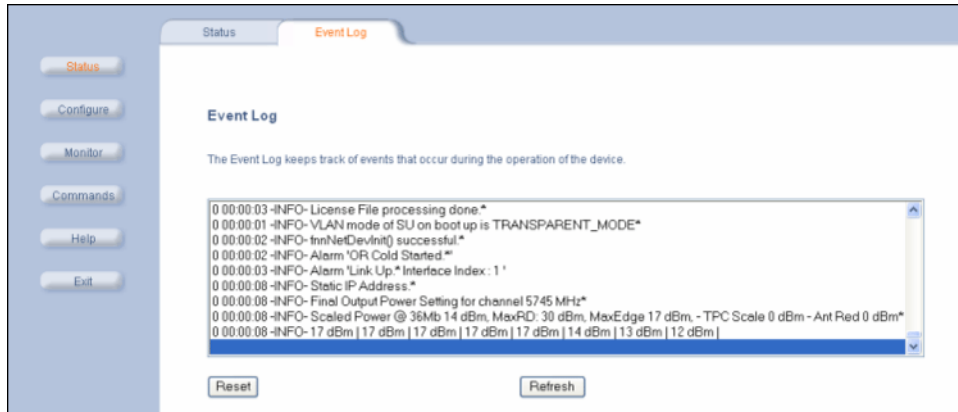
The basic system status is shown in this section, including the version number of the embedded software.

Systems Traps

The status of system traps is shown in this section. System traps occur when the unit encounters irregularities. Deleting system traps has no effect on the operation of the unit. System traps also are sent to an SNMP manager station (if so configured). See "Alarm Traps" in the *Tsunami MP.11 Reference Manual* for a list and description of the traps.

Event Log

Click **Status > Event Log** to view the contents of your Event Log. The **Event Log** keeps track of events that occur during the operation of the unit. The **Event Log** displays messages that may not be captured by System Traps, such as the **Transmit Power** for the **Frequency Channel** selected.



See “Event Log Error Messages” in the *Tsunami MP.11 Reference Manual* for an explanation of messages that can appear in the Event Log.

Configuration

This chapter describes configuring the unit's settings using the unit's Web Interface.

Click the **Configure** button to access configuration settings.

The following topics are discussed in this section:

- [System Parameters](#)
- [Network Parameters](#)
- [Interface Parameters](#)
- [SNMP Parameters](#)
- [RIP Parameters](#)
- [Management Parameters](#)
- [Security Parameters](#)
- [Filtering Parameters](#)
- [Intra-Cell Blocking \(Base Station Unit Only\)](#)
- [VLAN Parameters](#)
- [QoS \(Quality of Service\) Parameters](#)
- [SU Access to the Public Network \(NAT\)](#)

Help and Exit buttons also appear on each page of the Web interface; click the **Help** button to access online help; click the **Exit** button to exit the application.

For an introduction to the basics of management, see [Basic Management](#).

System Parameters

The **System** configuration page lets you change the unit's **System Name**, **Location**, **Mode of Operation**, and so on. These details help you to distinguish the unit from other routers and let you know whom to contact in case you experience problems.

Click **Configure** > **System**; the following window is displayed.

The screenshot shows a web-based configuration interface for a network device. The 'System' tab is selected, and the 'Information' section is active. The configuration fields are as follows:

- System Name:** Tsunami MP.114954-R
- Country:** UNITED STATES (US)
- Location:** Contact Location
- Contact Name:** Contact Name
- Contact Email:** name@Organization.com
- Contact Phone:** Contact Phone Number
- ObjectID:** 1.3.6.1.4.1.11898.2.4.9
- Ethernet MAC Address:** 00:20:A6:59:4A:34
- Descriptor:** Tsunami MP.11 4954-R v2.5.0(162) SN-05UT10710022
- Up Time (DD:HH:MM:SS):** 00:00:13:09
- Mode of Operation:** Bridge
- Temperature Logging Interval:** 60 Minutes

There are 'OK' and 'Cancel' buttons at the bottom of the window.

You can enter the following details:

- **System Name:** This is the system name for easy identification of the BSU or SU. The System Name field is limited to a length of 32 bytes. Use the system name of a BSU to configure the Base Station System Name parameter on an SU if you want the SU to register only with this BSU. If the Base Station System Name is left blank on the SU, it can register with any Base Station that has a matching Network Name and Network Secret.
- **Country:** Displays the country of operation.
- **Location:** This field can be used to describe the location of the unit, for example “Main Lobby.”
- **Contact Name, Contact Email, and Contact Phone:** In these fields, you can enter the details of the person to contact.
- **Mode of Operation:** This field sets the unit as **bridge** (layer 2) or as **router** (layer 3). See [Bridge and Routing Modes](#) for more information.
- **Temperature Logging Interval:** This field sets the interval at which unit temperature is logged.

The static fields on this window are described as follows:

- **ObjectID:** This field shows the OID of the product name in the MIB.
- **Ethernet MAC Address:** The MAC address of the Ethernet interface of the device.
- **Descriptor:** Shows the product name and firmware build version.
- **Up Time:** The length of time the device has been up and running since the last reboot.

Bridge and Routing Modes

Bridge Mode

A bridge is a product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet). You can envision a bridge as being a device that decides whether a message from you to someone else is going to the local area network in your building or to someone on the local area network in the building across the street. A bridge examines each message on a LAN, passing those known to be within the same LAN, and forwarding those known to be on the other interconnected LAN (or LANs).

In bridging networks, computer or node addresses have no specific relationship to location. For this reason, messages are sent out to every address on the network and accepted only by the intended destination node. Bridges learn which

addresses are on which network and develop a learning table so that subsequent messages can be forwarded to the correct network.

Bridging networks are generally always interconnected LANs since broadcasting every message to all possible destination would flood a larger network with unnecessary traffic. For this reason, router networks such as the Internet use a scheme that assigns addresses to nodes so that a message or packet can be forwarded only in one general direction rather than forwarded in all directions.

A bridge works at the data-link (physical) layer of a network, copying a data packet from one network to the next network along the communications path.

The default Bridging Mode is **Transparent Bridging**.

This mode works if you do not use source routing in your network. If your network is configured to use source routing, then you should use either Multi-Ring SRTB or Single-Ring SRTB mode.

In Multi-Ring SRTB mode, each unit must be configured with the Bridge number, Radio Ring number, and Token Ring number. The Radio Ring number is unique for each Token Ring Access Point and the Bridge number is unique for each Token Ring Access Point on the same Token Ring segment.

Alternatively, you may use the Single-Ring SRTB mode. In this mode, only the Token Ring number is required for configuration.

Routing Mode

Routing mode can be used by customers seeking to segment their outdoor wireless network using routers instead of keeping a transparent or bridged network. By default the unit is configured as a bridge device, which means traffic between different outdoor locations can be seen from any point on the network.

By switching to routing mode, your network now is segmented by a layer 3 (IP) device. By using Routing mode, each network behind the BSU and SUs can be considered a separate network with access to each controlled through routing tables.

The use of a router on your network also blocks the retransmission of broadcast and multicast packets on your networks, which can help to improve the performance on your outdoor network in larger installations.

The use of Routing mode requires more attention to the configuration of the unit and thorough planning of the network topology of your outdoor network. The unit can use Routing mode in any combination of BSU and SUs. For example, you may have the BSU in Routing mode and the SU in Bridge mode, or vice versa.

When using Routing mode, pay close attention to the configuration of the default gateway both on your unit and on your PCs and servers. The default gateway controls where packets with unknown destinations (Internet) should be sent. Be sure that each device is configured with the correct default gateway for the next hop router. Usually this is the next router on the way to your connection to the Internet. You can configure routes to other networks on your Intranet through the addition of static routes in your router's routing table.

Key Reasons to Use Routing Mode

One key reason why customers would use Routing mode is to implement virtual private networks (VPNs) or to let nodes behind two different SUs communicate with each other. Many customers do this same thing in Bridging mode by using secondary interfaces on the router at the BSU or virtual interfaces at the BSU in VLAN mode to avoid some of the drawbacks of IP Routing mode.

Routing mode prevents the transport of non-IP protocols, which may be desirable for Service Providers.

Routing mode is usually more efficient because Ethernet headers are not transported and non-IP traffic is blocked.

Benefits of using Routing Mode

- Enabling RIP makes the unit easier to manage for a Service Provider that uses RIP to dynamically manage routes. RIP is no longer very common for Service Providers or Enterprise customers and an implementation of a more popular routing protocol like OSPF would be desirable.

- Routing mode saves bandwidth by not transporting non-IP protocols users might have enabled, like NetBEUI or IPX/SPX, which eliminates the transmission of broadcasts and multicasts.
 - The MAC header is:
 - Destination MAC: 6 bytes
 - Source MAC: 6 bytes
 - Ethernet Type: 2 bytes

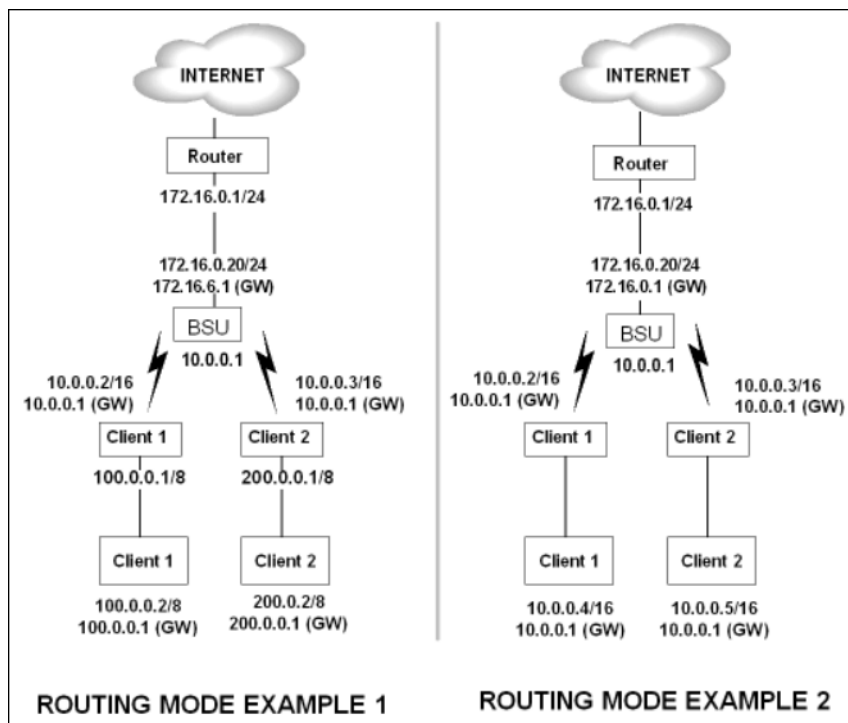
If the average packet size is 1000 bytes, the overhead saved is 1.5%; With a frame size of 64 bytes, the overhead saved is 20%; and for frame sizes of 128 bytes, the saving is 10%. Network researches claim that most network traffic consists of frames smaller than 100 bytes.

In order to support routers behind the SUs with multiple subnets and prevent routing loops, you want individual routes (and more than one) per SU.

Routing Mode Examples

In the first example, both the BSU and the SUs are configured for Routing mode. This example is appropriate for businesses connecting remote offices that have different networks.

In example 2, the BSU is in Routing mode and the SUs are in Bridge mode. Notice the PCs behind the SUs must configure their default gateways to point to the BSU, not the SU.



Notes:

- One of the most important details to pay attention to in Routing mode are the unit's and the PC's default gateways. It is a common mistake to set up the PC's gateway to point to the SU when the SU is in Bridge mode and the BSU is in Routing mode. Always check to make sure the PCs on your network are configured to send their IP traffic to the correct default gateway.

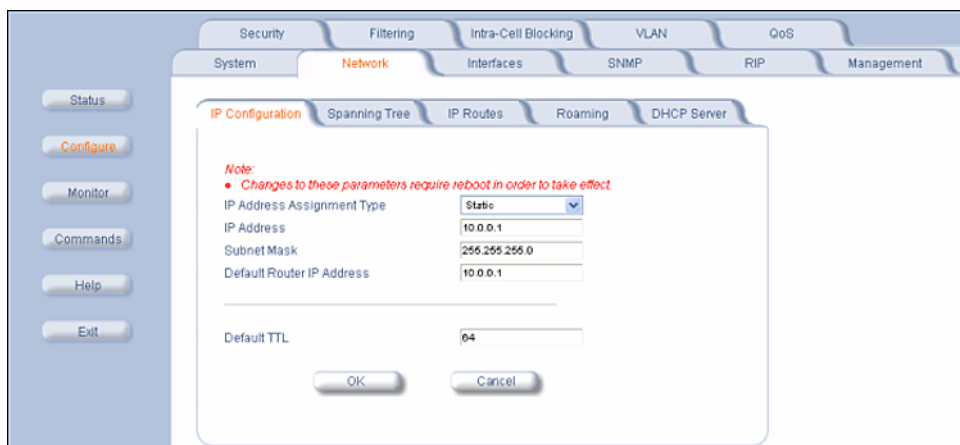
- Be sure to reboot the unit to permanently save static routes. New routes take effect immediately without a reboot, but are not permanently saved with your configuration until you do reboot the device. An unexpected power outage could cause static routes you entered to “disappear” when the unit reboots if they have not been saved. You also should save a copy of your unit’s configuration file in case the unit must be reloaded. This saves you from being required to re-enter numerous static routes in a large network.
- The routing table supports up to 500 static routes.

Network Parameters

Change IP Parameters

The IP Configuration window lets you change the IP parameters. These settings differ when the unit is in **Routing** mode.

Click **Configure > Network > IP Configuration** to view and configure local IP address information. See [Setting the IP Address with ScanTool](#) for more information.



If the device is configured in **Bridge** mode, you can set the **IP Address Assignment Type** parameter:

- Select **Static** if you want to assign a static IP address to the unit.
- Select **Dynamic** to have the device run in DHCP client mode, which gets an IP address automatically from a DHCP server over the network.

If you do not have a DHCP server or if you want to manually configure the IP settings, set this parameter to **Static**.

When the unit is in **Bridge** mode, only one IP address is required. This IP address also can be changed with ScanTool (see [Setting the IP Address with ScanTool](#)). In **Routing** mode, both Ethernet and Wireless interfaces require an IP address.

You can set the following remaining parameters only when the **IP Address Assignment Type** is set to **Static**.

- **IP Address:** The unit's static IP address (default IP address is 10.0.0.1).
- **Subnet Mask:** The mask of the subnet to which the unit is connected (the default subnet mask is 255.255.255.0).
- **Default Router IP Address:** The IP address of the default gateway.
- **Default TTL:** The default time-to-live value.

Configure Spanning Tree Options

This protocol is executed between the bridges to detect and logically remove redundant paths from the network. Spanning Tree can be used to prevent link-layer loops (broadcast is forwarded to all port where another device may forward it and, finally, it gets back to this unit; therefore, it is looping). Spanning Tree can also be used to create redundant links and operates by disabling links: hot standby customer is creating a redundant link without routing function.

If your network does not support Spanning Tree, be careful to avoid creating network loops between radios. For example, creating a WDS link between two units connected to the same Ethernet network creates a network loop (if spanning tree is disabled).

The Spanning Tree configuration options are advanced settings. Proxim recommends that you leave these parameters at their default values unless you are familiar with the Spanning Tree protocol.

Click the **Spanning Tree** tab to change Spanning Tree values.

Spanning Tree Status:

Bridge Priority:

Max Age (1/100 sec.):

Hello Time (1/100 sec.):

Forward Delay (1/100 sec.):

OK Cancel

Priority and Path Cost Table

Port	Priority	Path Cost	State	Status
1	128	100	Forwarding	Enable
2	128	100	Disabled	Enable
3	128	100	Disabled	Enable
4	128	100	Disabled	Enable
5	128	100	Disabled	Enable
6	128	100	Disabled	Enable
7	128	100	Disabled	Enable
8	128	100	Disabled	Enable
9	128	100	Disabled	Enable
10	128	100	Disabled	Enable
...				
246	128	100	Disabled	Enable
247	128	100	Disabled	Enable
248	128	100	Disabled	Enable
249	128	100	Disabled	Enable
250	128	100	Disabled	Enable
251	128	100	Disabled	Enable

Edit Table Entries

Click **Edit Table Entries** to make changes; enter your changes and click **OK**.

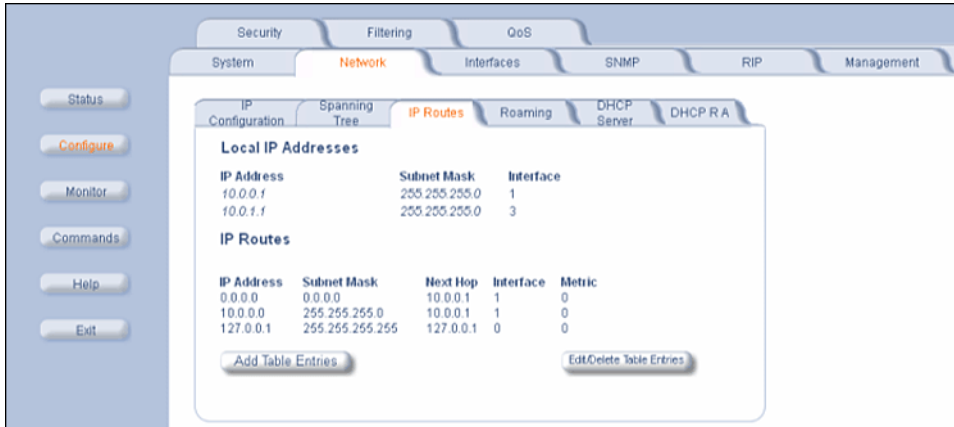
Port	Priority	Path Cost	Status
1	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
2	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
3	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
4	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
5	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
6	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
7	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
8	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
9	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
10	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
11	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
12	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
13	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
14	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
15	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
16	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
17	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
18	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
19	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
20	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
...			
248	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
249	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
250	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>
251	<input type="text" value="120"/>	<input type="text" value="100"/>	<input type="text" value="Enable"/>

NOTE: Changes made will only take effect after the device is rebooted.

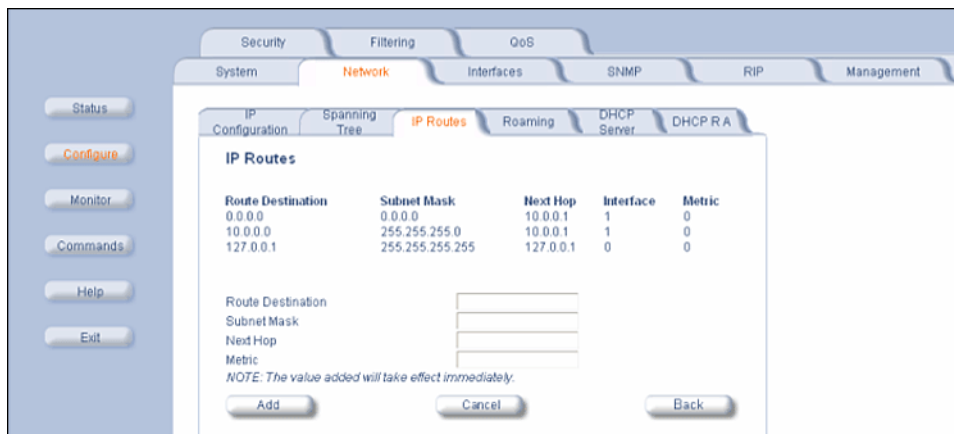
OK Cancel Back

Configure IP Routes (Routing Mode only)

Click **Configure > Network > IP Routes** to configure IP routes. You cannot configure IP Routes in **Bridge** mode. In **Routing** mode, the **Add Table Entries** and **Edit/Delete Table Entries** buttons are enabled.



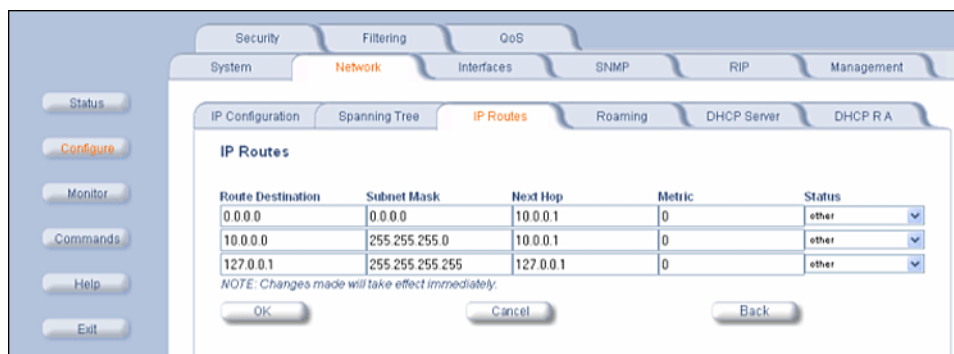
Click the **Add** button to add entries; a window such as the following is displayed:



Enter the route information and click **Add**. The **IP Address** and **Subnet Mask** combination is validated for a proper combination.

NOTE: When adding a new entry, the IP address of the Route Destination must be in either the Ethernet subnet or in the wireless subnet of the unit.

Click the **Edit/Delete Table Entries** button to make changes to or delete existing entries.



Edit the route information and click **OK**. The IP address and subnet mask combination is validated for a proper combination.

Enable or Disable Roaming

Roaming Overview

Roaming is a feature by which an SU terminates the session with the current BSU and starts the registration procedure with another BSU when it finds the quality of the other BSU to be better. Roaming provides MAC level connectivity to the SU that roams from one BSU to another. Roaming takes place across the range of frequencies and channel bandwidths (5, 10, or 20 MHz) that are available per configuration. The current release offers handoff times of up to a maximum of 80 ms. This is fast enough to allow the SU to seamlessly roam from one BSU to the other therefore supporting session persistence for delay-sensitive applications. The feature also functions as BSU backup in case the current BSU fails or becomes unavailable.

The Roaming feature lets the SU monitor local SNR and data rate for all frames received from the current BSU. As long as the average local SNR for the current BSU is greater than the slow scanning threshold, and the number of retransmitted frames is greater than the slow scanning threshold given in percentage, the SU does not scan other channels for a better BSU.

- The **normal scanning** procedure starts when the average local SNR for the current BSU is less than or equal to the slow scanning threshold and the number of retransmitted frames is greater than the slow scanning threshold given in percentage. During the normal scanning procedure the SU scans the whole list of active channels while maintaining the current session uninterrupted.
- **Fast scanning** is the scanning procedure performed when the average local SNR for the current BSU is very low (below the fast scanning threshold) and the number of retransmitted frames is greater than the fast scanning retransmission threshold given in%, so that the current session should terminate as soon as possible. During this procedure, the SU scans other active channels as fast as possible.

Roaming can only occur if the normal scanning or fast scanning procedure is started under the following conditions:

1. If the roaming is started from the normal scanning procedure (after the SU scans all the active channels), the SU selects the BSU with the best SNR value on all available channels. The SU roams to the best BSU only if the SNR value for the current BSU is still below the slow scanning SNR threshold, and best BSU offers a better SNR value for at least roaming threshold than the current BSU. The SU starts a new registration procedure with the best BSU without ending the current session.
2. If the roaming is started from the fast scanning procedure, the SU selects the first BSU that offers better SNR than the current BSU, and starts a new registration procedure with the better BSU without ending the current session.

Roaming with Dynamic Data Rate Selection (DDRS) Enabled

When an SU roams from BSU-1 to BSU-2 and DDRS is enabled, the data rate at which the SU connects to BSU-2 is the default DDRS data rate. If this remains at the factory default of 6 Mbps, there can be issues with the application if it requires more than 6 Mbps (for example multiple video streams).

Applications requiring a higher data rate could experience a slight data loss during the roaming process while DDRS selects a higher rate (based upon link conditions).

When the applications re-transmit at a possibly slower rate, the WORP protocol initially services the data at 6 Mbps and increases the data rate up to the "Maximum DDRS Data Rate" (*ddrsmaxdata rate*) one step at a time. Because the applications are not being serviced at the best possible rate, they further slow down the rate of data send.

The DDRS algorithm requires data traffic (a minimum of 128 frames) to raise the rate to a higher value. Although roaming occurs successfully, the previous scenario causes applications to drop their sessions; hence session persistence is not maintained.

For a discussion on how to configure DDRS, see [Dynamic Data Rate Selection \(DDRS\)](#).

NOTE: You must know the data rate required for the applications running and you must ensure (during network deployment) that the ranges and RF links can support the necessary data rate. You also must set the default DDRS data rate at the capacity necessary for the application so that it connects to the next Base Station at the required capacity if roaming occurs. Set the “Default DDRS Data Rate” (ddrsdefdatarate) to a greater value (24, 36, 48 or 54 Mbps, for example) for applications requiring session persistence when roaming occurs.

Configuring Roaming

Click **Configure > Network > Roaming** to configure Roaming. The screen differs depending on whether the unit is configured as a BSU or as an SU.

BSU Screen

Enable or disable the Roaming feature by selecting the **Enable Roaming Status** check box. The default value is disabled (clear). If you enable roaming, you may set the **Announcement Period** (from 25 to 100 ms, default is 100 ms).

On this screen you may also enable or disable the **Multi-Frame Bursting** (default value is enabled).

The screenshot shows the 'Roaming' configuration screen. At the top, there are tabs for 'Security', 'Filtering', and 'QoS'. Below that are 'System', 'Network', 'Interfaces', 'SNMP', 'RIP', and 'Management'. The 'Network' tab is selected, and within it, 'Roaming' is the active sub-tab. The 'Enable Roaming Status' checkbox is checked. The 'Announcement Period' is set to 100 ms, and 'Multi-Frame Bursting' is set to 'Enable'. A note states: 'Changes take effect immediately after clicking Ok Button.' Below the configuration options is an 'Auto Scanning Table' with the following data:

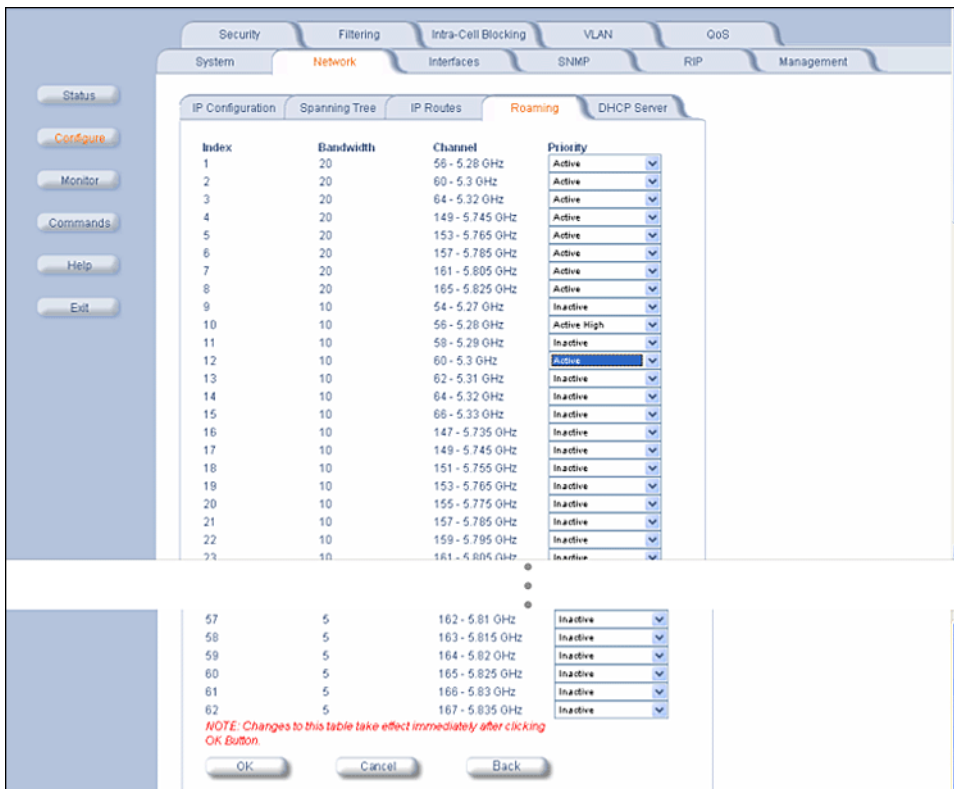
Index	Bandwidth	Channel	Priority
1	20	58 - 5.29 GHz	Active
2	20	60 - 5.3 GHz	Active
3	20	64 - 5.32 GHz	Active
4	20	149 - 5.745 GHz	Active
5	20	153 - 5.765 GHz	Active
6	20	157 - 5.785 GHz	Active
7	20	161 - 5.805 GHz	Active
8	20	165 - 5.825 GHz	Active
9	10	54 - 5.27 GHz	Inactive
10	10	58 - 5.29 GHz	Inactive
11	10	59 - 5.29 GHz	Inactive
12	10	60 - 5.3 GHz	Inactive
13	10	62 - 5.31 GHz	Inactive
		•	
		•	
		•	
57	5	162 - 5.81 GHz	Inactive
58	5	163 - 5.815 GHz	Inactive
59	5	164 - 5.82 GHz	Inactive
60	5	165 - 5.825 GHz	Inactive
61	5	166 - 5.83 GHz	Inactive
62	5	167 - 5.835 GHz	Inactive

An SU scans all available channels for a given bandwidth during roaming. In order to reduce the number of channels an SU has to scan and thus decrease the roaming time, a channel priority list that tells the SU what channels to scan is implemented. Each channel in the channel priority list is specified with its corresponding bandwidth and the priority with which it should be scanned, either “Active” (standard priority), “Active High” (high priority), or “Inactive”.

An SU will scan all channels indicated as “Active” during roaming. However, it will scan active channels indicated as “High Priority” before scanning active channels indicated as standard priority. Channels that are not going to be used in the wireless network should be configured as “Inactive” so that the SU can skip over those channels during scanning saving this way time.

A BSU broadcasts the channel priority list to all valid authenticated SUs in its sector. It re-broadcasts the channel priority list to all SUs every time the list is updated on the BSU.

Click **Edit Table Entries** to make changes; enter your changes and click **OK**.



Note that an SU may roam from one BSU with a bandwidth setting to another BSU with a different bandwidth setting. Since in this case more channels need to be scanned than with only one channel bandwidth setting, it is important that the channel priority list mentioned above is properly used to limit scanning time.

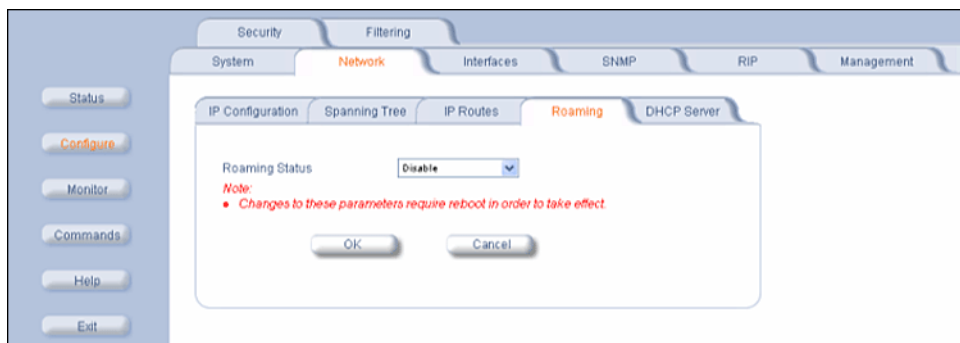
When **Scanning Across Bandwidth** on the SU is enabled (see [Interface Parameters](#)), the SU supports bandwidth selection of the communications channel of either 20 MHz, 10 MHz, or 5 MHz. This allows the BSUs in the network to be set to different bandwidths while an SU can still roam from one BSU to the next, because it will not only scan other frequencies (when the signal level or quality are lower than the threshold) but it will also switch to other bandwidths to find a BSU that may be on another bandwidth than its current one.

During roaming, the SU will start scanning first the channels on its *current* bandwidth from the “Active” channel list provided by the BSU in order to find a BSU to register, since that is the most likely setting for other BSUs in the network. If the SU cannot find an acceptable roaming candidate, it will switch bandwidth and start scanning channels on that corresponding bandwidth from the “Active” channel list provided by the BSU. The process is repeated until the SU finds an appropriate BSU to register.

In the example above, an SU whose current bandwidth is 20 MHz will start scanning all active channels within the bandwidth of 20 MHz. If it cannot find a suitable BSU, it will switch to a 10 MHz bandwidth and start scanning all active channels within that bandwidth, in this case channel 56 first since it is configured as high priority and channel 60 next. No channels will be scanned on the 5 MHz bandwidth since all those channels are configured as inactive.

SU Screen

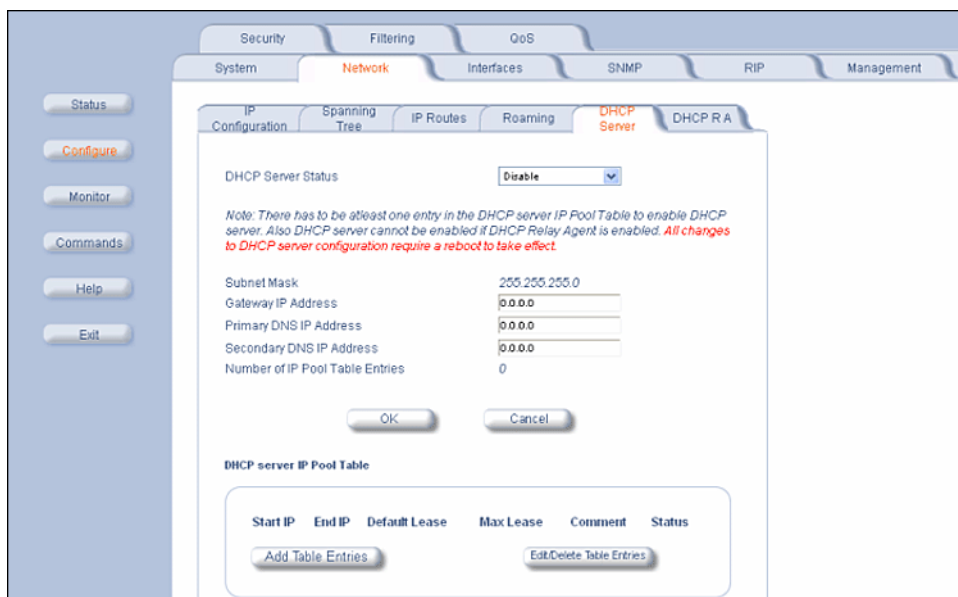
Enable or disable the Roaming feature in the **Roaming Status** drop-down box. The default value is disabled.



NOTE: To enable roaming, you must enable **Roaming Status** on both the BSU and the SU.

Enable and Configure the DHCP Server

Click **Configure > Network > DHCP Server** to enable the unit on a DHCP Server. The **Gateway IP Address** and **Primary DNS IP Address** must be entered, there must be at least one entry in the DHCP Server IP Pool Table, and the DHCP Relay Agent must be disabled, in order to enable the DHCP Server.



When enabled, the DHCP server allows allocation of IP addresses to hosts on the Ethernet side of the SU or BSU. Specifically, the DHCP Server feature lets the SU or BSU respond to DHCP requests from Ethernet hosts with the following information:

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

The following parameters are configurable:

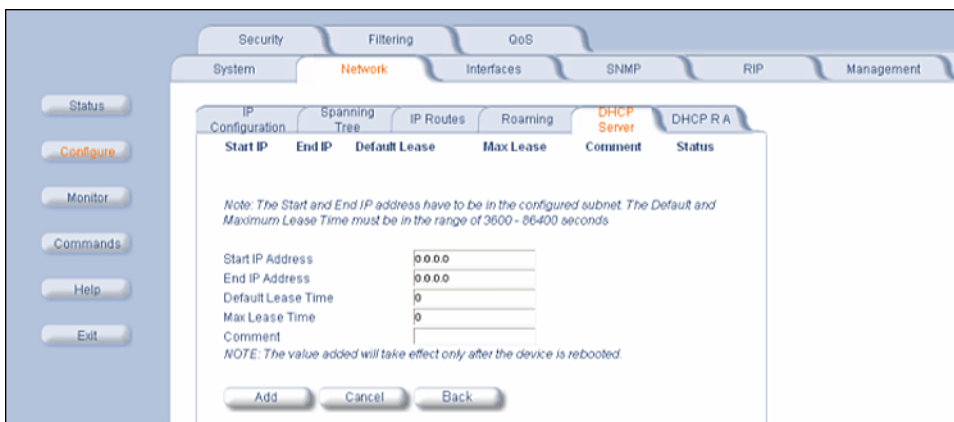
- **DHCP Server Status:** Verify that DHCP Relay Agent is disabled. After you have made at least one entry in the DHCP server IP Pool Table, enable DHCP Server by selecting “Enable” from the **DHCP Server Status** pull-down menu.

NOTE: There must be at least one entry in the DHCP server IP Pool Table to enable DHCP server. Also, DHCP server cannot be enabled if DHCP Relay Agent is enabled.

- **Subnet Mask:** The unit supplies this subnet mask in its DHCP response to a DHCP request from an Ethernet host. Indicates the IP subnet mask assigned to hosts on the Ethernet side using DHCP.
- **Gateway IP Address:** The unit supplies this gateway IP address in the DHCP response. Indicates the IP address of a router assigned as the default gateway for hosts on the Ethernet side.
- **Primary DNS IP Address:** The unit supplies this primary DNS IP address in the DHCP response. Indicates the IP address of the primary DNS server that hosts on the Ethernet side uses to resolve Internet host names to IP addresses
- **Secondary DNS IP Address:** The unit supplies this secondary DNS IP address in the DHCP response.
- **Number of IP Pool Table Entries:** The number of IP pool table entries is a read-only field that indicates the total number of entries in the DHCP server IP Pool Table. See [Add Entries to the DHCP Server IP Pool Table](#).

Add Entries to the DHCP Server IP Pool Table

You can add up to 20 entries in the IP Pool Table. An IP address can be added if the entry's network ID is the same as the network ID of the device. To add an entry click **Add Table Entries**.



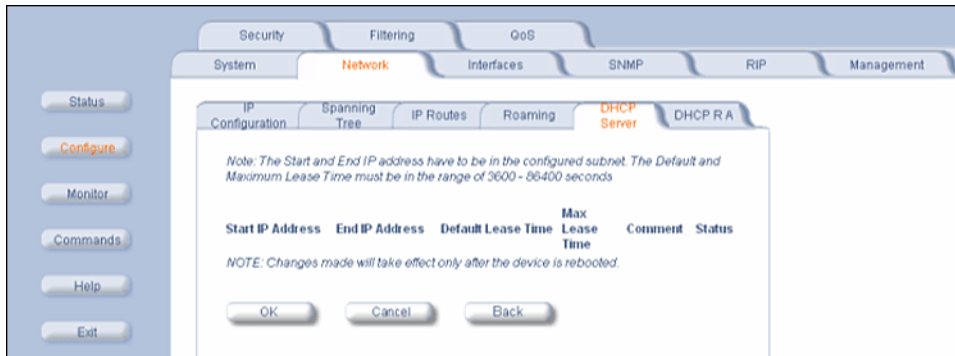
Enter the following parameters and click **Add**:

NOTE: After adding entries, you must reboot the unit before the values take effect.

- **Start IP Address:** Indicates the starting IP address that is used for assigning address to hosts on the Ethernet side in the configured subnet.
- **End IP Address:** Indicates the ending IP address that is used for assigning address to hosts on the Ethernet side in the configured subnet.
- **Default Lease Time:** Specifies the default lease time for IP addresses in the address pool. The value is 3600-86400 seconds.
- **Max Lease Time:** The maximum lease time for IP addresses in the address pool. The value is 3600-86400 seconds.
- **Comment:** The comment field is a descriptive field of up to 255 characters.

Edit/Delete Entries to the DHCP Server IP Pool Table Entries

Click **Edit/Delete Table Entries** to make changes; enter your changes and click **OK**.



Enable the DHCP Relay Agent (Routing Mode Only)

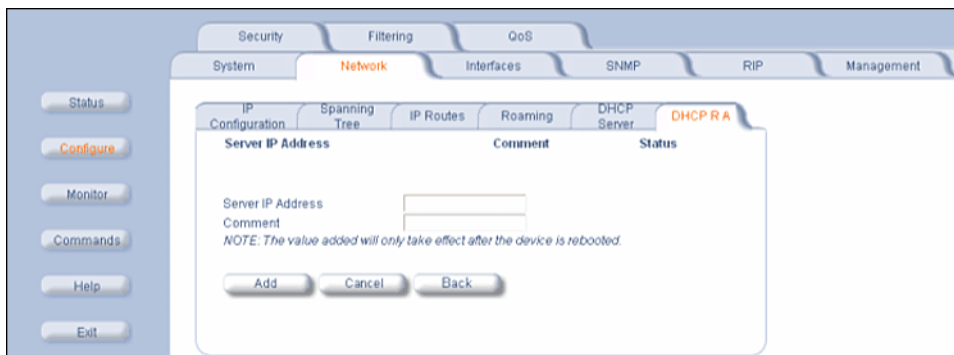
Click **Configure** > **Network** > **DHCP RA** to enable the unit's DHCP Relay Agent. When enabled, the DHCP relay agent forwards DHCP requests to the set DHCP server. There must be at least one entry in the corresponding Server IP Address table in order to enable the DHCP Relay Agent.

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



Add Entries to the DHCP Relay Agent Table

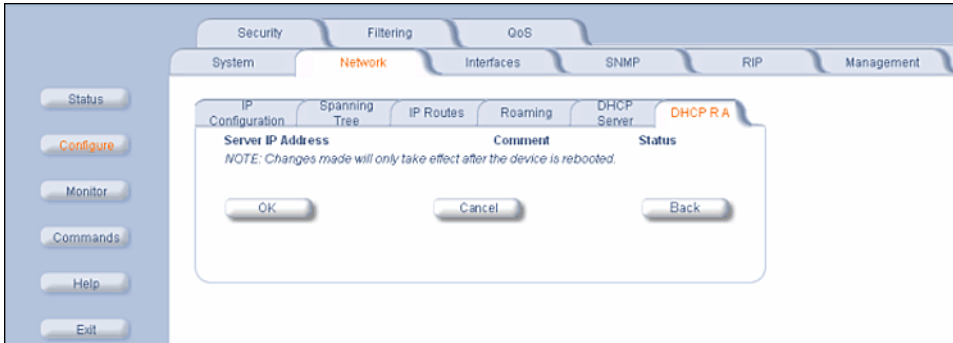
To add entries to the table of DHCP Relay Agents, click **Add Table Entries**; the following window is displayed:



Enter the **Server IP Address** and any optional comments; click **Add**.

Edit/Delete Entries to the DHCP Relay Agent Table

Click **Edit/Delete Table Entries** to make changes; enter your changes and click **OK**.



Interface Parameters

Configure the Wireless Interface

To configure the wireless interface, click **Configure > Interfaces > Wireless**.

For Base Station units, the wireless interface can be placed in either WORP Base or WORP Satellite mode (selected from the **Interface Type** drop-down box). SUs can be placed only in WORP Satellite mode. The wireless interface settings depend upon whether the mode is Base or Satellite.

The Wireless Outdoor Router Protocol (WORP) is a polling algorithm designed for wireless outdoor networks. WORP takes care of the performance degradation incurred by the so-called “hidden-node” problem, which can occur when wireless LAN technology is used for outdoor building-to-building connectivity. In this situation, when multiple radios send an RTS, if another radio is transmitting, it corrupts all data being sent, degrading overall performance. The WORP polling algorithm ensures that these collisions cannot occur, which increases the performance of the overall network significantly.

WORP dynamically adapts to the number of SUs that are active on the network and the amount of data they have queued to send.

The following are examples of the Wireless window when the country selected is US:

Base Mode

The following parameters may be configured or viewed:

- **Interface Type:** The interface type can be **WORP Satellite** or **WORP Base**.

- **MAC Address:** The factory-assigned MAC address of the unit. This is a read-only field.
- **Network Name:** A Network Name is a name given to a network so that multiple networks can reuse the same frequency without problems. An SU can only register to its base if it has the same Network Name. The Network Name is one of the parameters that allow a Subscriber Unit to register on a Base Station. The **Base Station System Name** and **Frequency Channel** also are parameters to guide the SU to the proper BSU on the network, but they provide no security. Basic security is provided through encryption, as it causes none of the messages to be sent in the clear. Further security is provided by mutual authentication of the BSU and SU using the **Network Secret**. The Network Name can be 2 to 32 characters in length.
- **Operational Mode:** This field indicates the operational mode of the unit – 4.9 GHz, 11a, 11b, or 11g – depending upon the specific Tsunami MP.11. This operational mode cannot be changed as it is based upon a license file.
- **Dynamic Data Rate Selection (DDRS) Status:** The **DDRS Status** is configurable only for the **WORP Base Mode**. For **WORP Base Mode**, select the **DDRS Status** “Enable” or “Disable” from the drop-down box provided.
For the **WORP Satellite Mode**, **DDRS Status** is read-only parameter and its value is based upon the **WORP Base** to which this SU is associated.

When you enable or disable DDRS on the BSU, the BSU sends an announcement to the SUs and the SUs enable or disable DDRS automatically.

- **Transmit Power Control (TPC):** By default, the unit lets you transmit at the maximum output power for the country or regulatory domain and frequency selected. However, with Transmit Power Control (TPC), you can adjust the output power of the unit to a lower level in order to reduce interference to neighboring devices or to use a higher gain antenna without violating the maximum radiated output power allowed for your country. Also, most countries in the ETSI regulatory domain require the transmit power to be set to a 6 dB lower value than the maximum allowed EIRP when link quality permits. You can see your unit’s current output power for the selected frequency in the event log. The event log shows the selected power for all data rates, so you must look up the proper data rate to determine the actual power level.

NOTE: This feature only lets you decrease your output power; it does not let you increase your output power beyond the maximum allowed defaults for your frequency and country.

Select one of the following options and click **OK** at the bottom of the window. Your original output power is adjusted relative to the value selected. The new setting takes effect immediately without rebooting:

TPC Selection (dB)	Maximum TX Power (dBm)
0 (default)	16
-3	13
-6	10
-9	7
-12	4
-15	1
-18 (minimum TPC level)	0

NOTE: 24 Mbps and lower modulation have maximum +16 dBm TX power, 36 Mbps has maximum +13 dBm TX power, 48 Mbps has maximum +12 dBm TX power, and 54 Mbps has maximum +11 dBm TX power. Because higher modulation has a lower maximum TX power, the total TPC range is smaller at a higher data rate. Because the minimum TX power is equal for all data rates, each TPC selection has constant TX power for all data rates except where the maximum TX power is limited.

- **Enable Turbo Mode:** Check this box to enable Turbo Mode. Turbo Mode is supported only in the United States, and only for the 4954-R.
Enabling turbo mode, in its current implementation, allows the unit to use two adjacent frequency channels to transmit and receive a signal. By enabling turbo mode, the receive sensitivity improves by 4 dB for the 36 Mbps data rate and by 2 dB for the 24 Mbps data rate.

NOTE: The additional sensitivity is provided with the impact of using twice as much spectrum and thus increasing the opportunity of interference and decreased ability for system collocation. Generally, Turbo mode is not recommended except when the extra sensitivity is absolutely required.

- **Frequency Channel:** The frequency channel indicates the band center frequency the unit uses for communicating with peers. This frequency channel can be set in several ranges, depending upon regulatory domain. Refer to [Frequency Bands and Channels](#) for channelization information.
- **Multicast Rate:** The rate at which data is to be transferred. This drop down box is unavailable when DDRS is enabled.

The default multicast rate for the unit is 36 Mbps. The SU must never be set to a lower data rate than the BSU because timeouts will occur at the BSU and communication will fail.

Selections for multicast rate for 5, 10 and 20 MHz channel bandwidths are shown in the following table:

Multicast Rates in Mbps			
5 MHz	10 MHz	20 MHz	Turbo Enabled* (40 MHz)
1.5	3	6	12
2.25	4,5	9	18
3	6	12	24
4.5	9	18	36
6	12	24	48
9	18	36	72
12	24	48	96 [†]
13.5	27	54	108 [†]

* Turbo Mode is available in the US only.

[†] If you select 48 or 54 Mbps (96 or 108 in Turbo mode) DDRS is automatically turned on (enabled).

- **Channel Bandwidth:** Select 5 MHz, 10 MHz or 20 MHz channel bandwidth.
- **Antenna Gain (BSU only):** You can modify the sensitivity of the radio card when detecting radar signals in accordance with ETSI and FCC Dynamic Frequency Selection (DFS) requirements. Given the radar detection threshold is fixed by ETSI and the FCC and that a variety of antennas with different gains may be attached to the unit, you must adjust this threshold to account for higher than expected antenna gains and avoid false radar detection events. This can result in the units constantly changing frequency channels.

You can 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 35. The default value is 0.

- **Satellite Density:** The **Satellite Density** setting is a valuable feature for achieving maximum bandwidth in a wireless network. It influences the receive sensitivity of the radio interface and improves operation in environments with a high noise level. Reducing the sensitivity of the unit enables unwanted “noise” to be filtered out (it disappears under the threshold).

You can configure the **Satellite Density** to be **Large**, **Medium**, **Small**, **Mini**, or **Micro**. The default value for this setting is Large. The smaller settings are appropriate for high noise environments; a setting of **Large** would be for a low noise environment.

A long distance link may have difficulty maintaining a connection with a small density setting because the wanted signal can disappear under the threshold. Consider both noise level and distance between the peers in a link when configuring this setting. The threshold should be chosen higher than the noise level, but sufficiently below the signal level. A safe value is 10 dB below the present signal strength.

If the Signal-to-Noise Ratio (SNR) is not sufficient, you may need to set a lower data rate or use antennas with higher gain to increase the margin between wanted and unwanted signals. In a point-to-multipoint configuration, the BSU should have a density setting suitable for all of its registered SUs, especially the ones with the lowest signal levels (longest links).

Take care when configuring a remote interface; check the available signal level first, using Remote Link Test.

WARNING: *When the remote interface accidentally is set at too small a value and communication is lost, it cannot be reconfigured remotely and a local action is required to bring the communication back. Therefore, the best place to experiment with the level is at the unit 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.*

To set the **Satellite Density**, click the **Configure** button, then the **Interfaces** tab and the **Wireless** sub-tab. Make your density selection from the drop-down menu. This setting requires a reboot of the unit.

Sensitivity threshold settings related to the density settings for the unit are:

Set Satellite Density to:	For a Receive Sensitivity Threshold of:	And a Defer Threshold of:
Large	-95 dBm	-62 dBm
Medium	-86 dBm	-62 dBm
Small	-78 dBm	-52 dBm
Mini	-70 dBm	-42 dBm
Micro	-62 dBm	-36 dBm

- **Maximum Satellites (BSU only):** You can specify a maximum value of 250 in this field, because up to 250 SUs can be connected to a BSU. If a BSU already has as many SUs as specified in this field, a new SU cannot connect to the BSU.
- **No-Sleep Mode (BSU only):** No-Sleep Mode was a feature used to control jitter in Tsunami MP.11 products running 2.2.6, and earlier, versions of software. The introduction of QoS and the new WORP resource scheduling mechanism have eliminated the need for No-Sleep Mode. Furthermore, QoS provides better control over jitter and latency-sensitive applications (see [QoS \(Quality of Service\) Parameters](#) for details on configuration). This field is inactive and makes no difference whether is enabled or disabled.
- **Automatic Multi-Frame Bursting (BSU only):** In order to achieve higher throughput, WORP protocol allows each side (BSU or SU) to send a burst of up to 4 data messages instead of a single data message. The sole criteria for sending a burst is enough traffic to be sent out. This feature is called Multi-Frame Bursting support.

Automatic Multi-Frame bursting optimizes multi-burst performance when configuring QoS high-priority Service Flows. Three scenarios may be defined:

- **No Multi-Frame Burst Support** –To disable Multi-Frame burst support, click **Configure > Network > Roaming**, and select “Disable” on the drop-down box (see [BSU Screen](#)). In this case, each active SFC is limited to send a single data message. Total throughput available to remaining best effort traffic is around 76% of the maximum available throughput.

Multi-Frame Burst Support – The system will enable Multi-Frame burst for *all* SFCs, but the maximum number of data messages sent in a burst will be defined by the parameter “Number of data messages in a burst” for each of the SFCs (see [Service Flow Class \(SFC\)](#)). This scenario is set by clicking **Configure > Network > Roaming** and enabling Multi-Frame burst on the drop-down box (see [BSU Screen](#)), and disabling **Automatic Multi-Frame Bursting** (this parameter).

The maximum number of data messages in a burst directly influences the total throughput of the system. Typical values are:

No. of messages in a burst:	% of the maximum throughput:
4	100%
3	97.6%
2	92.9%
1	76.2%

- **Automatic Multi-Frame Burst Support** – The system will continuously be monitoring which of the active SFCs has the highest priority and dynamically enable Multi-Frame burst for the highest priority SFC only, keeping all the lower priority SFCs with Multi-Frame burst disabled. If there are multiple SFCs having the same, highest priority, all of them will have Multi-Frame burst enabled. The maximum number of data messages sent in a burst is defined by the parameter “Number of data messages in a burst” and it can be different for each SFC (see [Service Flow Class \(SFC\)](#)). This scenario is set by clicking **Configure > Network > Roaming** and enabling Multi-Frame burst on the drop-down box (see [BSU Screen](#)), and enabling **Automatic Multi-Frame Bursting** (this parameter). In this case, even the lowest priority SFC will have Multi-Frame burst dynamically enabled as long as it is the only SFC in the system that has traffic. By default, configuring even a single high priority SFC with automatic multi-frame bursting enabled will decrease throughput of low priority best-effort traffic to approximately 76% of maximum available throughput, because low priority traffic will have Multi-Frame burst disabled to optimize bandwidth for the high priority traffic.
- **Registration Timeout:** This is the registration process time-out of an SU on a BSU. Default is 5 seconds.
- **Network Secret:** A network secret is a secret password given to all nodes of a network. An SU can only register to a BSU if it has the same Network Secret. The Network Secret is sent encrypted and can be used as a security option.
- **Input / Output Bandwidth Limit:** These parameters limit the data traffic received on the wireless interface and transmitted to the wireless interface, respectively. Selections are in steps of 64 Kbps from 64 Kbps to 108,064 Kbps.

Satellite Mode

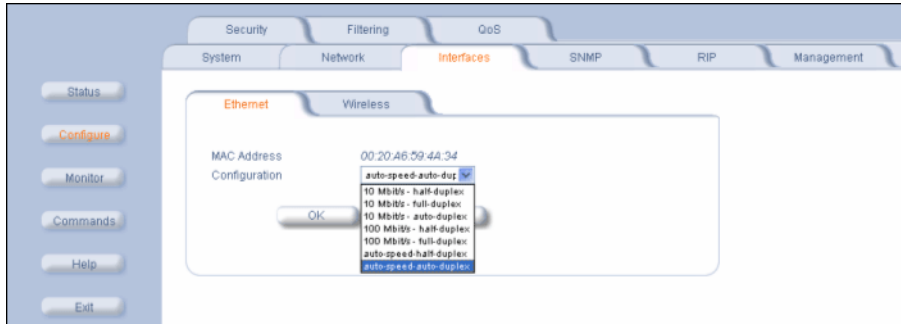
The screenshot displays a configuration window for a wireless interface. The 'Wireless' tab is active, showing various parameters. The 'Interface Type' is set to 'Worq Satellite'. The 'MAC Address' is '00:30:F1:E8:82:96'. The 'Base Station System Name' field is empty, with a note below it stating: 'Note: Base Station System Name is the System Name found on the system page of the Base Station this satellite is connecting to, if blank satellite can connect to any Base Station'. Other settings include 'Operational Mode' (802.11a), 'Network Name' (DR_WORP), 'Dynamic Data Rate Selection (DDRS) Status' (Disabled), 'Transmit Power Control (TPC)' (-0 dB), 'Enable Turbo Mode' (unchecked), 'Frequency Channel' (140 - 5.745 GHz), 'Scanning Across Bandwidth' (Enable), 'Multicast Rate' (30 Mbps), 'Channel Bandwidth' (20 MHz), 'Satellite Density' (Large), 'RegistrationTimeout' (5), 'Network Secret' (*****), 'Input bandwidth limit (in kbits/s)' (108032), and 'Output bandwidth limit (in kbits/s)' (108032). There are 'OK' and 'Cancel' buttons at the bottom.

All the fields that are common to both the BSU and the SU are applicable here. The SU features two additional fields:

- **Base Station System Name (SU only):** The name found on the system page of the BSU to which this SU is connecting. This parameter can be used as an added security measure, and when there are multiple BSUs in the network and you want an SU to register with only one when it may actually have adequate signal strength for either. The System Name field is limited to a length of 32 bytes.
If the Base Station System Name is left blank on the SU, it can register with any BSU with a matching Network Name and Network Secret.
- **Scanning Across Bandwidth (SU only):** Enable this field if you want the SU to scan across the whole range of channel bandwidths (5, 10, or 20 MHz) with or without roaming enabled. Disable this field if you wish the SU to scan only across its configured channel bandwidth.

Configure the Ethernet Interface

To set the Ethernet speed, duplex mode, and input and output bandwidth limits, click **Configure** > **Interfaces** > **Ethernet**.



You can set the desired speed and transmission mode by clicking on **Configuration**. Select from these settings for the type of Ethernet transmission:

- **Half-duplex** means that only one side can transmit at a time.
- **Full-duplex** lets both sides transmit.
- **Auto-duplex** selects the best transmission mode available when both sides are set to auto-select.

The recommended setting is **auto-speed-auto-duplex**.

SNMP Parameters

Click **Configure** > **SNMP** to enable or disable trap groups, and to configure the SNMP management stations to which the unit sends system traps. See “Trap Groups” in the *Tsunami MP.11 Reference Manual* for a list of the system traps.

The screenshot shows the SNMP configuration page. At the top, there are tabs for Security, Filtering, Intra-Cell Blocking, VLAN, OoS, System, Network, Interfaces, SNMP (selected), RIP, and Management. On the left, there is a sidebar with buttons: Status, Configure, Monitor, Commands, Help, and Exit. The main content area is titled "Trap Groups" and contains six rows of trap status settings, each with a dropdown menu set to "Enable": Configuration Trap Status, Security Trap Status, Wireless Interface Trap Status, Operational Trap Status, Flash Memory Trap Status, and TFTP Trap Status. Below these is an "Image Trap Status" dropdown also set to "Enable". There are "OK" and "Cancel" buttons. Below that is a "Trap Host Table" section with a table header: IP Address, Password, Comment, Status. Below the header are two buttons: "Add Table Entries" and "Edit/Delete Table Entries".

- **Trap Groups:** You can enable or disable different types of traps in the system. By default, all traps are enabled.
- **Trap Host Table:** This table shows the SNMP management stations to which the unit sends system traps.

Add Entries to the Trap Host Table

Click the **Add Table Entries** button to add entries to the Trap Host Table.

The screenshot shows the "Add Table Entries" form. It has the same top navigation and sidebar as the previous screenshot. The main content area has a table header: IP Address, Password, Comment, Status. Below the header are four input fields: "IP Address", "Password", "Password Confirm", and "Comment". At the bottom of the form are three buttons: "Add", "Cancel", and "Back".

Edit/Delete Entries to the Trap Host Table

Click the **Edit/Delete Table Entries** button to make changes to or delete existing entries.

The image shows a web-based configuration interface for SNMP parameters. The interface has a top navigation bar with tabs for Security, Filtering, Intra-Cell Blocking, VLAN, and QoS. Below this is a sub-navigation bar with tabs for System, Network, Interfaces, SNMP (highlighted in orange), RIP, and Management. On the left side, there is a vertical menu with buttons for Status, Configure (highlighted in orange), Monitor, Commands, Help, and Exit. The main content area contains five columns: IP Address, Password, Confirm, Comment, and Status. Below the IP Address and Status columns are buttons labeled OK and Back, respectively. Below the Confirm column is a button labeled Cancel.

RIP Parameters

Routing Internet Protocol (RIP) is a dynamic routing protocol you can use to help automatically propagate routing table information between routers. The unit can be configured as RIPv1, RIPv2, RIPv1 Compatible, or a combination of the three versions while operating in **Routing** mode. In general, the unit's RIP module is based upon RFC 1389.

NOTE: RIP does not work when Network Address Translation (NAT) is enabled.

The screenshot shows a configuration window for RIP parameters. It has a sidebar on the left with buttons for Status, Configure, Monitor, Commands, Help, and Exit. The main area has tabs for Security, Filtering, QoS, System, Network, Interfaces, SNMP, RIP, and Management. The RIP tab is active, showing configuration for two interfaces: Ethernet and Wireless-slot A. The configuration includes fields for Address, Network Mask, Authentication Type (set to No Authentication), Authentication Key, Confirm Authentication Key, Enable RIP Interface (checked), Advertize (set to Do Not Send), and Receive (set to RIPv2). A note at the bottom states: "NOTE: Changes take effect immediately after clicking OK Button. Authentication Key should be in Hexadecimal." There are OK and Cancel buttons at the bottom.

Note the following:

- RIPv2 is enabled by default when routing mode is selected.
- You may turn RIP off by clearing the **Enable RIP Interface** check box for the Ethernet or the wireless interface. Any RIP advertisements that are received on the designated interface are ignored. All other options on the page are dimmed.
- If the Enable RIP Interface check box is selected, the unit sends RIP requests and “listens” for RIP updates coming from RIP-enabled devices advertising on the network. You may configure the Receive field for RIPv1, RIPv2, or a combination of both. Although the unit receives and processes these updates, it does not further propagate these updates unless configured to advertise RIP. Again, you may configure the **Advertize** field for RIPv1, RIPv2, or a combination of both.
- The ability to enable or disable default route propagation is not user configurable. Once initialized, the unit uses its static default route and does not advertise this route in RIP updates. If another router on your network is configured to advertise its default route, this route overwrites the static default route configured on the unit. The unit then also propagates the new dynamic default route throughout the network.

Be aware that, once a dynamic default route is learned, it behaves just as any other dynamic route learned through RIP. This means if the device sending the default route stops sending RIP updates, the default route times out and the unit has no default route to the network. Workarounds for this condition include rebooting or re-entering a static default route. In general, the best approach is to disable the propagation of default routes on the other routers in your network unless you understand the risks.

The following table describes the properties and features of each version of RIP supported.

Properties and Features of Supported RIP Versions		
RIPv1	RIPv2	RIPv1 Compatible
Broadcast	Multicast	Broadcast
No Authentication	Authentication	Authentication
Class routing	Classless routing (VLSM)	Classless routing (VLSM)
Distance-vector protocol	Distance-vector protocol	Distance-vector protocol

Properties and Features of Supported RIP Versions		
RIPv1	RIPv2	RIPv1 Compatible
Metric-Hops	Metric-Hops	Metric-Hops
Maximum Distance 15	Maximum Distance 15	Maximum Distance 15
IGP	IGP	IGP

RIP Example

In the following example, assume that both the BSU and the SUs all are configured in **Routing** mode with RIP enabled to send and receive on both the Ethernet and Wireless interfaces. The network converges through updates until each unit has the following routing table:

BSU

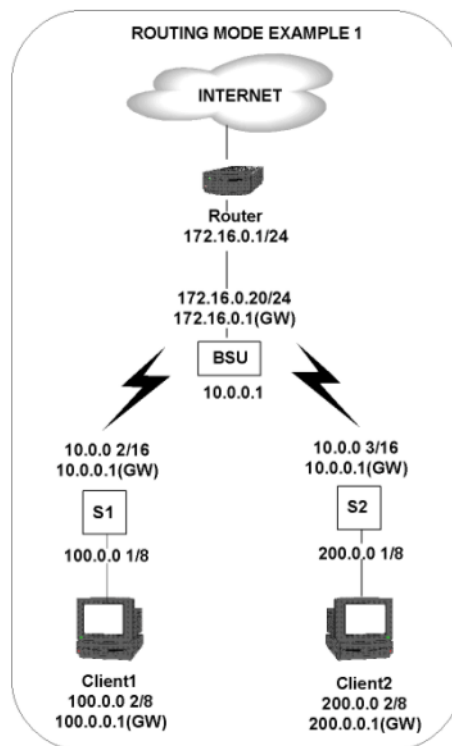
```
0.0.0.0      172.16.0.1    metric 1
172.16.0.0  172.16.0.20  metric 1
10.0.0.0    10.0.0.1     metric 1
100.0.0.0   10.0.0.2     metric 2
200.0.0.0   10.0.0.3     metric 2
```

SU1

```
0.0.0.0      10.0.0.1     metric 1
10.0.0.0    10.0.0.2     metric 1
100.0.0.0   100.0.0.1    metric 1
172.16.0.0  10.0.0.1     metric 2
200.0.0.0   10.0.0.2     metric 2
```

SU2

```
0.0.0.0      10.0.0.1     metric 1
10.0.0.0    10.0.0.3     metric 1
200.0.0.0   200.0.0.1    metric 1
172.16.0.0  10.0.0.1     metric 2
100.0.0.0   10.0.0.2     metric 2
```



RIP Notes

- Ensure that routers on the same physical network are configured to use the same version of RIP.
- Routing updates occur every 30 seconds. It may take up to 3 minutes for a route that has gone down to timeout in a routing table.
- RIP is limited to networks with 15 or fewer hops.

Management Parameters

When you click the **Management** button, Passwords is displayed automatically. The other tab under **Management** is the **Services** tab.

Configure Passwords

The **Password** tab lets you configure the SNMP, Telnet, and HTTP (Web Interface) passwords.

The screenshot shows a web interface for configuring passwords. At the top, there are tabs for Security, Filtering, Intra-Cell Blocking, VLAN, QoS, System, Network, Interfaces, SNMP, RIP, and Management. The Management tab is selected. Below the tabs, there are two sub-tabs: Passwords and Services. The Passwords tab is active. The main content area contains the following text and fields:

This tab is used to configure SHMPv1 v2c community, Telnet (CLI) and HTTP (web) passwords.

Change the default passwords to a value known only to you. If this is not done, then users may be able to manage the device and modify its configuration without your knowledge.

Note: Changes to Passwords must be between 6 and 32 characters. Changes will take effect immediately after clicking OK Button.

SNMP Read Community Password: [Password field] Confirm: [Confirm field]

SNMP Read/Write Community Password: [Password field] Confirm: [Confirm field]

Telnet (CLI) Password: [Password field] Confirm: [Confirm field]

HTTP (web) Password: [Password field] Confirm: [Confirm field]

At the bottom, there are OK and Cancel buttons.

For all password fields, the passwords must be between 6 and 32 characters. Changes take effect immediately after you click **OK**. The following passwords are configurable:

- **SNMP Read Community Password:** The password for read access using SNMP. Enter a password in both the **Password** field and the **Confirm** field. The default password is **public**.
- **SNMP Read/Write Community Password:** The password for read and write access using SNMP. Enter a password in both the **Password** field and the **Confirm** field. The default password is **public**.
- **Telnet (CLI) Password:** The password for the CLI interface. Enter a password in both the **Password** field and the **Confirm** field. The default password is **public**.
- **HTTP (Web) Password:** The password for the Web browser HTTP interface. Enter a password in both the **Password** field and the **Confirm** field. The default password is **public**.

Configure Service Parameters

The **Services** tab lets you configure the SNMP, Telnet, and HTTP (Web Interface) parameters. Changes to these parameters require a reboot to take effect.



SNMP Configuration Settings

- **SNMP Interface Bitmask:** Configure the interface or interfaces (**Ethernet, Wireless, All Interfaces**) from which you will manage the unit using SNMP. You also can select **Disabled** to prevent a user from accessing the unit through SNMP.

HTTP Configuration Settings

- **HTTP Interface Bitmask:** Configure the interface or interfaces (**Ethernet, Wireless, All Interfaces**) from which you will manage the unit through the Web interface. For example, to allow Web configuration through the Ethernet network only, set **HTTP Interface Bitmask** to **Ethernet**. You can also select **Disabled** to prevent a user from accessing the unit from the Web interface.
- **HTTP Port:** Configure the HTTP port from which you will manage the unit through the Web interface. By default, the HTTP port is 80.

Telnet Configuration Settings

NOTE: To use HyperTerminal for CLI access, make sure to check “Send line ends with line feeds” in the ASCII Setup window (in the HyperTerminal window, click Properties; then select Setup > ASCII Setup. See “HyperTerminal Connection Properties” in the Tsunami MP.11 Reference Manual for more information).

- **Telnet Interface Bitmask:** Select the interface (Ethernet, Wireless, All Interfaces) from which you can manage the unit through telnet. This parameter can also be used to disable telnet management.
- **Telnet Port Number:** The default port number for Telnet applications is 23. However, you can use this field if you want to change the Telnet port for security reasons (but your Telnet application also must support the new port number you select).
- **Telnet Login Timeout (seconds):** Enter the number of seconds the system is to wait for a login attempt. The unit terminates the session when it times out. The range is 1 to 300 seconds; the default is 30 seconds.
- **Telnet Session Timeout (seconds):** Enter the number of seconds the system is to wait during a session while there is no activity. The unit ends the session upon timeout. The range is 1 to 36000 seconds; the default is 900 seconds.

Serial Configuration Settings

The serial port interface on the unit is enabled at all times. See “Serial Port” in the *Tsunami MP.11 Reference Manual* for information about how to access the CLI interface through the serial port. You can configure and view following parameters:

- **Serial Baud Rate:** Select the serial port speed (bits per second). Choose between 2400, 4800, 9600, 19200, 38400, or 57600; the default Baud Rate is 9600.
- **Serial Flow Control:** Select either None (default) or Xon/Xoff (software controlled) data flow control. To avoid potential problems when communicating with the unit through the serial port, Proxim recommends that you leave the Flow Control setting at None (the default value).
- **Serial Data Bits:** This is a read-only field and displays the number of data bits used in serial communication (8 data bits by default).
- **Serial Parity:** This is a read-only field and displays the number of parity bits used in serial communication (no parity bits by default).
- **Serial Stop Bits:** This is a read-only field that displays the number of stop bits used in serial communication (1 stop bit by default).

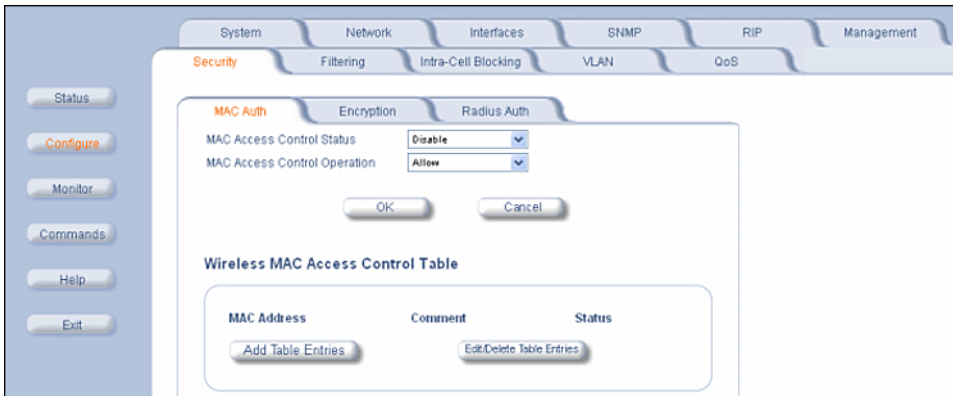
The serial port bit configuration is commonly referred to as 8N1.

Security Parameters

Configure MAC Authentication

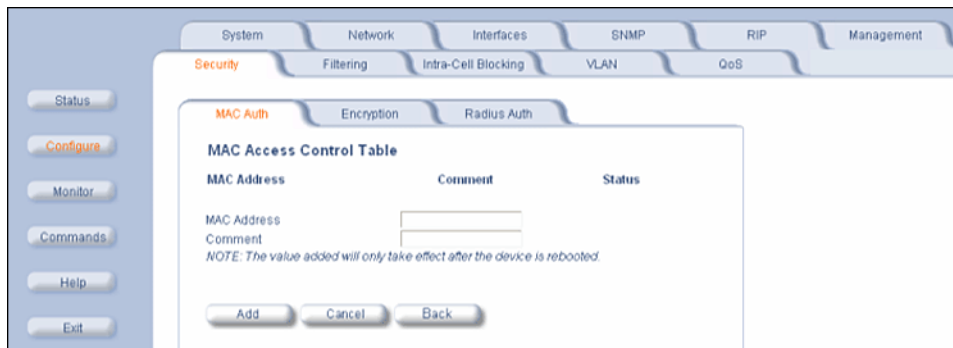
Click **Configure** > **Security** > **MAC Auth** to build a list of authorized wireless stations that can register at the unit and access the network.

MAC authentication is available only for BSUs.



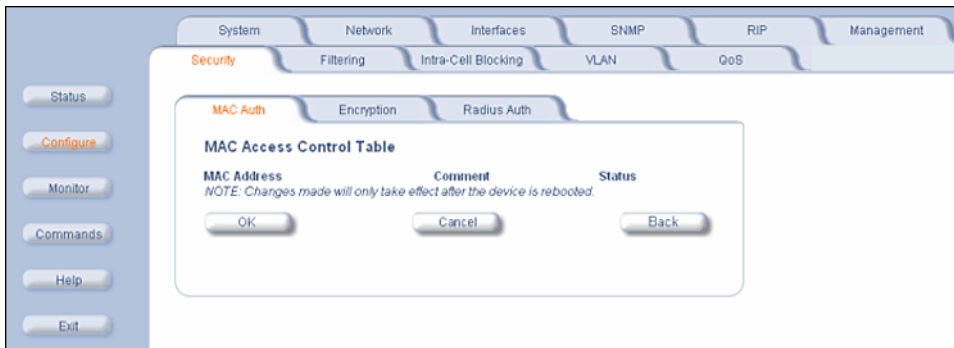
This feature is supported on the wireless interface and only wireless MAC addresses should be entered in the list. For example, build a list of wireless MAC addresses on the BSU for the authorized SUs.

To add table entries, click the **Add Table Entries** button; a window such as the following is displayed:



Enter the MAC address and any comment, then click **Add**. The maximum number of MAC addresses that can be entered is 250.

To edit or delete table entries, click the **Edit/Delete Table Entries** button; make your corrections in the window displayed and click **OK**.



Configure Encryption Parameters

NOTE: Be sure to set the encryption parameters and change the default passwords.

You can protect the wireless data link by using encryption. Encryption keys can be 5 (64-bit), 13 (WEP 128-bit), or 16 (AES 128-bit) characters in length. Both ends of the wireless data link must use the same parameter values.

In addition to Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP), the unit supports Advanced Encryption Standard (AES) 128-bit encryption. To provide even stronger encryption, the AES CCM Protocol is also supported.

Click **Configure > Security > Encryption** to set encryption keys for the data transmitted and received by the unit. Note that all devices in one network must use the same encryption parameters to communicate to each other.



Configure RADIUS Authentication

Click **Configure > Security > Radius Auth** to set the IP address of the RADIUS server containing the central list of MAC addresses that are allowed to access the network. The RADIUS parameters let you enable HTTP or Telnet RADIUS management access to configure a RADIUS Profile for management access control, to enable or disable local user access, and to configure the local password.

RADIUS authentication is available only for BSUs.



In large networks with multiple units, you can maintain a list of MAC addresses on a centralized location using a RADIUS authentication server that grants or denies access. If you use this kind of authentication, you must specify at least the primary RADIUS server. The backup RADIUS server is optional.

Filtering Parameters

Click **Configure > Filtering** to configure packet filtering. Packet filtering can be used to control and optimize network performance.

Overview

The Filtering feature can selectively filter specific packets based upon their Ethernet protocol type. Protocol filtering is done at the Bridge layer.

Protocol filters are useful for preventing bridging of selected protocol traffic from one segment of a network to other segments (or subnets). You can use this feature both to increase the amount of bandwidth available on your network and to increase network security.

Increasing Available Bandwidth

It may be unnecessary to bridge traffic from a subnet using IPX/SPX or AppleTalk to a segment of the network with UNIX workstations. By denying the IPX/SPX AppleTalk traffic from being bridged to the UNIX subnet, the UNIX subnet is free of this unnecessary traffic.

Increasing Network Security

By bridging IP and IP/ARP traffic and blocking LAN protocols used by Windows, Novell, and Macintosh servers, you can protect servers and client systems on the private local LAN from outside attacks that use those LAN protocols. This type of filtering also prevents private LAN data from being bridged to an untrusted remote network or the Internet.

To prevent blocking your own access (administrator) to the unit, Proxim recommends that IP (0x800) and ARP (0x806) protocols are always passed through.

Sample Use and Validation

Configure the protocol filter to let only IP and ARP traffic pass through the unit (bridge) from one network segment to another. Then, attempt to use Windows file sharing across the bridge. The file should not allow sharing; the packets are discarded by the bridge.

Setting the ARP Filter

There may be times when you need to set the ARP or Multicast. Usually, this is required when there are many nodes on the wired network that are sending ARP broadcast messages or multicast packets that unnecessarily consume the wireless bandwidth. The goal of these filters is to allow only necessary ARP and multicast traffic through the 1.6 Mbps wireless pipe.

The TCP/IP Internet Protocol Suite uses a method known as ARP (Address Resolution Protocol) to match a device's MAC (Media Access Control) address with its assigned IP address. The MAC address is a unique 48-bit identifier assigned to each hardware device at the factory by the manufacturer. The MAC address is commonly represented as 6 pairs of hexadecimal digits separated by colons. For example, a device may have the MAC address of 00:20:A6:33:ED:45.

When devices send data over the network (Ethernet, Token Ring, or wireless), they use the MAC address to identify a packet's source and destination. Therefore, an IP address must be mapped to a MAC address in order for a device to send a packet to particular IP address. In order to resolve a remote node's IP address with its MAC address, a device sends out a broadcast packet to all nodes on the network. This packet is known as an ARP request or ARP broadcast and requests that the device assigned a particular IP address respond to the sender with its MAC address.

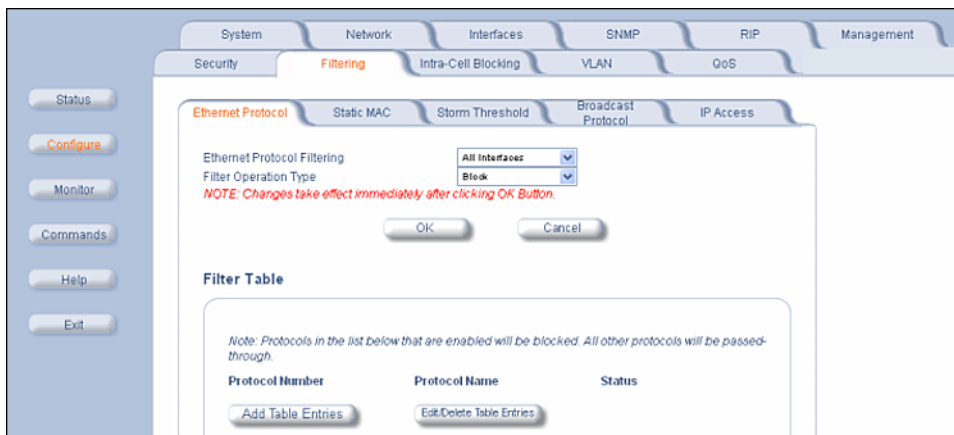
Because ARP requests are broadcast packets, these packets are forwarded to wireless nodes by default, even if the packet is not meant for a wireless node. As the number of nodes on a network backbone increases, so does the number of ARP broadcasts that are forwarded to the wireless nodes. Many of these ARP broadcasts are unnecessary and can

consume valuable wireless bandwidth. On some networks, there are so many ARP broadcasts that the performance of the wireless network will degrade due to the amount of bandwidth being consumed by these messages.

To reduce the number of ARP broadcasts that are forwarded to the wireless nodes, you can enable ARP filtering. When enabled, the ARP Filter allows the unit to forward only those ARP broadcasts destined for an IP address that falls within the range specified by the ARP Filter Network Address and the ARP Filter Subnet Mask. The ARP Filter performs a logical AND function (essentially keeping what is the same and discarding what is different) on the IP address of the ARP request and the ARP Filter Subnet Mask. It then compares the result of the logical AND to the ARP Filter Network Address. If the two values match, the ARP broadcast is forwarded to the wireless network by the unit.

Configure Ethernet Protocol Filtering

The Ethernet Protocol filter blocks or forwards packets based upon the Ethernet protocols they support. Click **Configure > Filtering > Ethernet Protocol** to enable or disable certain protocols in the table. Entries can be selected from a drop-down box.



Follow these steps to configure the Ethernet Protocol Filter:

1. Select the interfaces that will implement the filter from the **Ethernet Protocol Filtering** drop-down menu.
 - Ethernet: Packets are examined at the Ethernet interface
 - Wireless-Slot A or Wireless-Slot B: Packets are examined at the Wireless A or B interfaces
 - All Interfaces: Packets are examined at both interfaces
 - Disabled: The filter is not used
2. Select the **Filter Operation Type**.
 - If set to Block, the bridge blocks enabled Ethernet Protocols listed in the Filter Table.
 - If set to Passthru, only the enabled Ethernet Protocols listed in the Filter Table pass through the bridge.
3. Configure the **Filter Table**.
 - To add an entry, click **Add Table Entries**. You may add one of the supplied Ethernet Protocol Filters, or you may enter additional filters by specifying the appropriate parameters:
 - To add one of the supplied Ethernet Protocol Filters to the filter table:
 - Select the appropriate filter from the **Specify Common Protocol** drop-down menu. Protocol Name and Protocol Number fields will be filled in automatically.
 - Click **Add**
 - To add a new filter to the filter table:
 - Enter the **Protocol Number**. See <http://www.iana.org/assignments/ethernet-numbers> for a list of protocol numbers.
 - Enter the Protocol Name.

- Click **Add**.
- To edit or delete an entry, click **Edit** and change the information, or select Enable, Disable, or Delete from the Status drop-down menu.

NOTE: Entries must be enabled in order to be subject to the filter.

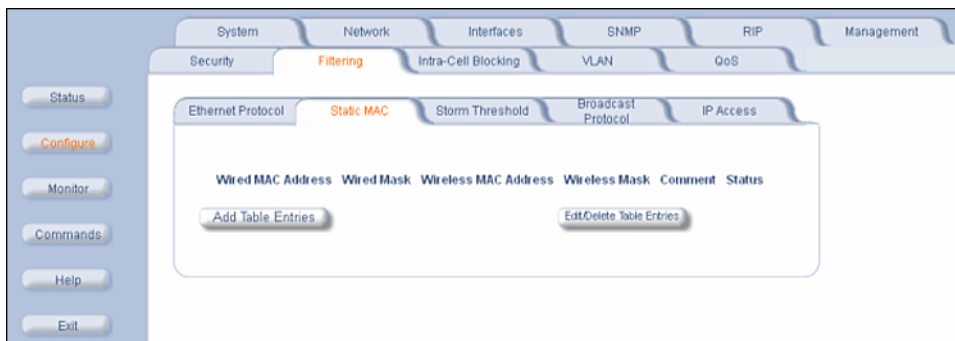
Configure Static MAC Pair Filtering

The Static MAC Address filter optimizes the performance of a wireless (and wired) network. When this feature is configured properly, the unit can block traffic between wired devices on the wired (Ethernet) interface and devices on the wireless interface based upon MAC address.

NOTE: The device on the wireless interface can be any device connected through the link, it can be directly connected to the Ethernet interface of the peer unit, or it can be attached through multiple hops. The MAC address in the packets arriving at the wireless interface is the important element.

The filter is an advanced feature that lets you limit the data traffic between two specific devices (or between groups of devices based upon MAC addresses and masks) through the unit's wireless interface. For example, if you have a server on your network with which you do not want wireless clients to communicate, you can set up a static MAC filter to block traffic between these devices. The Static MAC Filter Table performs bi-directional filtering. However, note that this is an advanced filter and it may be easier to control wireless traffic through other filter options, such as **Protocol Filtering**.

Click **Configure > Filtering > Static MAC** to access the Static MAC Address filter.



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

Taken together, a MAC address/mask pair specifies an address or a range of MAC addresses that the unit looks for when examining packets. The unit uses Boolean logic to perform an “and” operation between the MAC address and the mask at the bit level. However, for most users, you do not need to think in terms of bits. It should be sufficient to create a filter using only the hexadecimal digits 0 and F in the mask (where 0 is any value and F is the value specified in the MAC address). 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 unit examines the source and destination addresses of each packet looking for any MAC address starting with 00:20:A6. If the mask is FF:FF:FF:FF:FF:FF, the unit looks only for the specific MAC address (in this case, 00:20:A6:12:54:C3).

When creating a filter, you can configure the Wired parameters only, the Wireless parameters only, or both sets of parameters. Which parameters to configure depends upon the traffic that you want to block:

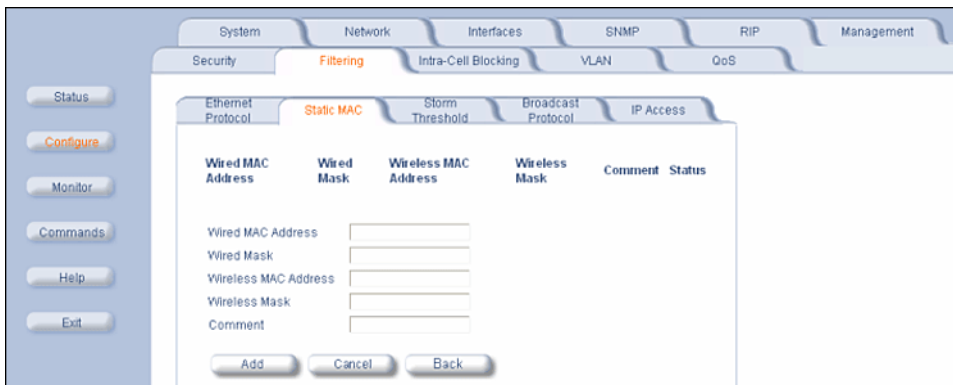
- To prevent all traffic from a specific wired MAC address from being forwarded to the wireless network, configure only the Wired MAC address and Wired mask (leave the Wireless MAC and Wireless mask set to all zeros).
- To prevent all traffic from a specific wireless MAC address from being forwarded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

- To block traffic between a specific wired MAC address and a specific wireless MAC address, configure all four parameters.

See [Static MAC Filter Examples](#) for more detailed examples.

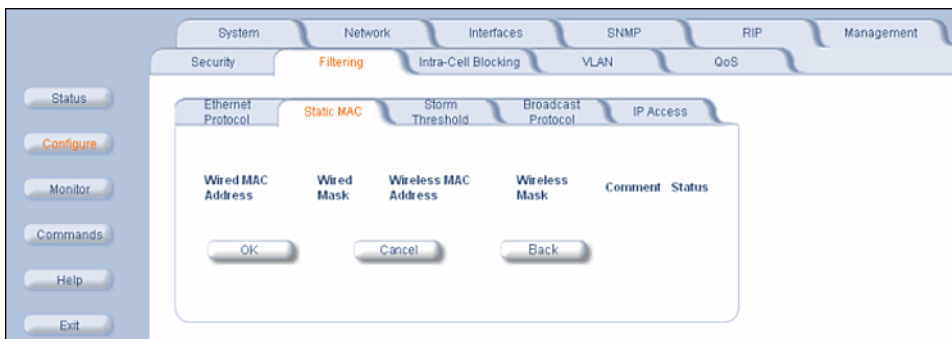
Add Entries to the Static MAC Filter Table

To add the entries to Filter table, click the **Add Table Entries** button.



After entering the data, click the **Add** button. The entry is enabled automatically when saved.

To edit an entry, click **Edit**. To disable or remove an entry, click **Edit** and change the **Status** field from **Enable** to **Disable** or **Delete**.



The following fields are may be configured or viewed:

- **Wired MAC Address:** Enter the MAC address of the device on the Ethernet network that you want to prevent from communicating with a device on the wireless network.
- **Wired Mask:** Enter the appropriate bit mask to specify the range of MAC addresses to which this filter is to apply. To specify only the single MAC address you entered in the Wired MAC Address field, enter 00:00:00:00:00:00 (all zeroes).
- **Wireless MAC Address:** Enter the MAC address of the wireless device on the wireless interface that you want to prevent from communicating with a device on the wired network.
- **Wireless Mask:** Enter the appropriate bit mask to specify the range of MAC addresses to which this filter is to apply. To specify only the single MAC address you entered in the Wireless MAC Address field, enter 00:00:00:00:00:00 (all zeroes).
- **Comment:** Enter related information.
- **Status:** The Status field can show **Enable**, **Disable**, or **Delete**.

Static MAC Filter Examples

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

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

Prevent two specific devices from communicating:

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

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

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

Prevent Multiple Wireless Devices From Communicating With a Single Wired Device

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

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

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

Prevent All Wireless Devices From Communicating With a Single Wired Device

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

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

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

Prevent A Wireless Device From Communicating With the Wired Network

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

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

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

Prevent Messages Destined for a Specific Multicast Group from Being Forwarded to the Wireless LAN

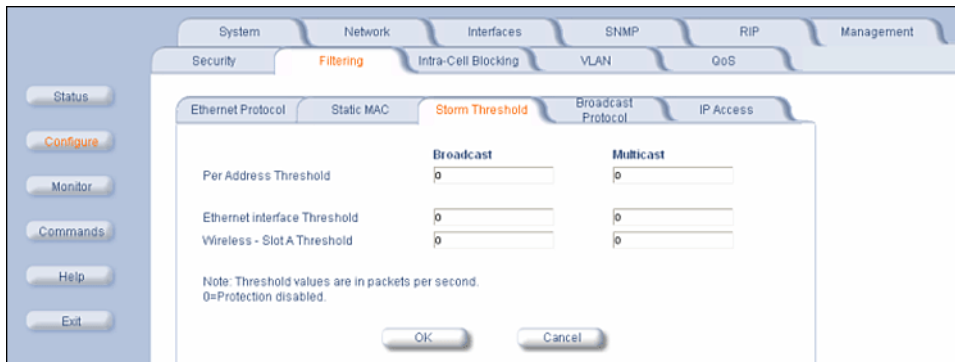
If devices on your Ethernet network use multicast packets to communicate and these packets are not required by your wireless clients, you can set up a Static MAC filter to preserve wireless bandwidth. For example, if routers on your network use a specific multicast address (such as 01:00:5E:00:32:4B) to exchange information, you can set up a filter to prevent these multicast packets from being forwarded to the wireless network:

- **Wired MAC Address:** 01:00:5E:00:32:4B
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:00:00:00:00:00
- **Wireless Mask:** 00:00:00:00:00:00

Result: The unit does not forward any packets that have a destination address of 01:00:5E:00:32:4B to the wireless network.

Configure Storm Threshold Filtering

Click **Configure > Filtering > Storm Threshold** to use threshold limits to prevent broadcast/multicast overload.



Storm Threshold is an advanced Bridge setup option that you can use to protect the network against data overload by specifying:

- A maximum number of frames per second as received from a single network device (identified by its MAC address).
- An absolute maximum number of messages per port.

The **Storm Threshold** parameters let you specify a set of thresholds for each port of the unit, identifying separate values for the number of broadcast messages per second and multicast messages per second.

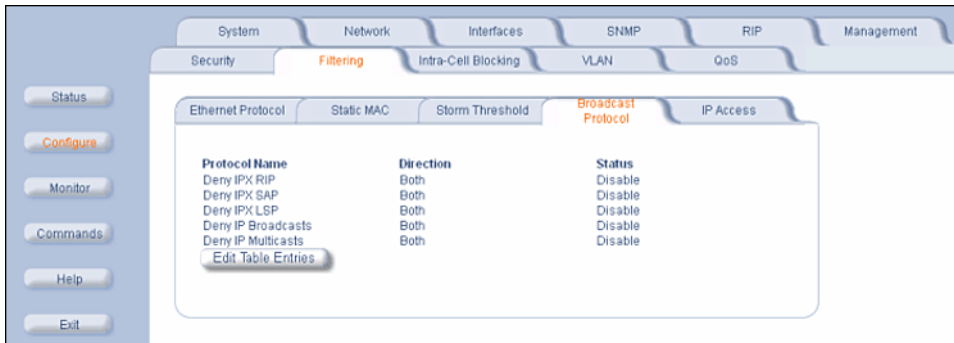
When the number of frames for a port or identified station exceeds the maximum value per second, the unit ignores all subsequent messages issued by the particular network device, or ignores all messages of that type.

The following parameters are configurable:

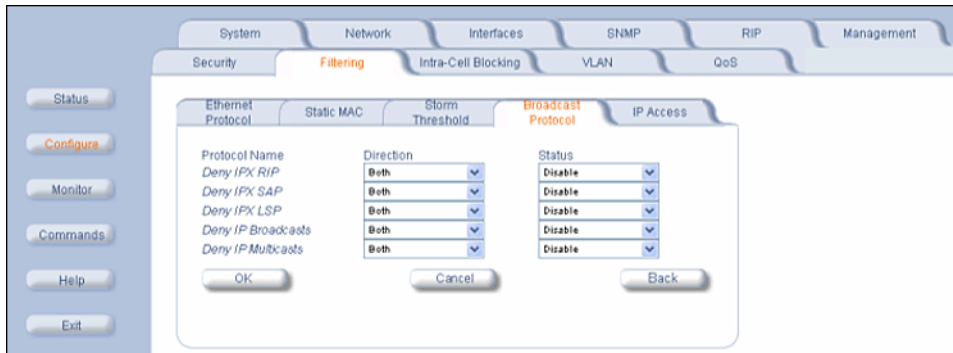
- **Per Address Threshold:** Enter the maximum allowed number of packets per second.
- **Ethernet Threshold:** Enter the maximum allowed number of packets per second.
- **Wireless Threshold:** Enter the maximum allowed number of packets per second.

Configure Broadcast Protocol Filtering

Click **Configure > Filtering > Broadcast Protocol** to deny specific IP broadcast, IPX broadcast, and multicast traffic.

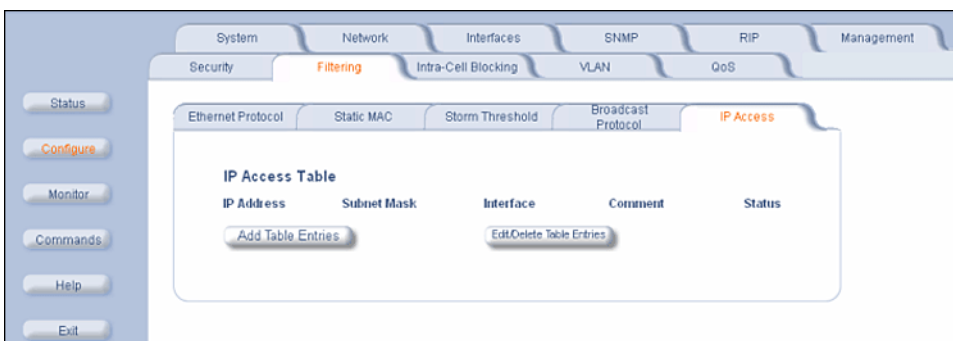


Click the **Edit Table Entries** button to display an editable window such as the following. You can configure whether this traffic must be blocked for Ethernet to wireless, wireless to Ethernet, or both.

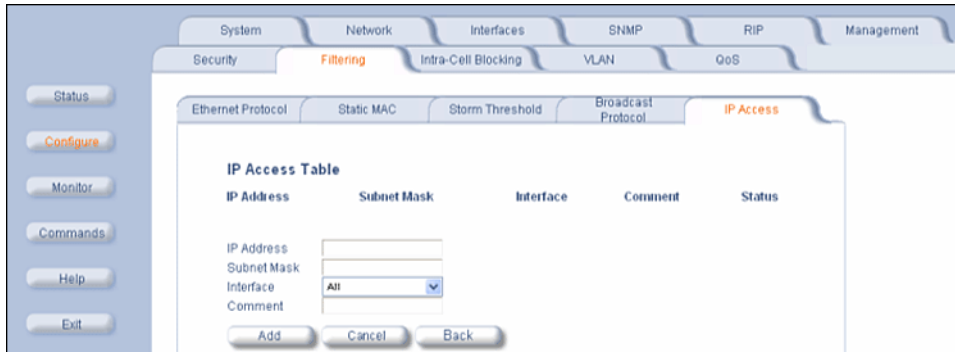


Configure IP Access Table Filtering

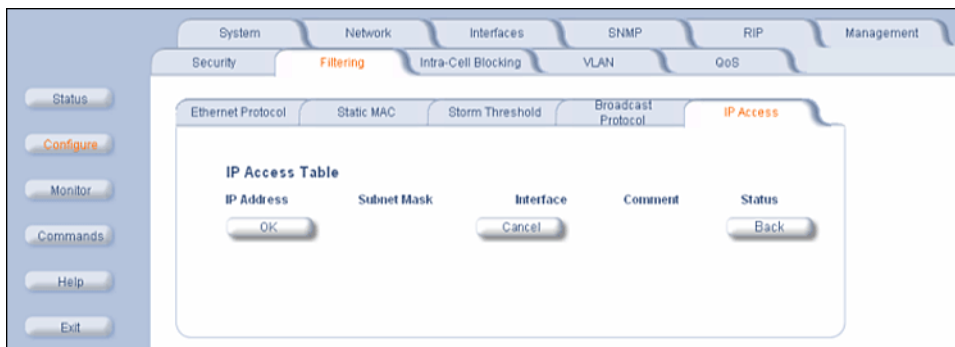
Click **Configure > Filtering > IP Access Table** to limit in-band management access to the IP addresses or range of IP addresses specified in the table. This feature applies to all management services (SNMP, HTTP, and CLI), except for CLI management over the serial port.



To add an entry, click the **Add Table Entries** button, specify the IP address and mask of the wireless stations to which you want to grant access, and click **Add**.



To edit or delete table entries, click the **Edit/Delete Table Entries** button, make your changes, and click **OK**.



For example, **172.17.23.0/255.255.255.0** allows access from all wireless stations with an IP address in the 172.17.23.xxx range.

Ensure that the IP address of the management PC you use is within the first entry in the table, as this filter takes effect immediately. Otherwise, you have locked yourself out.

When you do lock yourself out, you may try to give the PC the correct IP address; otherwise you must reset the unit.

Intra-Cell Blocking (Base Station Unit Only)

Overview

The Intra-Cell Blocking feature lets traffic be blocked between two SUs registered to the same Base Station. There are two potential reasons to isolate traffic among wireless subscribers:

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

You can form groups of SUs at the Base Station, which define the filtering criteria. All data to or from SUs belonging to the same group are bridged. All other data from SUs that do not belong to a particular group are automatically forwarded through the Ethernet interface of the Base Station. If an SU does not belong to any group, the Base Station discards the data.

You 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 Base Station are forwarded to the Security Gateway MAC address (configured in the *Security Gateway* tab).

When you change the device from **Bridge** to **Routing** mode, Intra-Cell Blocking stops working with or without a reboot. When you change the device from **Routing** to **Bridge** mode, Intra-Cell Blocking starts working with or without a reboot.

Intra-Cell Blocking Group Rules

The following rules apply to Intra-Cell Blocking Groups:

- One 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.

Example of Intra-Cell Blocking Groups

Assume that four Intra-Cell Blocking Groups have been configured on one BSU. SUs 1 through 6 are registered to BSU 1. SUs 7 through 9 are registered to BSU 2.

Intra-Cell Blocking Group Example			
Group 1	Group 2	Group 3	Group 4
SU 1	SU 2	SU 6	SU 8
SU 4	SU 3	SU 1	SU 9
SU 5	SU 8	SU 3	SU 2

In this example, SU 1 belongs to two groups, Group 1 and Group 3. Therefore, packets from SU 1 destined to SU 4, SU 5, SU 6, and SU 3 are not blocked. However, SU 9 belongs to group 4 only and packets from SU 9 are blocked unless sent to SU 8 or SU 2.

Achieving Communication Between Two SUs

In a multipoint configuration, an SU can communicate with another SU through the BSU when in Bridge mode by default. Use the intra-cell blocking feature if this is not desired. In a routing configuration, each of the SUs must have a different subnet on their Ethernet port to distinguish traffic for each SU, and each subnet must be entered into a routing rule in the BSU as well as into an upstream router. The wireless side of all SUs must share the same subnet with the BSU wireless interface. These IP addresses must be used as next hop when creating the routes for the SU subnets.

Enable Intra-Cell Blocking

Click **Configure > Intra-Cell Blocking > Group Table** to enable the Intra-Cell Blocking feature and to configure Intra-Cell Blocking Groups.

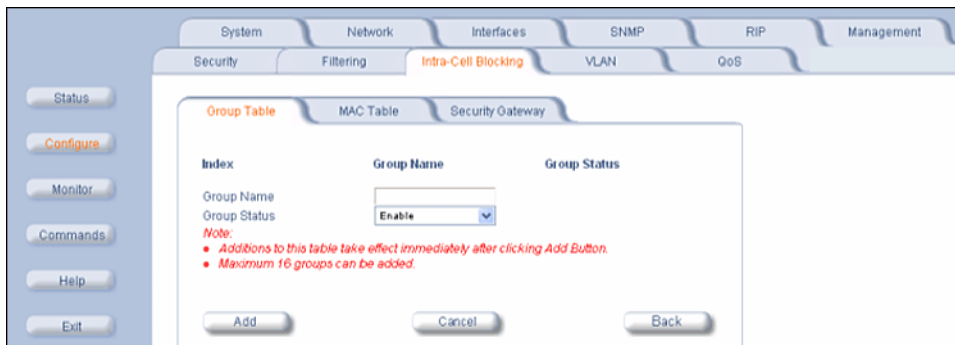


The following items are configurable:

- **Intra-Cell Blocking Status:** Enables or disables the Intra-Cell Blocking feature.
- **Group Table:** Entries in this table show the Intra-Cell Blocking filter groups that have been configured. When Intra-Cell Blocking is enabled, the Base Station Unit discards all packets coming from one SU to another SU, if both SUs do not belong to the same filter group.

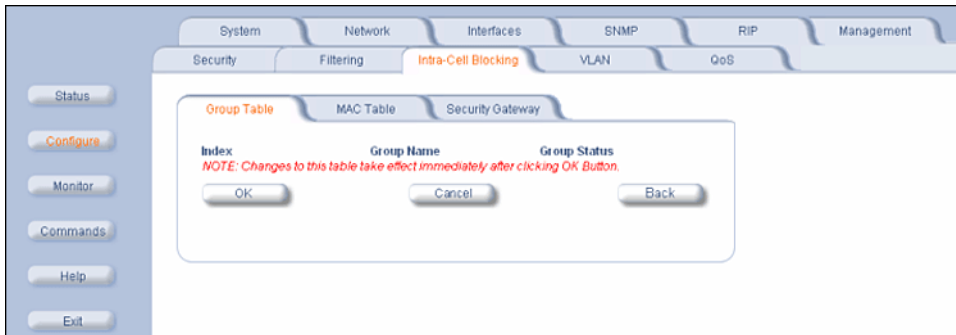
Configure Intra-Cell Blocking Groups

Click the **Add Table Entries** button to add groups to the Group Table.



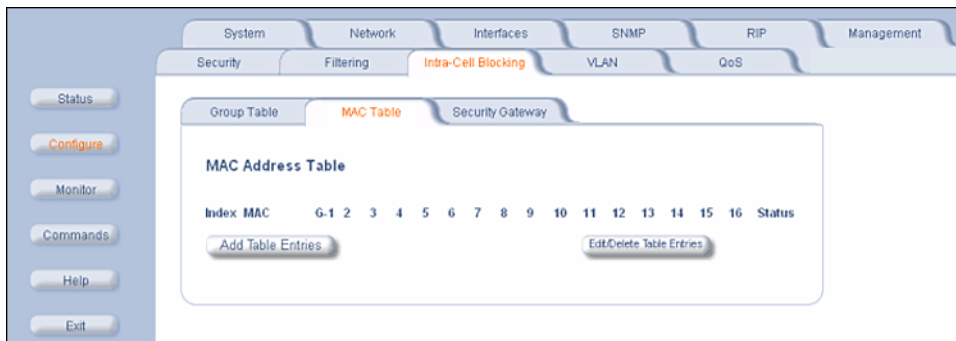
Enter the group name, and click **Add**. The group is assigned an Index and appears in the Group Table. Up to 16 groups can be configured per Base Station.

You can enable, disable or delete an existing filter group by using the **Edit/Delete Table Entries** button.



Assign MAC Addresses (MAC Table)

After configuring the Intra-Cell Blocking Groups on the **Group Table** tab, use the **MAC Table** tab to assign specific MAC addresses to an Intra-Cell Blocking Group.



Adding Entries

Click the **Add Table Entries** button.

