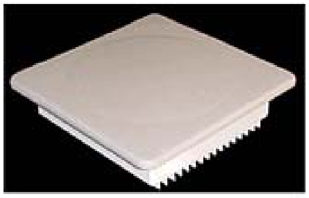
Part Number 72235r1

Tsunami MP.11
Models 2454-R, 5054-R, and 5054-R-LR
Installation and Management
Version 2.4



Proxim WIRELESS

COPYRIGHT

TRADEMARKS

REGULATORY COMPLIANCE

Please refer to the *Tsunami MP.11 Models 2454-R and 5054-R Safety and Regulatory Compliance* flyer for detailed regulatory compliance information about your product.

Contents

Chapter 1. Overview

The Tsunami MP.11 Model 5054-R (hereinafter referred to as the 5054-R) and the Model 2454-R (hereinafter referred to as the 2454-R) are flexible wireless outdoor routers that let you design solutions for point-to-point links and point-to-multipoint networks. The Tsunami MP.11 is a product family comprising several products (such as the 5054-R Base Station Unit and Subscriber Unit).

Some of the key features of the units are:

- The use of a highly optimized protocol for outdoor situations
- 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 “Overview” (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” on page 10
Provides detailed installation instructions.

Chapter 3 “Management Overview” on page 21
Explains how to access the unit for configuration and maintenance.

Chapter 4 “Basic Management” on page 33
Explains the most common settings used to manage the unit.

Chapter 5 “Web Interface” on page 40
Depicts the Web Interface in a hierarchical manner, so you can easily find details about each item.

Chapter 6 “Procedures” on page 119
This chapter provides a set of procedures, including TFTP Server Setup, Configuration Backup, Restore, and Download, Forced Reload, and Reset to Factory Defaults.

Chapter 7 “Troubleshooting” on page 124
This chapter helps you to isolate and solve problems with your unit.

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

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 traps that can be set for alarm notification.

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.

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

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 5054-R and 2454-R are 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.***

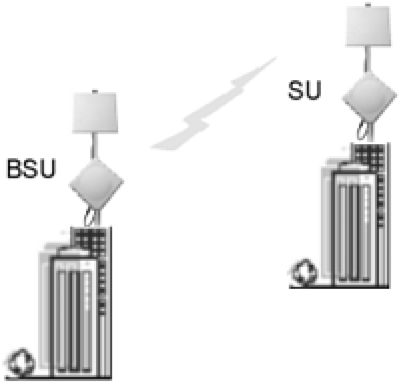
You can set up the following types of topologies:

- 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 BSU can, depending upon its configuration, connect to one or more SUs. An SU, however, can connect only to one BSU. A direct link between two locations always consists of a BSU and a SU.

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.

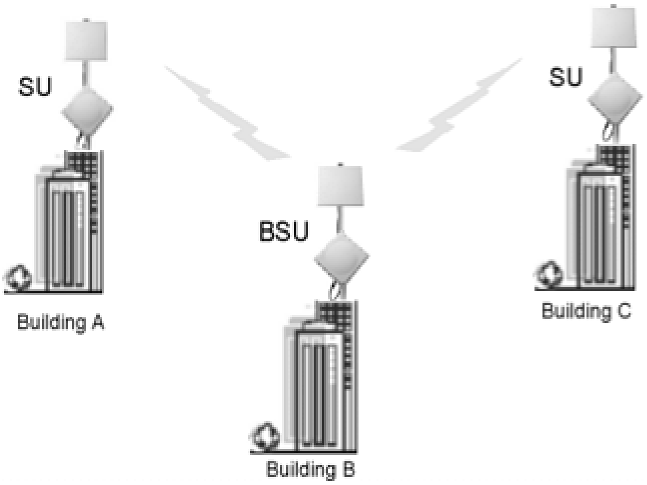


A point-to-point link lets you set up a connection between two locations as an alternative to:

- 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 SUs, a new SU cannot be connected to the BSU. In the previous figure, the system is designed as follows:

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

POWER-OVER-ETHERNET

The unit is equipped with an Active Ethernet module. Using Power-over-Ethernet (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 Active Ethernet 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 “midspan” power injection, see the IEEE 802.3af standard.
- Heating or cooling discussion: 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.

FINDING A SUITABLE LOCATION

To make optimal use of the unit, you must find a suitable location for the hardware. The range of the 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 the unit from the power outlet if necessary.
- The unit must not be covered and the air must be able to flow freely around the unit.
- The unit must be kept away from vibration and excessive heat, and must be kept free from dust buildup.
- The installation must conform to local regulations at all times.

Notes:

- The **Configure System** window provides a selectable **Country** field that automatically provides the allowed bandwidth and frequencies for the selected country as well as, where applicable, Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC).
- Non-US installers should not add an antenna system until the **Country** is selected, the unit is rebooted, and the proper power level is configured. The output power level of the final channel selected by DFS scan can be found in the Event Log (see “View the Event Log Contents” on page 41).

Chapter 2. Installation

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.

The 5054-R and 2454-R units contain 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.

IMPORTANT!

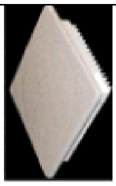
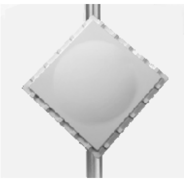
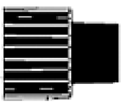
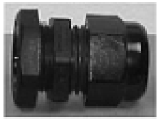
Before installing this product, see "Safety and Regulatory Information" on the product CD for important safety and regulatory compliance information.

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 National Electric Codes (NEC).

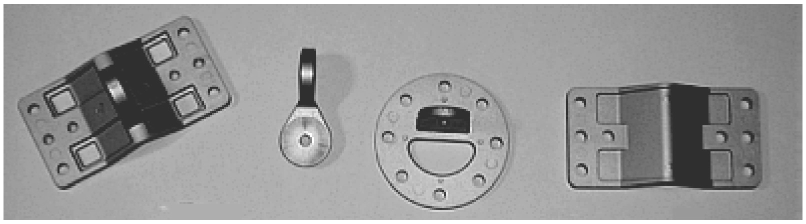
1) VERIFY PACKAGE CONTENTS

Each Tsunami MP.11 5054-R or 2454-R shipment includes the items in the table as well as the mounting hardware listed on the following page. Verify that you have received all parts of the shipment.

SU with Integrated Antenna or BSU / SU with external antenna connector	 
RJ11 to DB9 serial connector (supplied with BSU only) (1 ea.)	
Installation CD (1 ea.)	
Power Injector and Cord (1 ea.)	
Cable Termination Kit (1 ea.)	RJ45 Connector  Weather-tight connector cap  Liquid-Tite Fitting Grounding Screw

Mounting Hardware

The mounting hardware can be one of the following two mounting kits, plus the hardware listed below.

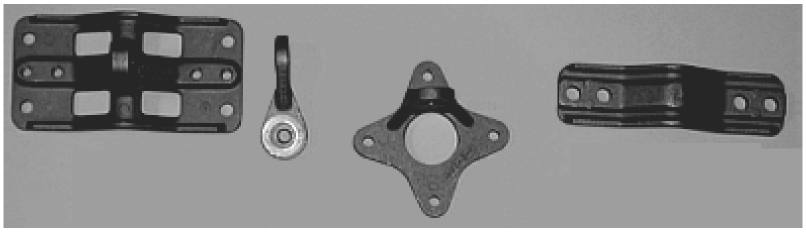


Mounting Clamp for wall/pole

Extension Arm

Mounting Plate to enclosure

Mounting Clamp for pole mounting



Item	Qty	Description
1	6 ea.	Plain washer #5/16
2	2 ea.	Hex Cap Screw NC 5/16-18 x 35
3	2 ea.	Nut NC 5/16-18
4	4 ea.	Helical Spring Lock Washer #1/4
5	4 ea.	Helical Spring Lock Washer #5/16
6	2 ea.	Hex Cap Screw NC 5/16-18 x 80
7	4 ea.	68764, SCREW, MACHINE, PAN, PHILIPS, 1/4"-20, 5/8"L,

Notes:

- Be sure to read the **Release Notes** file on the installation CD as it contains software version and driver information that may not have been available when this document was produced.
- Cables are not provided with the unit.

2) PRE-ASSEMBLE THE HARDWARE

Before mounting the unit, note the Ethernet and Mac addresses of the SU, as well as the serial number; these addresses may be used when configuring the BSU. The serial number is required to obtain support from Proxim. Keep this information in a safe place.

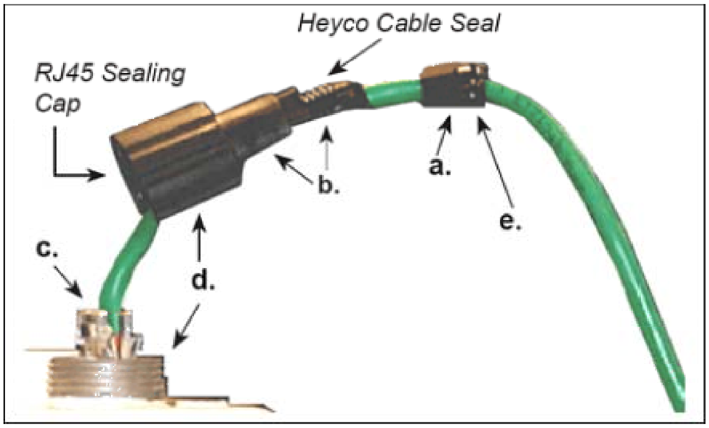
The units are designed to directly mount to a pole. Using the supplied brackets and hardware, you can mount them to a 1.25 inch to 4.5-inch pole (outside diameter). Using just one of the pole mounting brackets, you can mount the units to a wall or other flat surface.

Note: Equipment is to be used with, and powered by, the power injector provided or by a power injector that meets the following requirements:

- UL-Listed/ITE (NWGQ)
- Limited Power Source Output per UL/IEC 60950
- CE-marked
- Approved for Power-over-Ethernet,
- Rated output, 48 Vdc/0.42 A
- Wired according to the 802.3af standard for mid-span devices

To install the unit:

1. Unpack the unit and accessories from the shipping box.
2. You will be attaching an outdoor-rated Cat5e cable (not provided) to the Power-over-Ethernet port on the back of the unit later in the installation procedure. First, you must construct the cable and assemble the Liquid-Tite cable covers as described in the following steps:
   a. Slide the plastic nut over the bare end of the Cat5e cable.
   b. Attach the Heyco cable seal to the RJ45 sealing cap. Finger tighten, and slide these two assembled parts over the bare end of the Cat5e cable.
   c. Terminate the RJ45 connector to the Cat5e cable. Insert into the mating RJ45 connector.
   d. Slide the RJ45 sealing cap assembly over the RJ45 connector and thread onto enclosure. Hand tighten.
   e. Thread the plastic nut onto Heyco seal, and hand tighten.

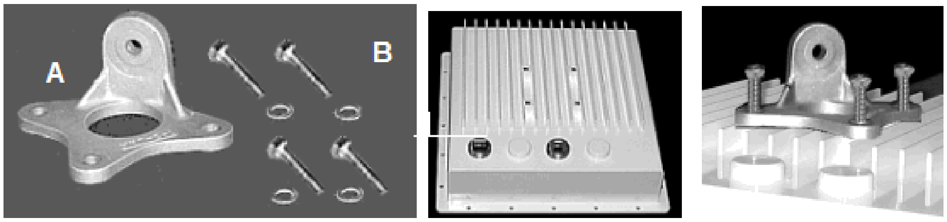


Caution! ***The domed sealing nut (item "a" above) of the Liquid-Tite connector must not be tightened until the cap over the RJ45 connector has been tightened to the unit during final installation; otherwise, the Ethernet cable may twist and damage.***

Notes:

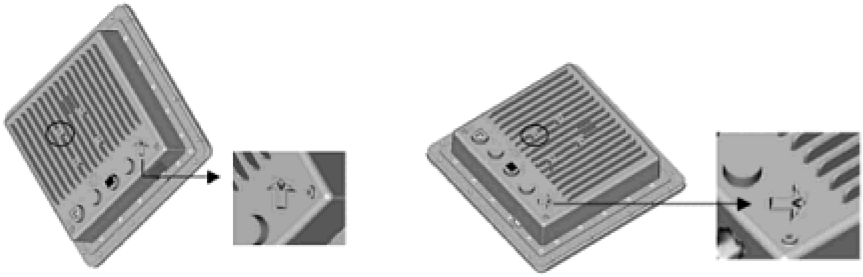
- The cable must feed through all parts of the weatherproof cap before the RJ45 is crimped on the outdoor Ethernet a cable.
- The cable between the power injector and the 5054-R or 2454-R must be a straight-through Ethernet cable (without crossover).
- Due to variance in CAT5e cable diameter, termination techniques of the installer, and the application of proper tightness of the connectors, it is strongly recommended that the CAT5e cable connector and the serial connector cap are further secured by external weatherproofing (in addition to the antenna N connector, where applicable). Butyl weatherproofing tape is the preferred material for securing any external connector.

3. Screw mounting piece (A) to the back of the unit with 4 screws and washers (B) as shown (TORQUE 75 IN-LBS):

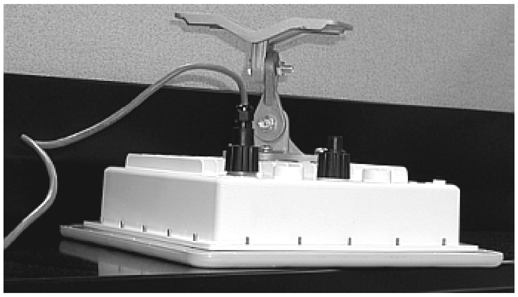


The arrow on the back of the unit indicates the direction to mount for vertical polarization when the unit has an integrated antenna. These units should be mounted with the upper portion of the bracket in the position circled in the following figure on the left for vertical alignment when not using the bracket connector C.

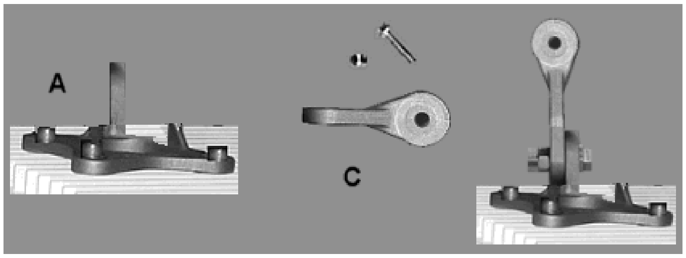
For horizontal alignment, mount the integrated-antenna unit as shown in the figure on the right. Due to the 90˚ angle between the connecting surfaces on the bracket connector C, the orientation of vertical and horizontal changes when adding the bracket.



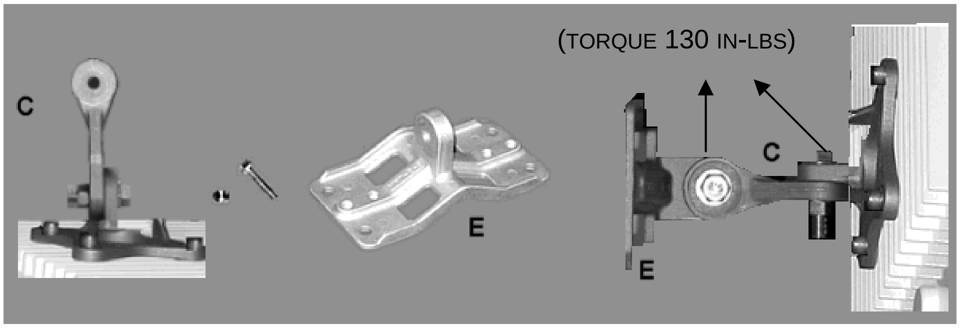
The following figure shows brackets mounted for vertical alignment:



4. Attach bracket connector (C) to mounting piece (A) with the screw and nut provided, as shown below. This extension piece gives the unit more possible tilt, letting you adjust for azimuth or elevation over a larger angle.

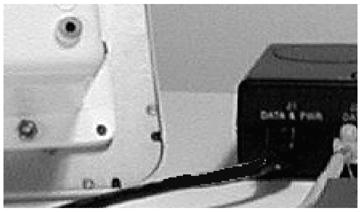


5. Attach bracket connector (C) to bracket (E) with the screw and nut provided.

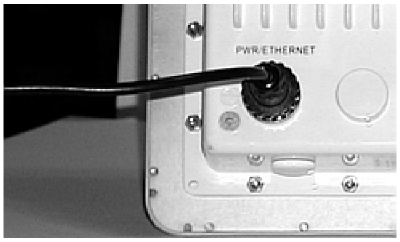


3) CONNECT THE CABLES

1. If you have not already done so, connect the normal RJ45 connector on an outdoor-rated Cat5 cable to the “Data & Power Out” port on the power injector.

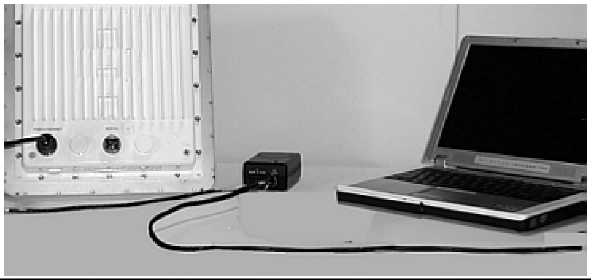


2. Attach the other end of the Cat 5 cable with RJ45 connector to the Power and Ethernet port on the back of the unit (see the following figure). Note that the first attachment of this cable is meant to verify operation and configure the unit; the final attachment and weatherproofing are to be done after the unit has been installed in the location at which it will operate. ***Do not tighten the connector nut; do not use a wrench to tighten the connector!***



3. To connect the unit through a hub or a switch to a PC, use 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.

Note: If you are connecting the PC directly to the unit, you must use a crossover Ethernet cable between the network interface card in the PC and the RJ45 "Data In" port on the power injector.



4) POWERING 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 8-pin DIN connector from the "Data and Power Out" port on the power injector.

Note: Proxim recommends the use of a lightning arrestor at the building ingress point. You can purchase the Proxim Lightning Protector MP.11/QB.11 (70251); see the documentation that comes with the unit for more information and installation instructions.

5) 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; unscrew the watertight cap if necessary to view the LEDs.

Note: Make sure the domed sealing nut of the Liquid-Tite connector is loose before unscrewing the cap or the Ethernet cable may be twisted and damaged.

During bootup, all LEDs are blinking. Blinking can continue for up to four minutes (when DFS is enabled, for example); however, if the LEDs are still blinking for over four minutes, you should check your installation and proper operation of the Ethernet and wireless links to other units. If they are correct, contact Technical Support; there could be a problem with your hardware.

Note: When powering the unit in below freezing temperatures, the unit must self-heat before booting. This is indicated by a solid red LED. This state can take up to 30 minutes, depending upon the ambient temperature.

Wireless Link LED Power & Ethernet Link LED	
Power & Ethernet Link	
BLINKING GREEN	Power is on and the Ethernet link is down

GREEN	Power is on and the Ethernet link is up.
RF (Wireless) Link	
RED	Power is on, unit is self-heating
BLINKING GREEN	A wireless link is being established.
GREEN	A wireless link has been established.

Note: The two LEDs also are continually blinking if there is any serious initialization error or when Ethernet and wireless connections both are not active. If the Ethernet is connected to a hub, check the powering of the hub and the Ethernet cable type (crossover, straight-through). If the peer unit is operational, check the configuration of the units.

6) INSTALLING DOCUMENTATION AND SOFTWARE

The CD contains the following documentation and software:

Online help

This is the help for the Web Interface. It is also stored on your computer or network during the installation process, so it is always available (see **c:\Program Files\Tsunami\MP.11**). You can also find the help in the **Docs** folder of the product CD.

Documentation

Documentation is provided in PDF format, including:

- Release Notes
- *Tsunami MP.11 2454-R and 5054-R Quick Install Guide*
- *Tsunami MP.11 2454-R and 5054-R Installation and Management*
- *Tsunami MP.11 Reference Manual*
- *Tsunami MP.11 Antenna Installation*
- *Tsunami MP.11 Recommended 5 GHz and 2.4 GHz Antennas*
- Safety and Regulatory Information

. You can find this documentation in the **Docs** folder of the product CD. This documentation also is installed at **c:\Program Files\Tsunami\MP.11**.

ScanTool

ScanTool lets you find the IP address of a Tsunami MP.11 5054-R or 2454-R by referencing the MAC address in a Scan List, or to assign an IP address if one has not been assigned. The tool automatically detects the units installed on your network, 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. See "Setting the IP Address Manually" on page 22 for details. You can find ScanTool in the **Xtras** directory of the product CD. It is installed at **c:\Program Files\Tsunami\MP.11**.

TFTP Server

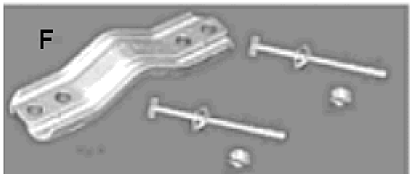
The TFTP (Trivial File Transfer Protocol) server lets you transfer files across the network. You can download configuration files, as well as image files for embedded software upgrades, and you can upload files from the unit for backup. Here *downloading* means transferring files to the unit and *uploading* means transferring files in the opposite direction. See "TFTP Server Setup" on page 119, "Download " on page 116, and "Upload" on page 117 for more information. You can find the TFTP Server in the **Xtras** directory of the product CD. It is installed at **c:\Program Files\Tsunami\MP.11**.

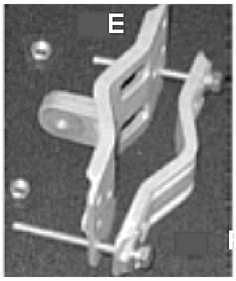
To install the documentation and software on a computer or network:

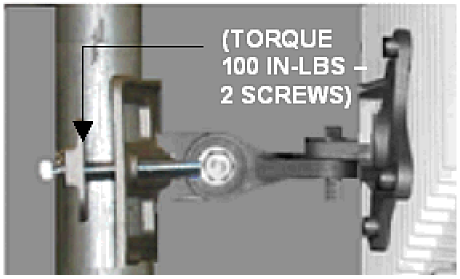
1. Place the CD in a CD-ROM drive. The installer normally starts automatically. (If the installation program does not start automatically, click **setup.exe** at the following location to begin: **\Docs\setup.exe** .)
2. Click the **Install Software and Documentation** button and follow the instructions displayed on the installer windows.

7) MOUNTING THE UNIT

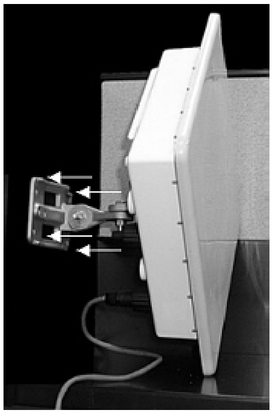
1. To pole-mount, insert screws through bracket F and fasten around pole to bracket E and secure.







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



Note: At the end of the installation, the Ethernet and serial ports must be made waterproof by installing the caps. Be careful not to over-tighten the caps as damage to the cable may occur.

8) ALIGNING THE ANTENNA

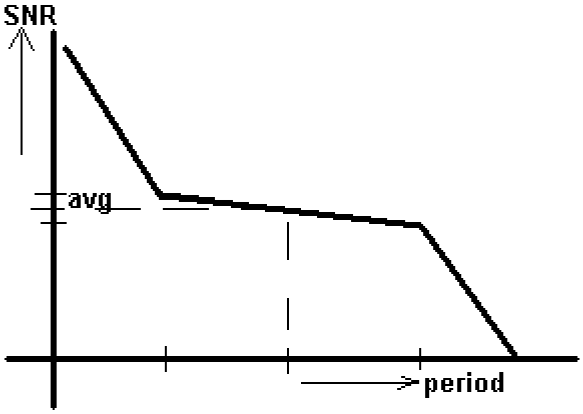
Antenna alignment is a process to physically align the antenna of the radio receiver or the transmitter to have the best possible link established between them. The antenna alignment process usually is performed during installation and after major repairs.

The unit has an audible antenna alignment tool that can be activated by plugging in the supplied serial dongle (supplied with every 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).

9) COMPLETING INSTALLATION

Be sure you have re-installed the waterproof caps on the serial and Ethernet port connections.

Caution! ***Do not over-tighten the rear nut on the waterproof connector assembly. Over-tightening can cause the Cat 5 cable to crush and can subsequently damage the power injector or the unit. The recommended torque for the rear nut is 25 to 30 inch-pounds(lbf inches) or 28.8 to 34.6 centimeter-kilograms (kgf cm).***

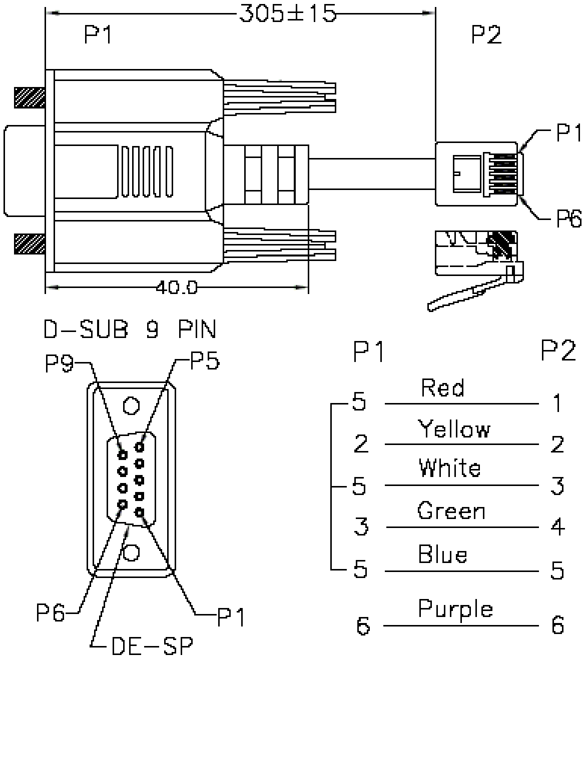
OTHER CONNECTIONS

Power and Ethernet Connection

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.



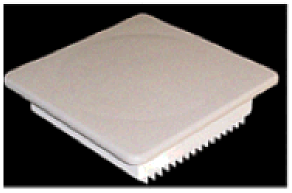
The connections are:

(D-shell - RJ-11)

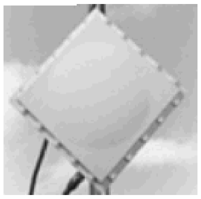
1	NC
2	2
3	4
4	NC
5	1 + 3 + 5
6	6
7	NC
8	NC
9	NC

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*.



SU with Integrated Antenna



BSU w/External Antenna Connector

Chapter 3. Management Overview

This chapter describes how to gain access to the unit for configuration and management.

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

For the serial connection, only the CLI can be used to configure and manage the unit. The other connections allow the use of the Web Interface and SNMP in addition to the CLI.

Note: These other connections require the use of the IP address of the unit in order to use the Web Interface, SNMP, or the CLI. See "IP Address" on page 22 for more information.

You can also manage the unit without an IP address by accessing the unit through the serial port with a terminal program such as HyperTerminal (see "HyperTerminal Connection Properties" in the *Tsunami MP.11 Reference Manual*).

THE INTERFACES

Three interfaces are provided for viewing or changing the unit's settings:

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 "Chapter 5. Web Interface" on page 40 for more information about 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 "Command Line Interface" in the *Tsunami MP.11 Reference Manual* for more information about the Command Line Interface.

SNMP

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 “Configure SNMP Parameters” on page 67 for setup procedures.

For the serial connection, you can use only the CLI to configure and manage the 5054-R or 2454-R units. The other connections allow the use of the Web Interface, SNMP, and the CLI; however, you must know the IP address of the unit before you can use these other connections, See “IP Address” below for more information.

IP ADDRESS

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. You can manage other basic parameters as well. ScanTool is included on the documentation and software CD to assist you in finding and changing the unit’s IP address.

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).

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.

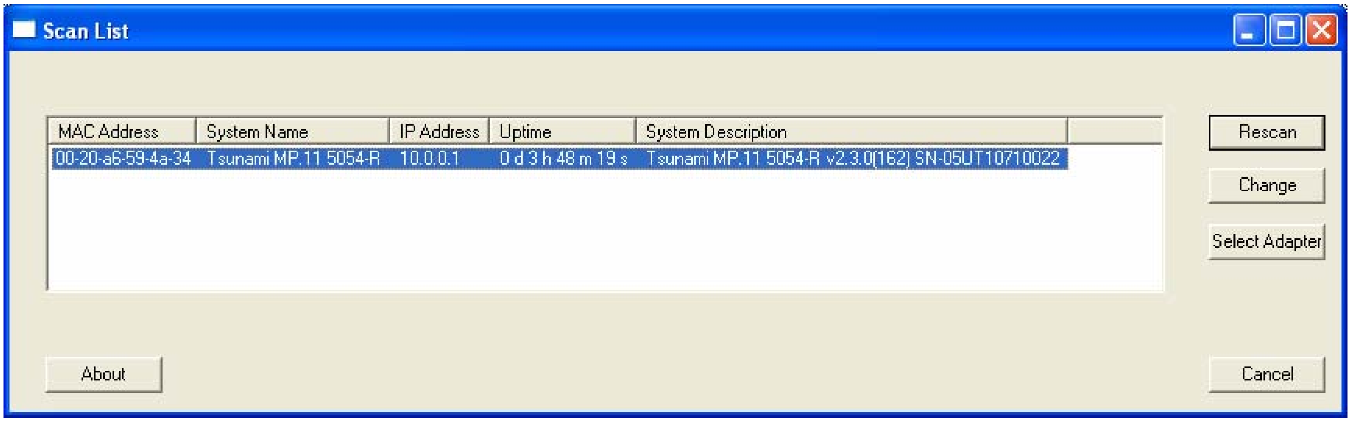
ScanTool lets you find the IP address of a Tsunami MP.11 5054-R or 2454-R by referencing the MAC address in a Scan List, or to assign an IP address if the correct one has not been assigned. The tool automatically detects the units installed on your network segment, regardless of IP address, and lets 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

If you want to set the IP address:

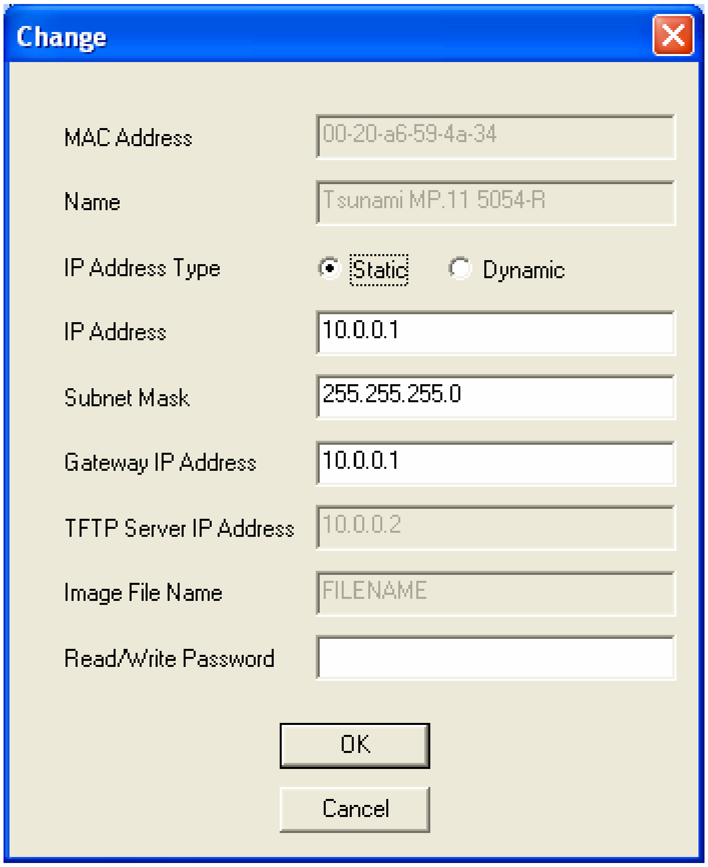
1. Run ScanTool on a computer connected to the same LAN subnet as the unit, or a computer directly connected to the unit with a cross-over Ethernet cable. ScanTool (scantool.exe) has been installed on your computer at the following location: **c:\Program Files\Tsunami\MP.11**

   ScanTool scans the subnet for 5054-R and 2454-R units and displays a list of the units it finds in the main window. The following figure is an example of the main window. 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.



MAC Address	System Name	IP Address	Uptime	System Description
00-20-a6-59-4a-34	Tsunami MP.11 5054-R	10.0.0.1	0 d 3 h 48 m 19 s	Tsunami MP.11 5054-R v2.3.0(162) SN-05UT10710022

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



MAC Address	00-20-a6-59-4a-34
Name	Tsunami MP.11 5054-R
IP Address Type	● Static ○ Dynamic
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	

3. 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.

4. 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.

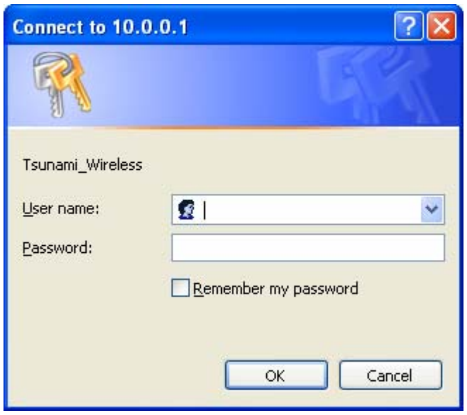
STARTING THE WEB INTERFACE

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; the Web Interface itself described in “Chapter 4. Basic Management” on page 33 and “Chapter 5. Web Interface” on page 39.

To use the Web Interface, you need only the HTTP password and IP address of the unit. (See “IP Address” on page 22 for details.)

Note: If the connection is slow or you are not able to connect, use the Internet Explorer **Tools** menu 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 in the **Address** box. The Web address should appear as **http://<ip address>** (for example, **http://10.0.0.1**). A window such as the following is displayed.



Connect to 10.0.0.1

Tsunami_Wireless

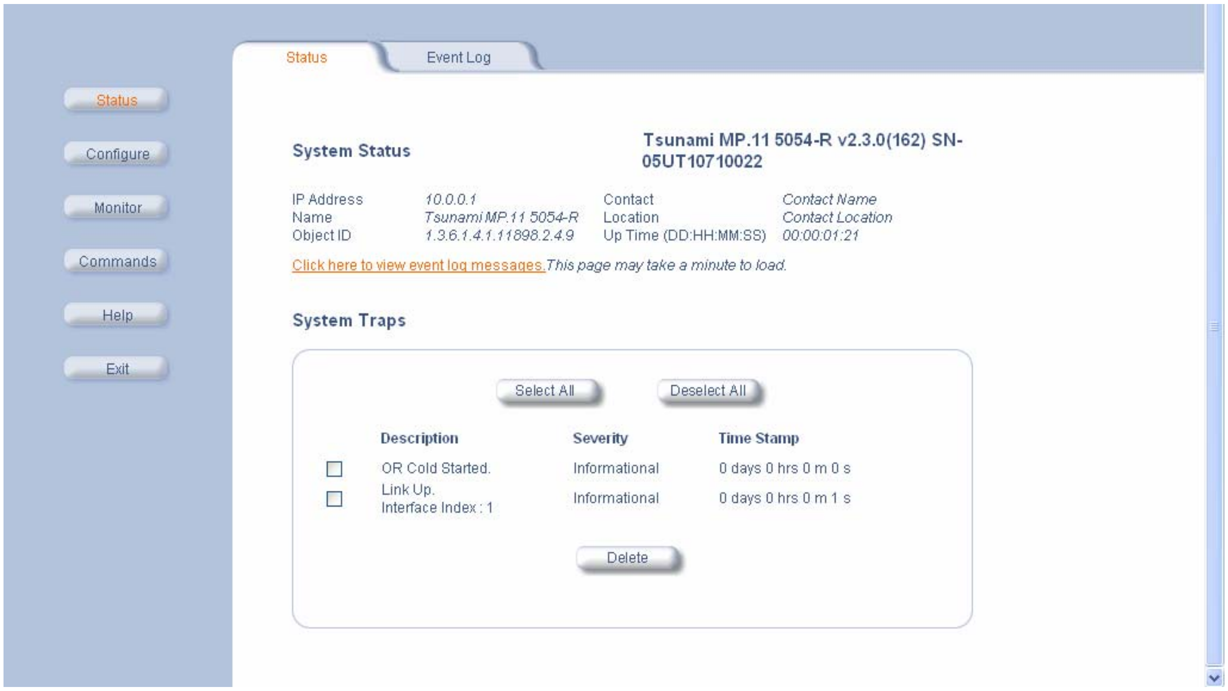
User name:

Password:

□ Remember my password

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. You now have access to the unit’s Web Interface. To find out more about the information presented in this window, see “System Status” on page 40.



System Status

Tsunami MP.11 5054-R v2.3.0(162) SN-05UT10710022

IP Address	10.0.0.1	Contact	Contact Name
Name	Tsunami MP.11 5054-R	Location	Contact Location
Object ID	1.3.6.1.4.1.11898.2.4.9	Up Time (DD:HH:MM:SS)	00:00:01:21

Click here to view event log messages.This page may take a minute to load.

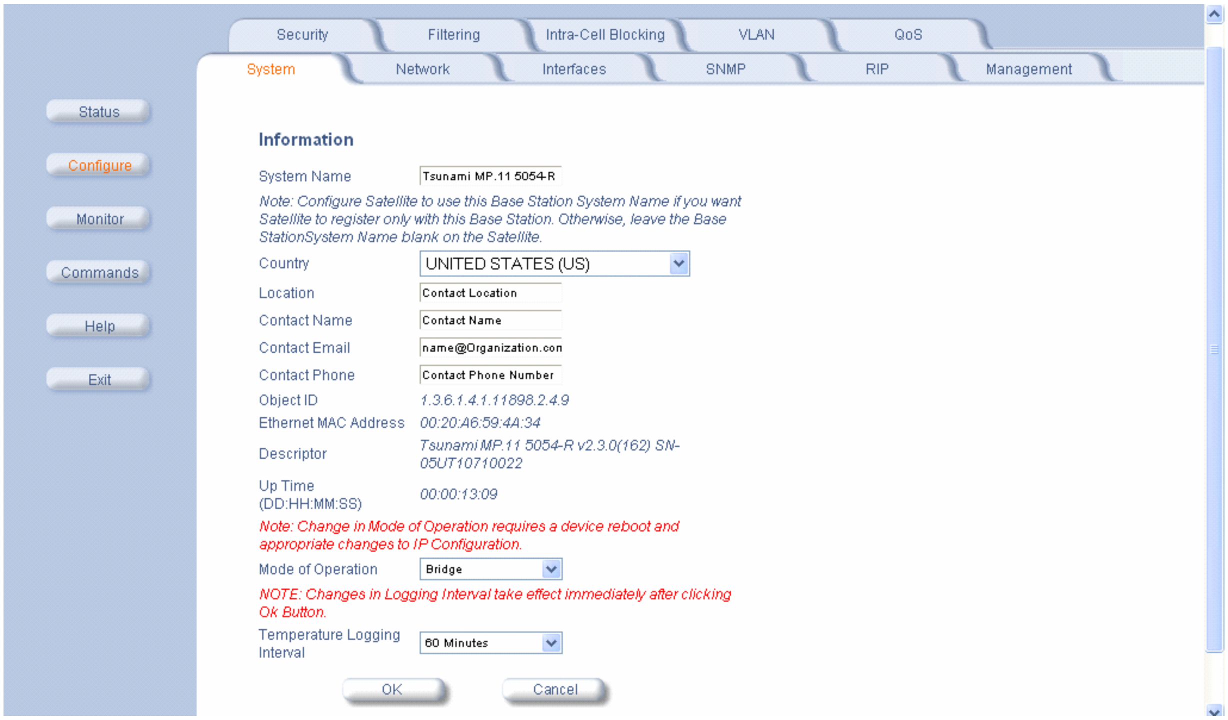
System Traps

	Description	Severity	Time Stamp
□	OR Cold Started.	Informational	0 days 0 hrs 0 m 0 s
□	Link Up. Interface Index : 1	Informational	0 days 0 hrs 0 m 1 s

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 “Configure System Parameters” on page 42 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.



Information

System Name: Tsunami MP.11 5054-R

Note: Configure Satellite to use this Base Station System Name if you want Satellite to register only with this Base Station. Otherwise, leave the Base StationSystem Name blank on the Satellite.

Country: UNITED STATES (US)

Location: Contact Location

Contact Name: Contact Name

Contact Email: name@Organization.con

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 5054-R v2.3.0(162) SN-05UT10710022*

Up Time (DD:HH:MM:SS): *00:00:13:09*

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

Mode of Operation: Bridge

NOTE: Changes in Logging Interval take effect immediately after clicking Ok Button.

Temperature Logging Interval: 60 Minutes

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. Units sold outside of the United States support the selection of a **Country** by the professional installer.

Note: Non-US installers should not add an antenna system until the **Country** is selected, the unit is rebooted, and the proper power level is configured. The output power level of the final channel selected by DFS scan can be found in the Event Log (see “Event Log” on page 41).

The Dynamic Frequency Selection (DFS) feature is enabled automatically when you choose a country with a regulatory domain that requires it. The Transmit Power Control (TPC) feature is always available.

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

Continue configuring settings as desired; then click the **Commands** button and the **Reboot** tab 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.

Dynamic Frequency Selection (DFS)

The Tsunami MP.11 5054-R supports Dynamic Frequency Selection (DFS) for European Telecommunications Standard Institute (ETSI) domains per EN 301-893 regulations. The ETSI requires that 802.11a devices use DFS to prevent interference with radar systems and other devices that already occupy the 5 GHz band.

During boot-up, the unit scans the available frequency and selects a channel that is quiet and free of radar interference. If the unit subsequently detects radar interference on its channel, it rescans to find a better channel. Upon finding a new channel, the unit waits 60 seconds to detect radar interference; if it finds no interference, it switches to the new channel.

If you are using a 5054-R unit in Europe or other applicable countries, keep in mind the following:

- DFS is not a configurable parameter; it is always enabled and cannot be disabled.
- You cannot manually select the device's operating channel; you must let the unit select the channel. However, you can specify a particular "preferred" channel that you want to scan first whenever the DFS process starts. You may also make channels unavailable by manually "blacklist" them and prevent those channels to be scanned, as well as display the Channel Blacklist Table.
- You cannot configure the **Auto Channel Select** option. Within the HTTP or CLI interface, this option always appears enabled.

With Tsunami MP.11 5054-R units, Dynamic Frequency Selection (DFS) is enabled automatically based upon the country you select. You can tell DFS is in use because the frequency selection field displays only the DFS-selected frequency. DFS scans all available frequencies, starting with the DFS preferred channel and skipping blacklisted channels, to select the operating frequency automatically.

A country selection with DFS enabled causes the Base Station to come up in scan mode. It scans the available frequencies and channels to avoid radar and selects a channel with the least interference.

Note: Scanning is performed only on the frequencies allowed in the regulatory domain of the country selected when it is required for radar detection and avoidance.

To comply with your country's regulations, change the DFS selection to specify your country. You can do this by logging into the unit, clicking the **Configure** button and selecting the **System** tab. There is a drop-down box labeled **Country** with all available countries from which to select. Choose your country, configure the unit as required, and reboot for the settings to take effect.

The SU also comes up in scan mode to scan all available frequencies to find a BSU with which it can register. Scanning may take several minutes. After establishing a wireless link, the wireless LED stops flashing and continues to shine green.

Note: Because DFS may need to scan for radar on multiple channels, you must allow a sufficient amount of time for the units to start up. This is considerably longer than when the unit is not using DFS. This is expected behavior. Startup time is within four minutes if no radar is detected, but up to one minute is added for every selected channel that results in radar detection.

DFS is required for two purposes:

1. *Radar avoidance both at startup and while operational*. To meet these requirements, the BSU scans available frequencies at startup for the presence of a radar signal on all available frequencies. If a radar signal is detected on any DFS enabled channel, the system will blacklist the channel for a period of 30 minutes in accordance to EN301-893. Once fully operational on a frequency, the BSU actively monitors the occupied frequency for radar interference. If radar interference is detected, the BSU blacklists the channel, logs a message and rescans to find a new frequency free of radar interference.

Radar detection is performed only by the BSU and not by the SU. When an SU is set to a country in which DFS is used, it scans all available channels upon startup looking for a BSU that best matches its connection criteria (such as **Base Station System Name**, **Network Name**, and **Shared Secret**). The SU connects to the BSU automatically on whatever frequency the BSU has selected. Because of this procedure, it is best to set up the BSU and have it fully operational before installing the SU, although this is not required. If a BSU rescans because of radar interference, the SU loses its wireless link. The SU waits 30 seconds (when the Mobility feature is enabled, the SU starts scanning for a BSU instantly rather than waiting 30 seconds); if it finds that it could not receive the BSU in this amount of time, it rescans the available frequencies for an active BSU.

2. *Guarantee the efficient use of available frequencies by all devices in a certain area*. To meet this requirement, the BSU scans each available frequency upon startup and selects a frequency based upon the least amount of noise and interference detected. This lets multiple devices operate in the same area with minimal interference. This procedure is done only at startup; if another non-radar device comes up on the same frequency, the BSU does not detect this or rescan because of it. It is expected that other devices using these frequencies also are in compliance with country regulations, so this should not happen.

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 System Parameters" on page 42 to configure **Country.** See "Configure the Wireless Interface" on page 57 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 or DFS)

See "Configure System Parameters" on page 42 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 and DFS is not required.
- 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.

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 5054-R and 2454-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 (see “Chapter 5. Using the Web Interface” on page 40)
- 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 “Configure VLAN Parameters” on page 88.

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
   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
- 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 according to the table on page 62
- 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

Chapter 4. Basic Management

This chapter describes how to configure and monitor the unit's basic features. In most cases, configuring these basic features is sufficient. A full overview of the Web Interface is provided in "Chapter 5. Using the Web Interface" on page 40. 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*.

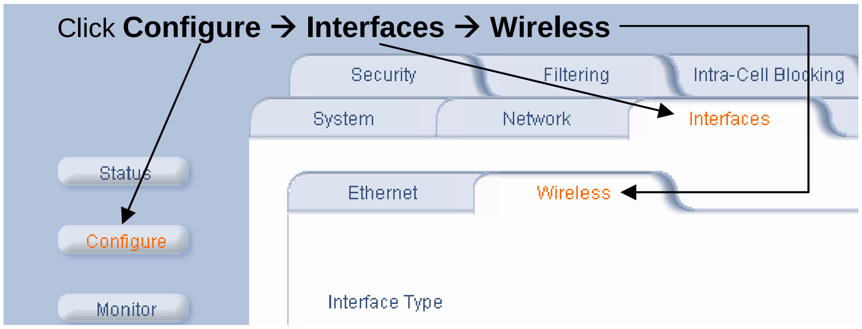
The following topics are discussed in this chapter:

- Rebooting and Resetting below
- General Configuration Settings on page 35
- Monitoring Settings on page 36
- Security Settings on page 36
- Default Settings on page 37
- Upgrading the Unit on page 39

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" on page 22 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 unit'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.


Click **Configure → Interfaces → Wireless**

The Web Interface also provides online help, which is stored on your computer (see "Installing Documentation and Software" on page 16 for details).

REBOOTING AND RESETTING

All configuration changes require a restart unless otherwise stated. New features explicitly state whether a reboot is required or not. You can restart the unit with the **Reboot** command; see the first method described in the following sub-sections.

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" on page 34).

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 the **Commands** button, then the **Reboot** tab. Click the **Reboot** button. 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 must be done only when you are experiencing problems. Resetting to the default settings requires reconfiguration of the unit.

To reset to factory default settings:

1. Click the **Commands** button, then the **Reset** tab.
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" on page 121 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 "View System Status" on page 40 for more information.

System Configuration

The System Configuration window lets you change the unit's c*ountry*, *system name*, *location name*, and so on (see the window to the right). The Country selection is required to enable the correct parameters. The other details help distinguish this unit from other routers, and let you know whom to contact in case of problems. See "1) Configure System Parameters" on page 42 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 "2) Configure Network Parameters" on page 47 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 the **Configure** button, the **Interfaces** tab, and the **Ethernet** sub-tab. 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" on page 67 for more information.

Wireless

To configure the **wireless** interface, click the **Configure** button followed by the **Interfaces** tab; then click the **Wireless** sub-tab. 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 "3) Configure Interface Settings" on page 57 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 "10) Configure VLAN Parameters" on page 88 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 the **Monitor** button and the **Wireless** tab. This tab lets you monitor the unit's general performance and the performance of the **WORP Base** or **WORP Satellite** interfaces.

Interfaces

To monitor transmission details, click the **Monitor** button and the **Interfaces** tab. The **Interfaces** tab provides detailed information about the MAC-layer performance of the wireless network and Ethernet interfaces.

Per Station

Click the **Monitor** button and the **Per Station** tab 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 5054-R and 2454-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 the **Configure** button and the **Interfaces** tab; then click the **Wireless** sub-tab. 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 the **Configure** button, the **Security** tab, and the **Encryption** sub-tab. See "Configure Encryption" on page 74.

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 the **Configure** button, the **Management** tab, and the **Password** sub-tab. See "Configure Passwords" on page 70.

DEFAULT SETTINGS

FEATURE / MODEL	5054-R	2454-R
System Name	Tsunami MP.11 5054-R	Tsunami MP.11 2454-R
Mode of Operation	Bridge	Bridge
Routing	Disabled	Disabled
IP Address Assignment Type	Static	Static
IP Address	10.0.0.1	10.0.0.1
Subnet Mask	255.255.255.0	255.255.255.0
Default Router IP Address	10.0.0.1	10.0.0.1
Default TTL	64	64
RIPv2	Enabled when in Routing Mode	Enabled when in Routing Mode
Base Station System Name	<blank>	<blank>
Network Name	OR_WORP	OR_WORP
Frequency Channel	Channel 149, Frequency 5.745 GHz (FCC Only devices) DFS Enabled (World Mode devices)	Channel 10 (2.412 – 2.462 GHz)
Transmit Power Control	0 dB	0 dB
Data Rate	36 Mbps	36 Mbps
Registration Timeout	5	5
Network Secret	public	public
Turbo Mode	Disabled	Not applicable
Channel Bandwidth	20 MHz	20 MHz
Input bandwidth limit (in Kbps)	36032	36032
Output bandwidth limit (in Kbps)	36032	36032
Ethernet Configuration	Auto-Speed Auto-Duplex	Auto-Speed Auto-Duplex
Serial port Baud Rate	9600	9600
SNMP Management Interface	Enabled	Enabled
Telnet Management Interface	Enabled	Enabled
HTTP Management Interface	Enabled	Enabled
HTTP Port	80	80
Telnet Port	23	23
Telnet Login Timeout	30	30
Telnet Session Timeout	900	900
Password	public	public
Maximum Satellites (per BSU)	250	250
MAC Authentication	Disabled	Disabled

FEATURE / MODEL	5054-R	2454-R
Radius Authentication	Disabled	Disabled
Encryption	Disabled	Disabled
Static MAC Address Filter	Disabled / No Entries	Disabled / No Entries
Ethernet Protocol Filtering	All Filters Disabled	All Filters Disabled
DFS Priority Frequency Channel	Disabled	N/A
Announcement Period (when roaming enabled)	100 ms	100 ms
Multi-Frame Bursting	Enabled	Enabled
Storm Threshold	Broadcast/Multicast Unlimited	Broadcast/Multicast Unlimited
Broadcast Protocol Filtering	All Protocols Allowed	All Protocols Allowed
Dynamic Data Rate Selection	Disabled	Disabled
Roaming	Disabled	Disabled
NAT	Disabled	Disabled
Intra-Cell Blocking	Disabled	Disabled
Antenna Alignment	Disabled	Disabled
Country Selection	US-only device – US World device – GB	US-only device – US World device – GB
DHCP Server	Disabled	Disabled
DHCP Relay	Disabled	Disabled
Spanning Tree Protocol	Disabled	Disabled
Antenna Gain (For DFS Threshold compensation)	0	0
Satellite Density	Large	Large
Temperature Logging	Enabled	Enabled
Temperature Logging Interval	60 minutes	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 “Download Files” on page 116, and in “Web Interface Image File Download” on page 120. A TFTP server is provided on the Documentation and Software CD; the server is required to transfer the downloaded file to the unit.

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.

Chapter 5. Using the Web Interface

This section covers the unit's Web Interface. The interface is described hierarchically according to these buttons, which appear on the left side of the Web page:

- System Status below
- Configure on page 42
- Monitor on page 108
- Commands on page 116

Help and Exit buttons also appear; 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 "Chapter 4. Basic Management" on page 33.

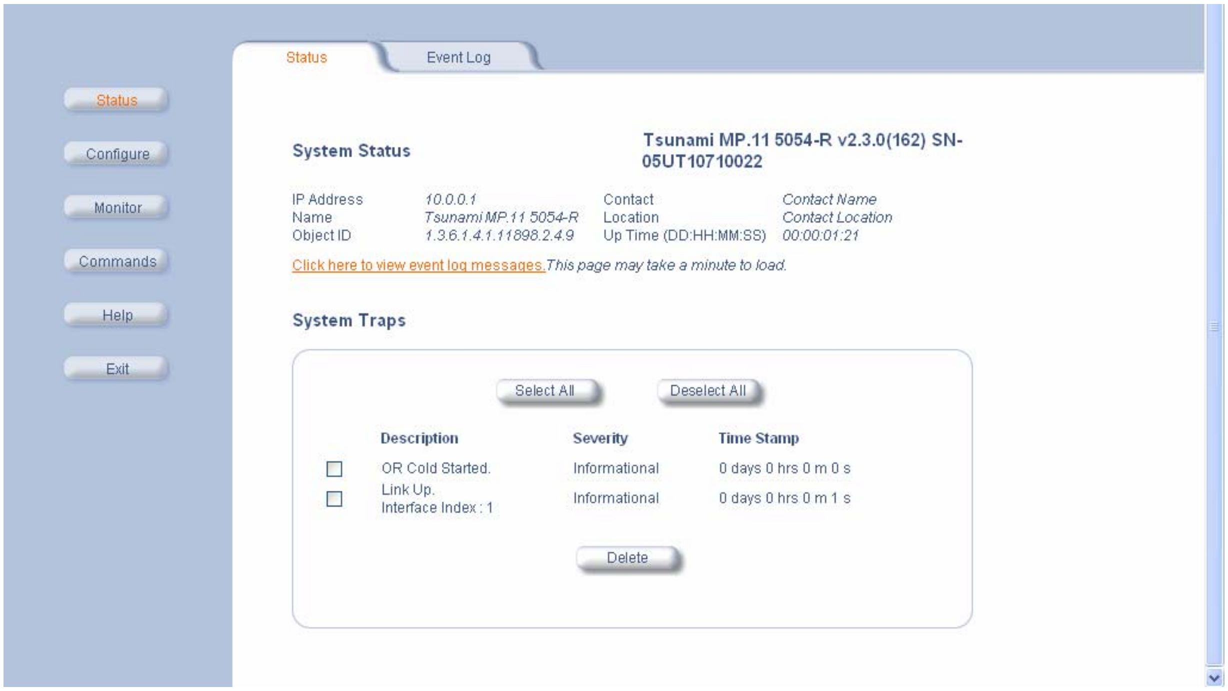
SYSTEM STATUS

When you click the **Status** button, System Status is displayed automatically. The other tab under **Status** is the **Event Log** tab.

View System 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**.



System Status

Tsunami MP.11 5054-R v2.3.0(162) SN-05UT10710022

IP Address	*10.0.0.1*	Contact	*Contact Name*
Name	*Tsunami MP.11 5054-R*	Location	*Contact Location*
Object ID	*1.3.6.1.4.1.11898.2.4.9*	Up Time (DD:HH:MM:SS)	*00:00:01:21*

Click here to view event log messages.*This page may take a minute to load.*

System Traps

	Description	Severity	Time Stamp
□	OR Cold Started.	Informational	0 days 0 hrs 0 m 0 s
□	Link Up. Interface Index : 1	Informational	0 days 0 hrs 0 m 1 s

System Status

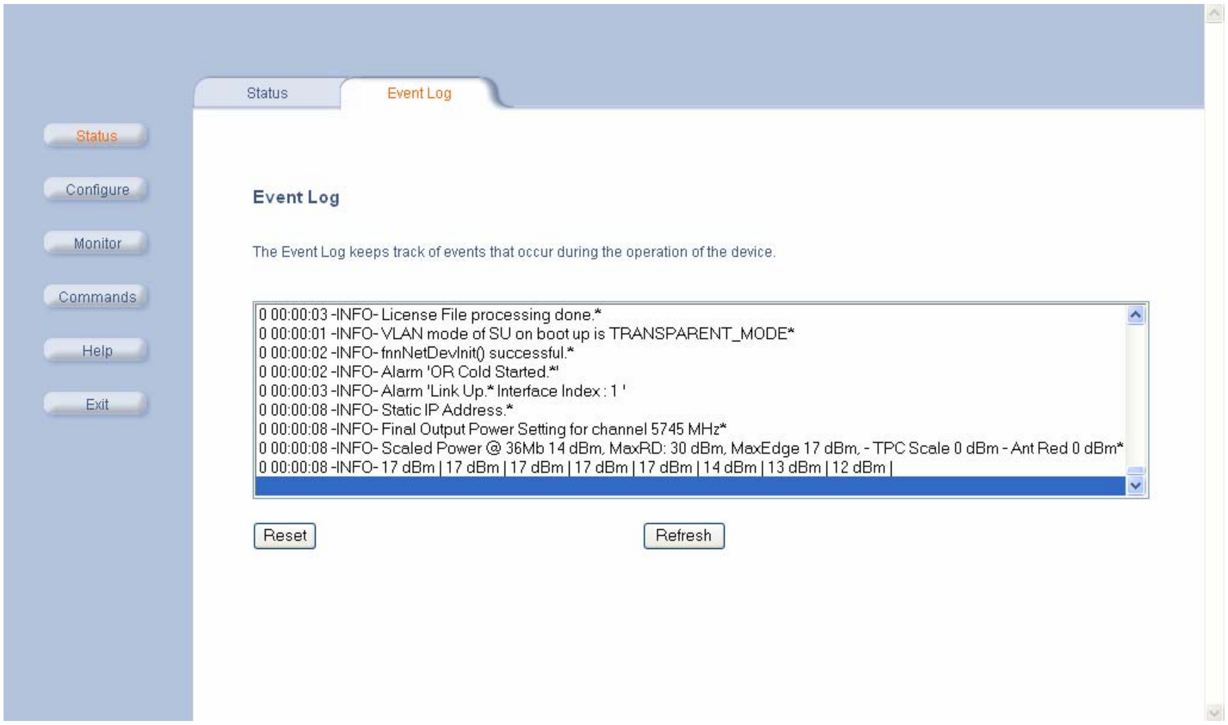
The basic system status is shown in this section, including the version number of the embedded software.

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.

View the Event Log Contents

Click the **Status** button and the **Event Log** tab 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.



Event Log

The Event Log keeps track of events that occur during the operation of the device.

```
0 00:00:03 -INFO- License File processing done.*
0 00:00:01 -INFO- VLAN mode of SU on boot up is TRANSPARENT_MODE*
0 00:00:02 -INFO- fnnNetDevInit() successful.*
0 00:00:02 -INFO- Alarm 'OR Cold Started.*'
0 00:00:03 -INFO- Alarm 'Link Up.* Interface Index : 1 '
0 00:00:08 -INFO- Static IP Address.*
0 00:00:08 -INFO- Final Output Power Setting for channel 5745 MHz*
0 00:00:08 -INFO- Scaled Power @ 36Mb 14 dBm, MaxRD: 30 dBm, MaxEdge 17 dBm, - TPC Scale 0 dBm - Ant Red 0 dBm*
0 00:00:08 -INFO- 17 dBm | 17 dBm | 17 dBm | 17 dBm | 17 dBm | 14 dBm | 13 dBm | 12 dBm |
```

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

CONFIGURE THE UNIT’S SETTINGS

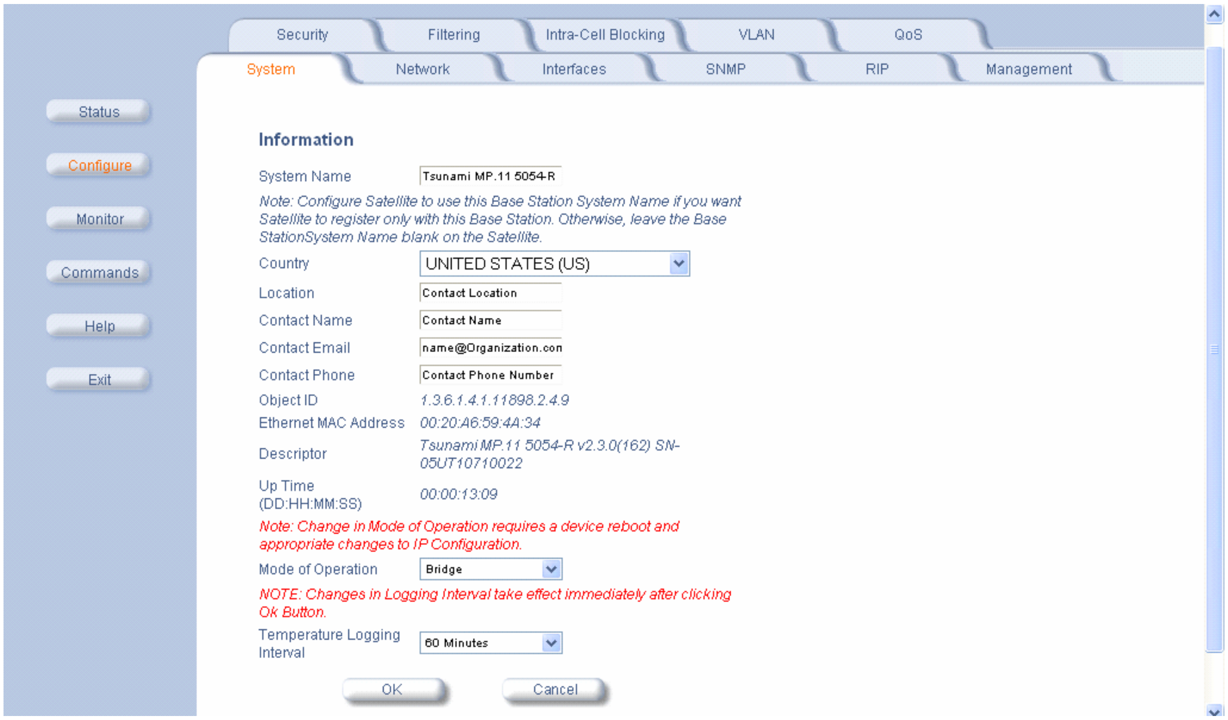
Use the **Configure** section to change the unit’s settings. The following tabs are in this section:

1. System Parameters below
2. Network Parameters on page 47
3. Interfaces on page 57
4. SNMP on page 67
5. RIP on page 67
6. Management on page 70
7. Security on page 73
8. Filtering on page 75
9. Intra-Cell Blocking on page 85 (for BSUs in Bridge mode only)
10. VLAN (Virtual Local Area Network) on page 88 (for BSUs in Bridge mode only)
11. QoS (Quality of Service) on page 96 (for BSUs only)
12. NAT (Network Address Translation) on page 98 (for SUs in Routing mode only)

1) Configure System Parameters

The **System** configuration page lets you change the unit’s **System Name**, **Location**, 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 the **Configure** button and the **System** tab; the following window is displayed.



Information

System Name: Tsunami MP.11 5054-R

Note: Configure Satellite to use this Base Station System Name if you want Satellite to register only with this Base Station. Otherwise, leave the Base StationSystem Name blank on the Satellite.

Country: UNITED STATES (US)

Location: Contact Location

Contact Name: Contact Name

Contact Email: name@Organization.con

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 5054-R v2.3.0(162) SN-05UT10710022*

Up Time (DD:HH:MM:SS): *00:00:13:09*

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

Mode of Operation: Bridge

NOTE: Changes in Logging Interval take effect immediately after clicking Ok Button.

Temperature Logging Interval: 60 Minutes

In this window, you can view or change the basic system information. **Mode of Operation** sets the unit as **bridge** (layer 2) or as **router** (layer 3).   See “Bridge and Routing Modes” on page 44 for more information.

Field Descriptions

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

The Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) features are enabled automatically when you choose a country with a regulatory domain that requires them. The **Country** selection pre-selects and displays only the allowed frequencies for the selected country.

Click the **Configure** button, the **Interfaces** tab, and the **Wireless** sub-tab to see the channel/frequency list for the selected Country.

Note: Units sold in the United States are pre-configured to scan and display only the outdoor frequencies permitted by the FCC. No other **Country** selections, channels, or frequencies can be configured. Units sold outside of the United States and Canada support the selection of a **Country** by the professional installer. If you change the **Country**, a reboot of the unit is necessary for the upgrade to take place.

Dynamic Frequency Selection is not supported in 2.4 GHz operational mode; it is supported on Model 5054-R units only.

Support for the 5.25 – 5.35 GHz and 5.725 – 5.825 GHz frequency bands is provided with a single country selection, **UNITED STATES (US)**, which does not provide DFS capability in these frequency bands.

For a non US-only device, the default country selected is **United Kingdom (GB)**.

Notes: (1) The channel center frequencies are not regulated; only the band edge frequencies are regulated.
(2) If, before upgrade, US was selected as a country for a non US-Only device (which is an incorrect configuration), the country is changed automatically to **United Kingdom** upon upgrade.

See “Appendix A. Country Code/Channels” Tables on page 131 for a list of country codes.

Location

This field can be used to describe the unit’s location, 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 lets you choose one of two operating modes: **Bridge** mode or **Routing** mode.

Temperature Logging Interval

This field lets you configure the temperature logging interval (in 5-minute intervals). See “Monitor: 12) Temperature Log” on page 115 for more information.

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

How long 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

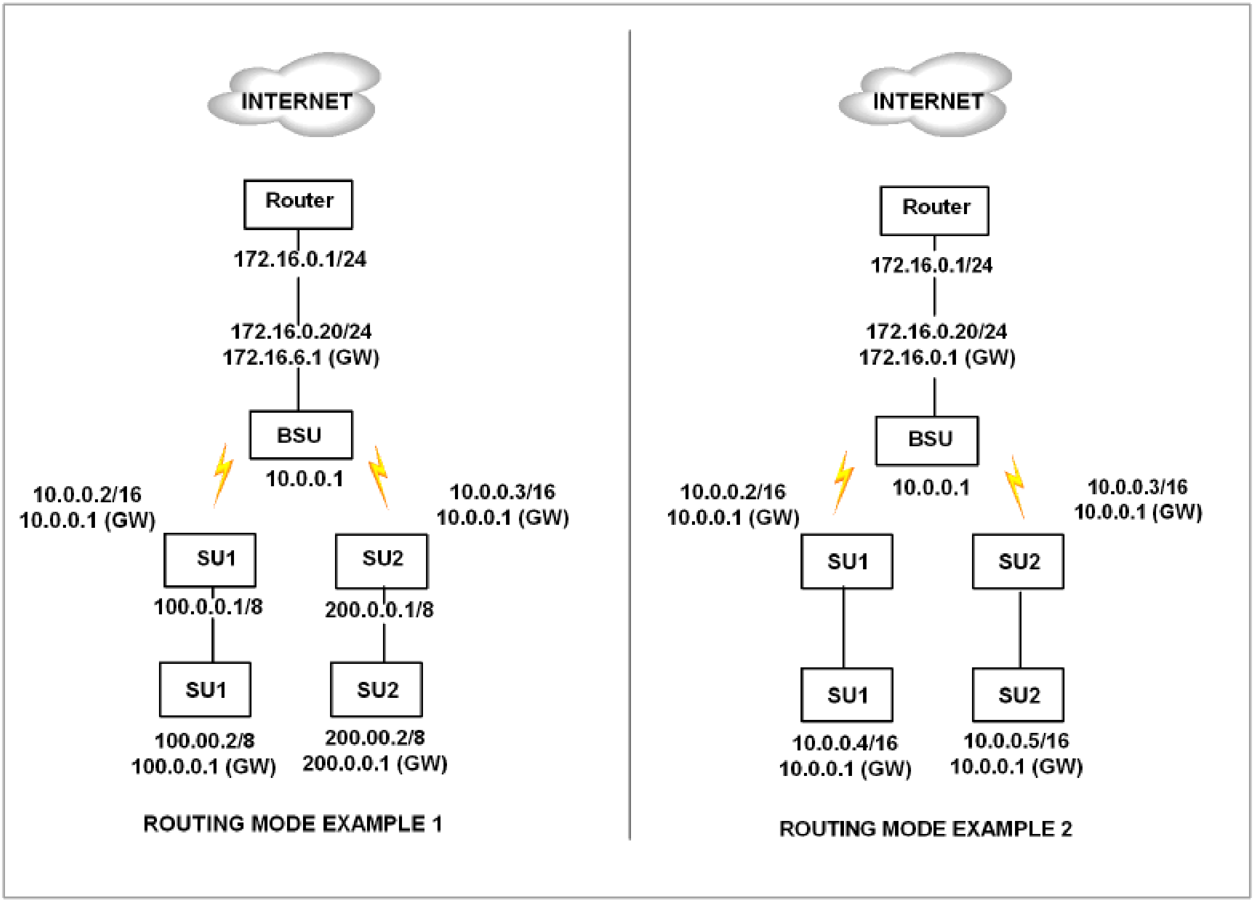
If the average packet size is 1000 bytes, the overhead saved is 1.5%; With a frame size of 64 bytes, the overhead saved is 20%; and for frame sizes of 128 bytes, the saving is 10%. Network researches claim that most network traffic consists of frames smaller than 100 bytes.

In order to support routers behind the SUs with multiple subnets and prevent routing loops, you want individual routes (and more then 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:

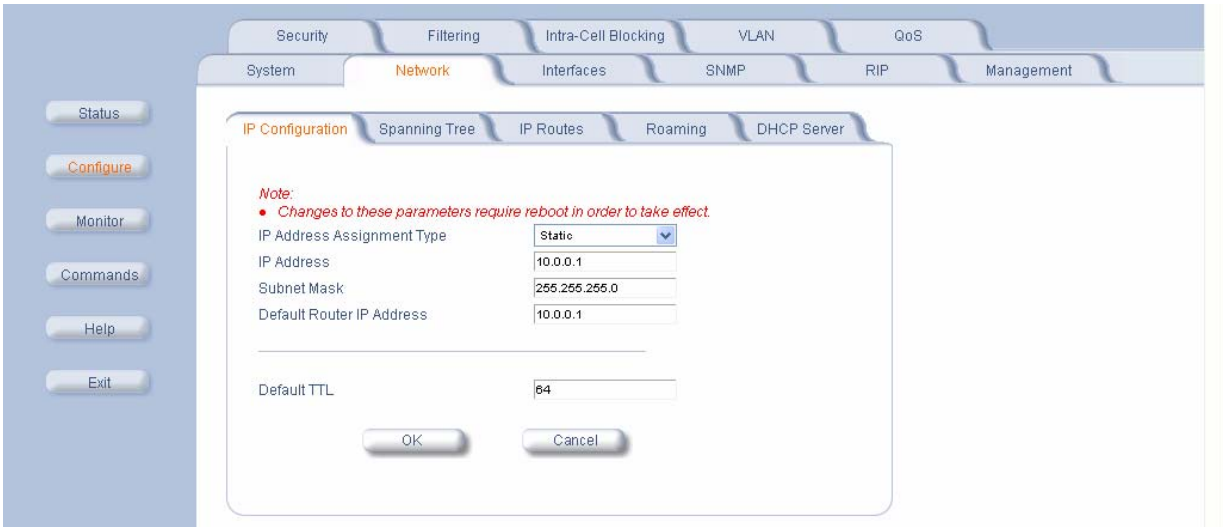
- One of the most important details to pay attention to in Routing mode are the unit's and the PC's default gateways. It is a common mistake to set up the PC's gateway to point to the SU when the SU is in Bridge mode and the BSU is in Routing mode. Always check to make sure the PCs on your network are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

2) Configure 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 the **Configure** button, the **Network** tab, and the **IP Configuration** sub-tab to view and configure local IP address information. See “Setting the IP Address” on page 22 for more information.



Note:
- *Changes to these parameters require reboot in order to take effect.*

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

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” on page 22). 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.

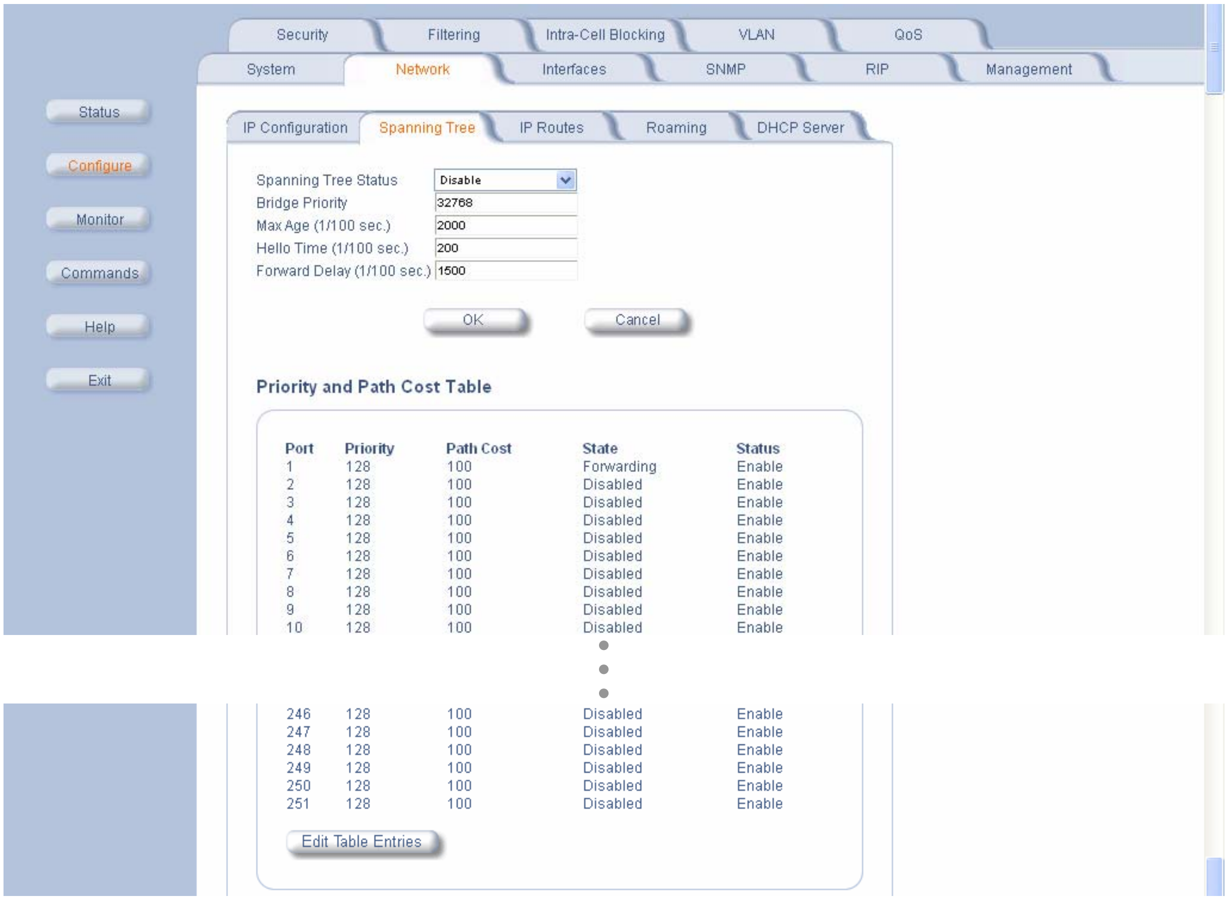
Configure Spanning Tree Options

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 ports 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 units. 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.

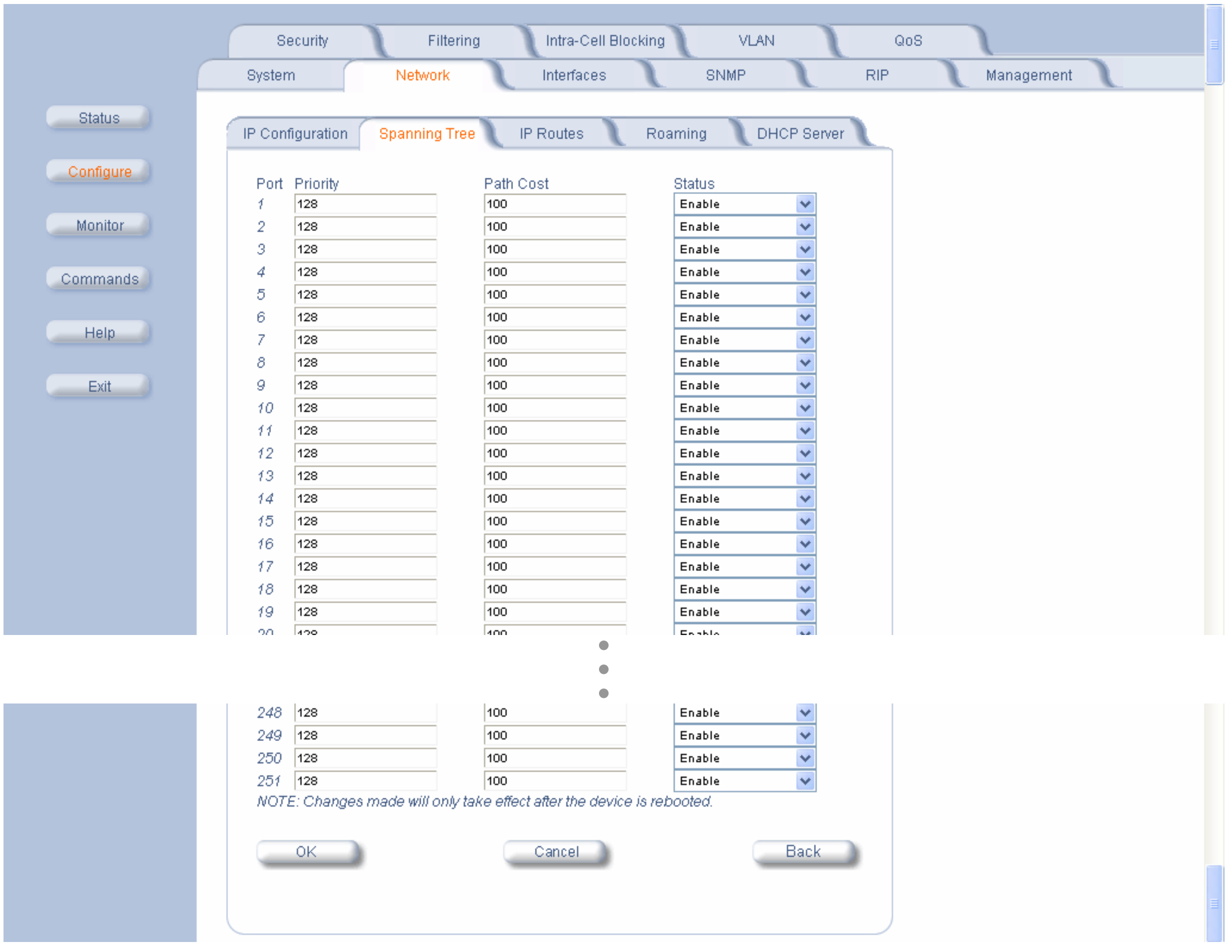


Spanning Tree Status: Disable
Bridge Priority: 32768
Max Age (1/100 sec.): 2000
Hello Time (1/100 sec.): 200
Forward Delay (1/100 sec.): 1500

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

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

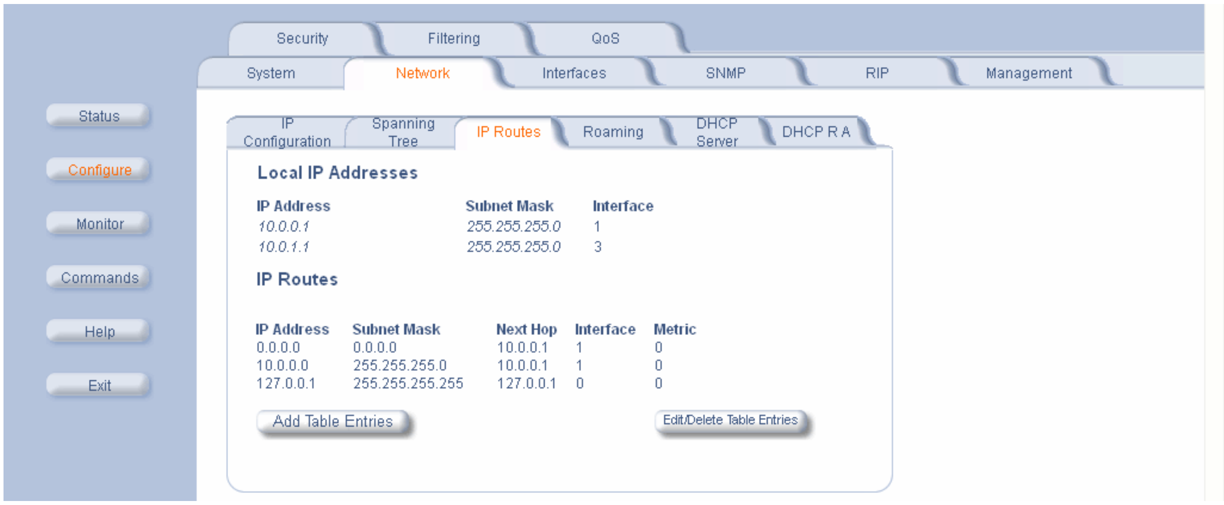


Port	Priority	Path Cost	Status
1	128	100	Enable
2	128	100	Enable
3	128	100	Enable
4	128	100	Enable
5	128	100	Enable
6	128	100	Enable
7	128	100	Enable
8	128	100	Enable
9	128	100	Enable
10	128	100	Enable
11	128	100	Enable
12	128	100	Enable
13	128	100	Enable
14	128	100	Enable
15	128	100	Enable
16	128	100	Enable
17	128	100	Enable
18	128	100	Enable
19	128	100	Enable
20	128	100	Enable
248	128	100	Enable
249	128	100	Enable
250	128	100	Enable
251	128	100	Enable

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

Configure IP Routes (Routing Mode only)

Click the **Configure** button, the **Network** tab and the **IP Routes** sub-tab 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.



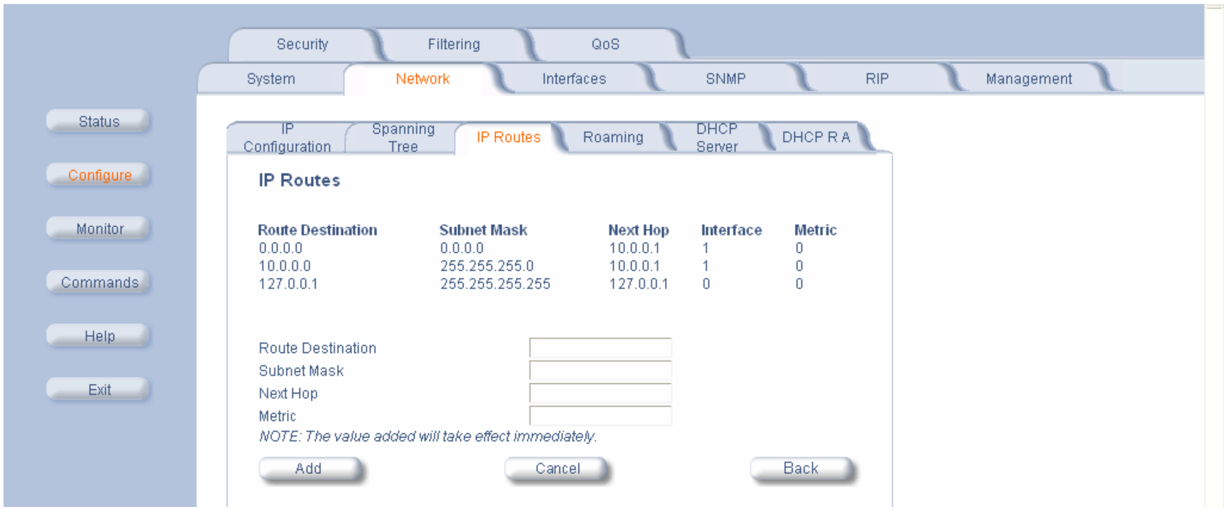
Local IP Addresses

IP Address	Subnet Mask	Interface
10.0.0.1	255.255.255.0	1
10.0.1.1	255.255.255.0	3

IP Routes

IP Address	Subnet Mask	Next Hop	Interface	Metric
0.0.0.0	0.0.0.0	10.0.0.1	1	0
10.0.0.0	255.255.255.0	10.0.0.1	1	0
127.0.0.1	255.255.255.255	127.0.0.1	0	0

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



IP Routes

Route Destination	Subnet Mask	Next Hop	Interface	Metric
0.0.0.0	0.0.0.0	10.0.0.1	1	0
10.0.0.0	255.255.255.0	10.0.0.1	1	0
127.0.0.1	255.255.255.255	127.0.0.1	0	0

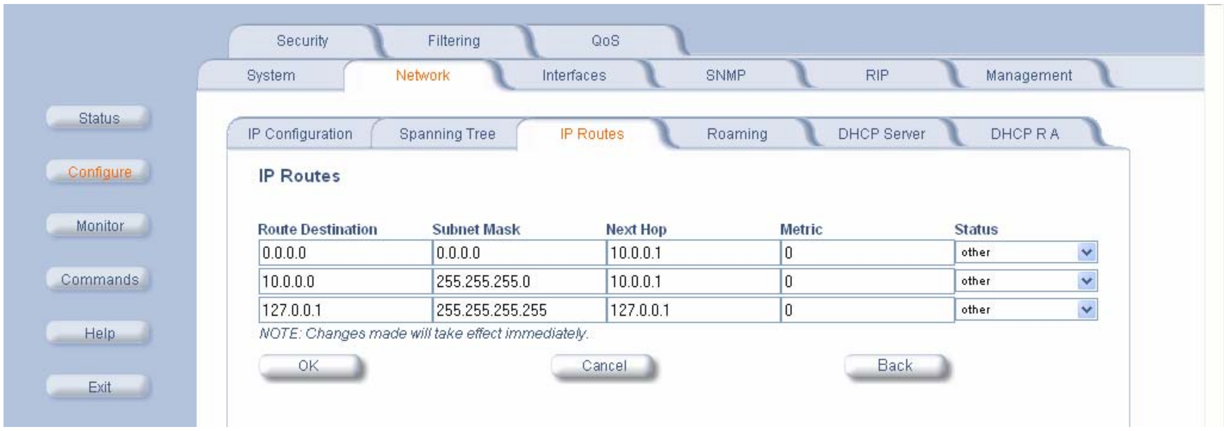
Route Destination
Subnet Mask
Next Hop
Metric

NOTE: The value added will take effect immediately.

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.



IP Routes

Route Destination	Subnet Mask	Next Hop	Metric	Status
0.0.0.0	0.0.0.0	10.0.0.1	0	other
10.0.0.0	255.255.255.0	10.0.0.1	0	other
127.0.0.1	255.255.255.255	127.0.0.1	0	other

NOTE: Changes made will take effect immediately.

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 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

There are two multicast rates to be configured when DDRS is enabled:

Default DDRS Data Rate (*ddrsdefdatarate*):
The data rate at which the BSU starts communication. This parameter is configurable; the default data rate is adapted to the actual condition of the radio link.

Maximum DDRS Data Rate (*ddrsmaxdatarate*):
The maximum data rate at which the device can operate (the default is 36 Mbps)

When an SU roams from BSU-1 to BSU-2, the data rate at which it connects to BSU 2 is the default data rate. If this remains at the factory default of 6 Mbps, there can be issues with the application if it requires more then 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 to the "Maximum DDRS Data 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 of DDRS, see “Dynamic Data Rate Selection (DDRS) Status” on page 58.

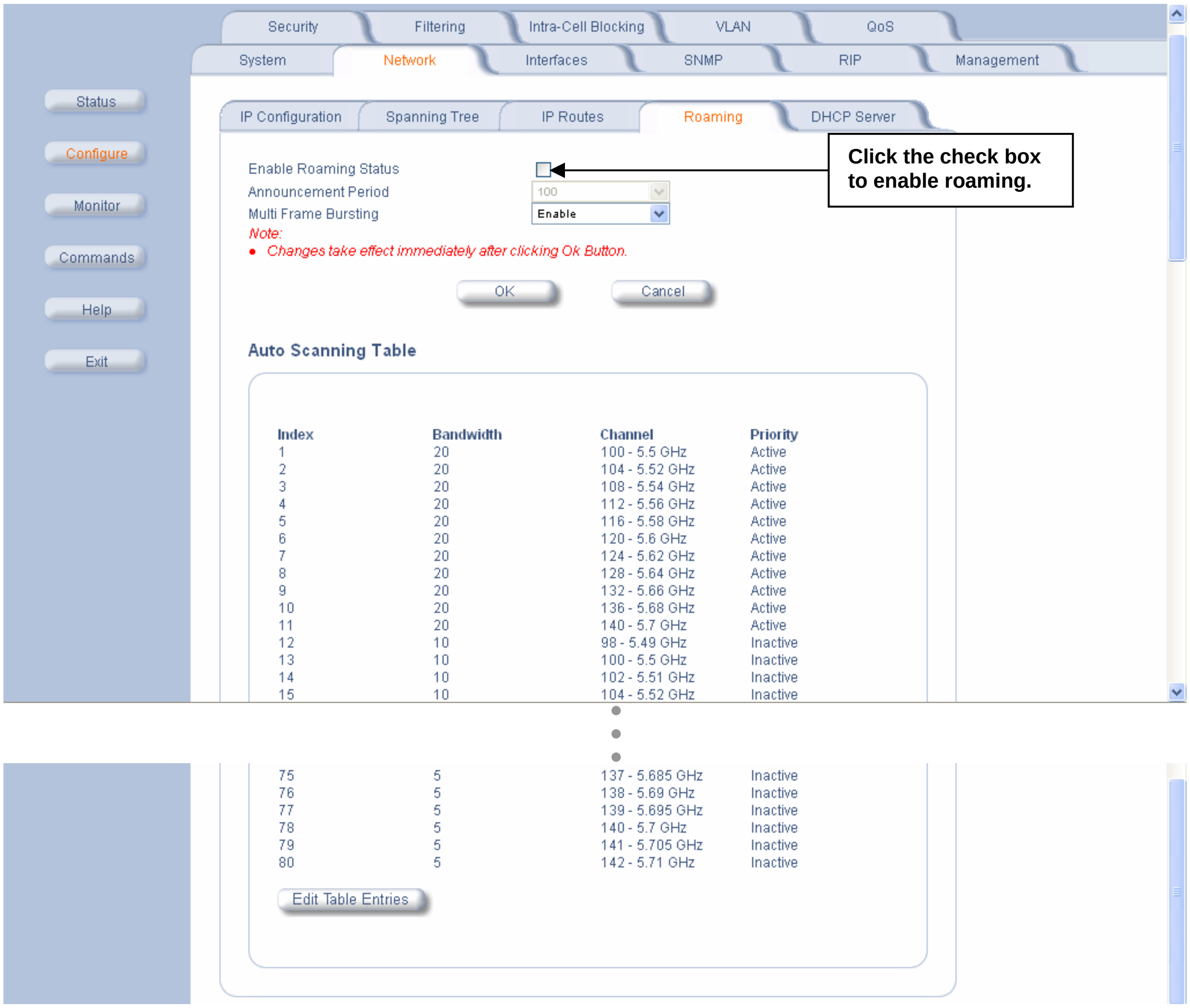
Note: You must know the data rate required for the applications running and you must ensure (during network deployment) that the ranges and RF links can support the necessary data rate. You also must set the default DDRS rate at the capacity necessary for the application so that it connects to the next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

Click the **Configure** button, the **Network** tab and the **Roaming** sub-tab 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 clicking on 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).



Click the check box to enable roaming.

Enable Roaming Status □
Announcement Period 100
Multi Frame Bursting Enable

Note:

- *Changes take effect immediately after clicking Ok Button.*

Auto Scanning Table

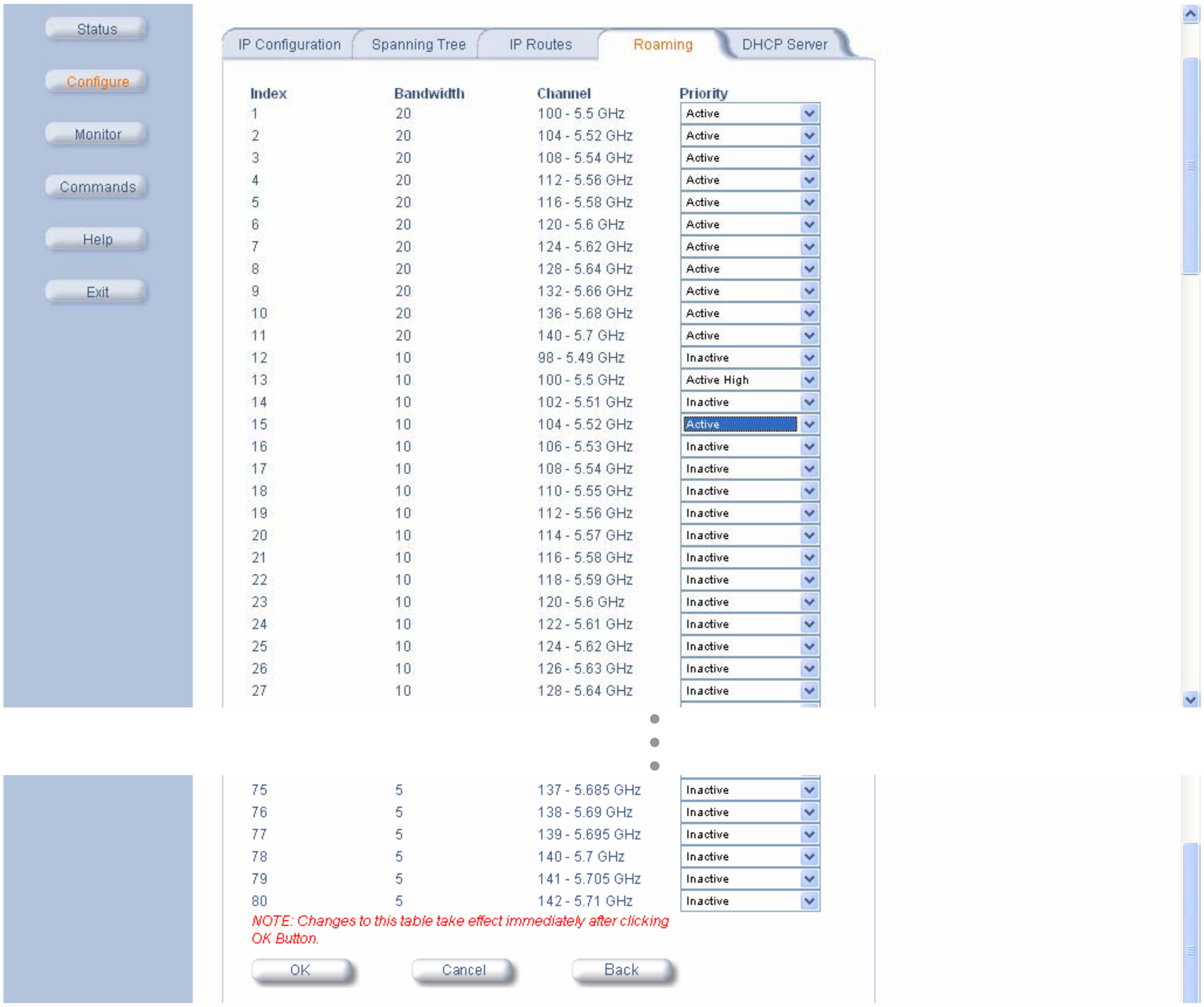
Index	Bandwidth	Channel	Priority
1	20	100 - 5.5 GHz	Active
2	20	104 - 5.52 GHz	Active
3	20	108 - 5.54 GHz	Active
4	20	112 - 5.56 GHz	Active
5	20	116 - 5.58 GHz	Active
6	20	120 - 5.6 GHz	Active
7	20	124 - 5.62 GHz	Active
8	20	128 - 5.64 GHz	Active
9	20	132 - 5.66 GHz	Active
10	20	136 - 5.68 GHz	Active
11	20	140 - 5.7 GHz	Active
12	10	98 - 5.49 GHz	Inactive
13	10	100 - 5.5 GHz	Inactive
14	10	102 - 5.51 GHz	Inactive
15	10	104 - 5.52 GHz	Inactive
●			
●			
●			
75	5	137 - 5.685 GHz	Inactive
76	5	138 - 5.69 GHz	Inactive
77	5	139 - 5.695 GHz	Inactive
78	5	140 - 5.7 GHz	Inactive
79	5	141 - 5.705 GHz	Inactive
80	5	142 - 5.71 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**.



Index	Bandwidth	Channel	Priority
1	20	100 - 5.5 GHz	Active
2	20	104 - 5.52 GHz	Active
3	20	108 - 5.54 GHz	Active
4	20	112 - 5.56 GHz	Active
5	20	116 - 5.58 GHz	Active
6	20	120 - 5.6 GHz	Active
7	20	124 - 5.62 GHz	Active
8	20	128 - 5.64 GHz	Active
9	20	132 - 5.66 GHz	Active
10	20	136 - 5.68 GHz	Active
11	20	140 - 5.7 GHz	Active
12	10	98 - 5.49 GHz	Inactive
13	10	100 - 5.5 GHz	Active High
14	10	102 - 5.51 GHz	Inactive
15	10	104 - 5.52 GHz	Active
16	10	106 - 5.53 GHz	Inactive
17	10	108 - 5.54 GHz	Inactive
18	10	110 - 5.55 GHz	Inactive
19	10	112 - 5.56 GHz	Inactive
20	10	114 - 5.57 GHz	Inactive
21	10	116 - 5.58 GHz	Inactive
22	10	118 - 5.59 GHz	Inactive
23	10	120 - 5.6 GHz	Inactive
24	10	122 - 5.61 GHz	Inactive
25	10	124 - 5.62 GHz	Inactive
26	10	126 - 5.63 GHz	Inactive
27	10	128 - 5.64 GHz	Inactive
⋮			
75	5	137 - 5.685 GHz	Inactive
76	5	138 - 5.69 GHz	Inactive
77	5	139 - 5.695 GHz	Inactive
78	5	140 - 5.7 GHz	Inactive
79	5	141 - 5.705 GHz	Inactive
80	5	142 - 5.71 GHz	Inactive

NOTE: Changes to this table take effect immediately after clicking OK Button.

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.

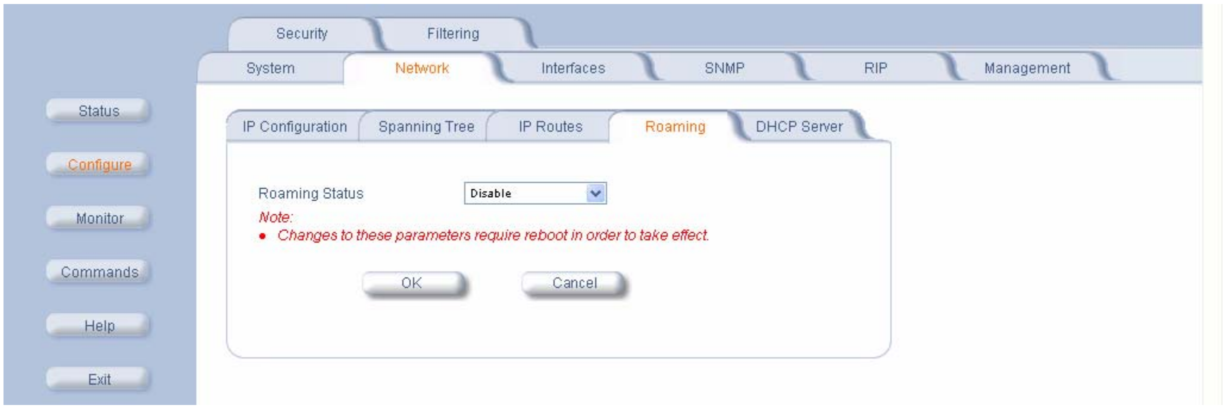
When **Scanning Across Bandwidth** on the SU is enabled (see “Configure Interface Settings” on page 57), the SU supports bandwidth selection of the communications channel of either 20 MHz, 10 MHz, or 5 MHz. This allows the BSUs in the network to be set to different bandwidths while an SU can still roam 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 <u>current</u> 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 100 first since it is configured as high priority and channel 104 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.



Roaming Status	Disable

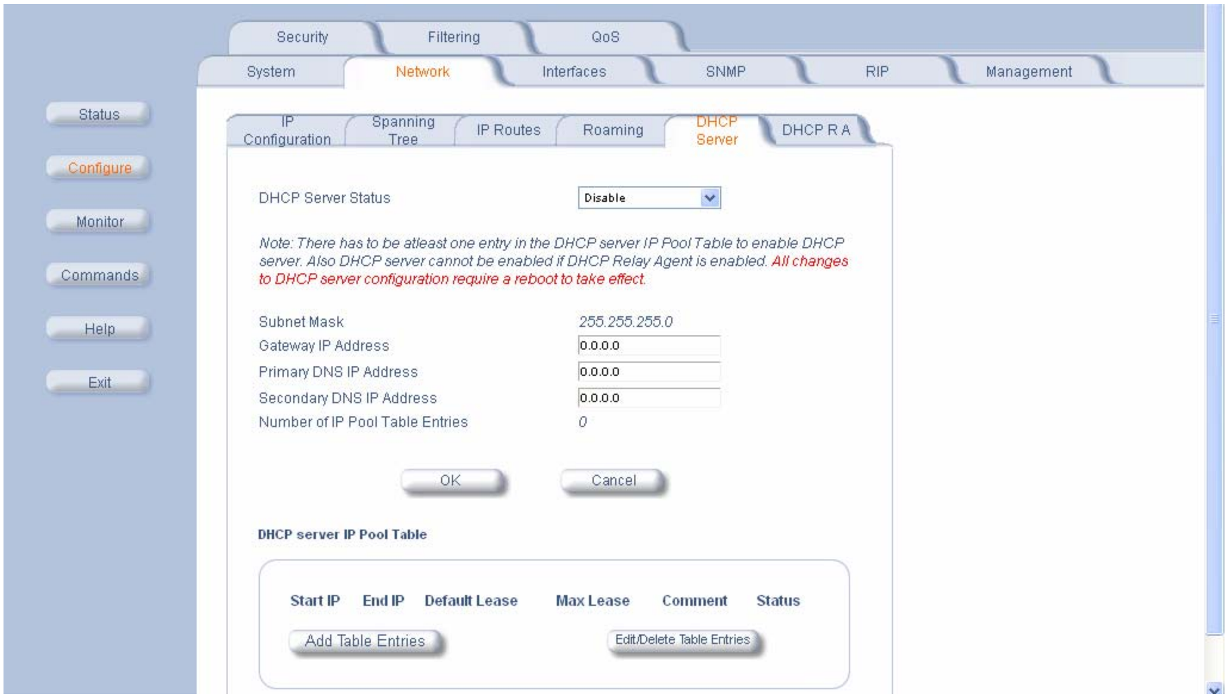
Note:

- Changes to these parameters require reboot in order to take effect.

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

Enable and Configure the DHCP Server

Click the **Configure** button, the **Network** tab and the **DHCP Server** sub-tab 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.



DHCP Server Status	Disable

Note: There has to be atleast 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. All changes to DHCP server configuration require a reboot to take effect.

Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
Primary DNS IP Address	0.0.0.0
Secondary DNS IP Address	0.0.0.0
Number of IP Pool Table Entries	0

DHCP server IP Pool Table

Start IP	End IP	Default Lease	Max Lease	Comment	Status

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 address

Field Descriptions

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

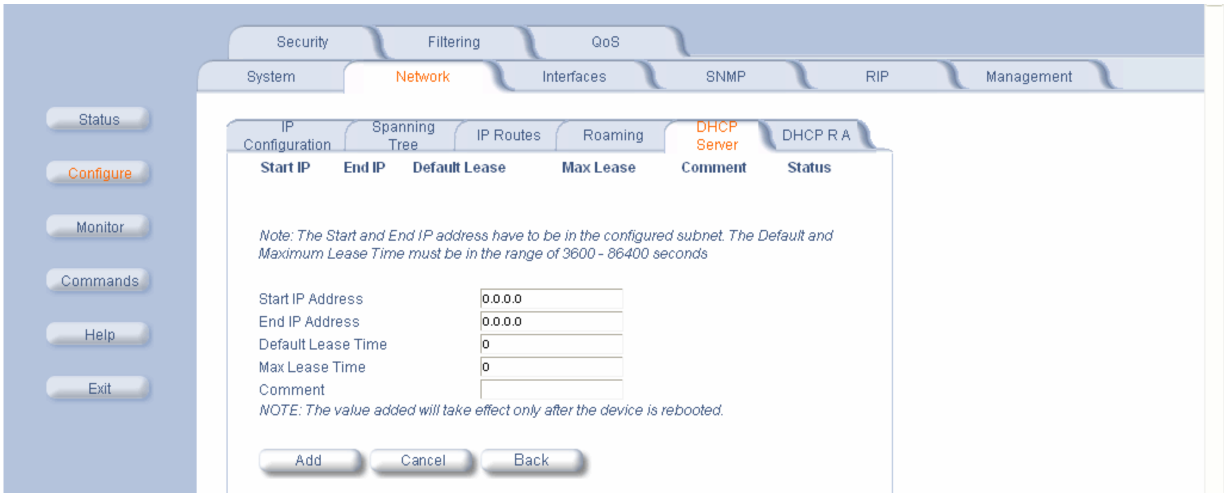
The unit supplies this secondary DNS IP address in the DHCP response.

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 “DHCP Server IP Pool Table” below.

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**.



Start IP	End IP	Default Lease	Max Lease	Comment	Status

Note: The Start and End IP address have to be in the configured subnet. The Default and Maximum Lease Time must be in the range of 3600 - 86400 seconds

Start IP Address	0.0.0.0
End IP Address	0.0.0.0
Default Lease Time	0
Max Lease Time	0
Comment	

NOTE: The value added will take effect only after the device is rebooted.

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

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

Field Descriptions

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

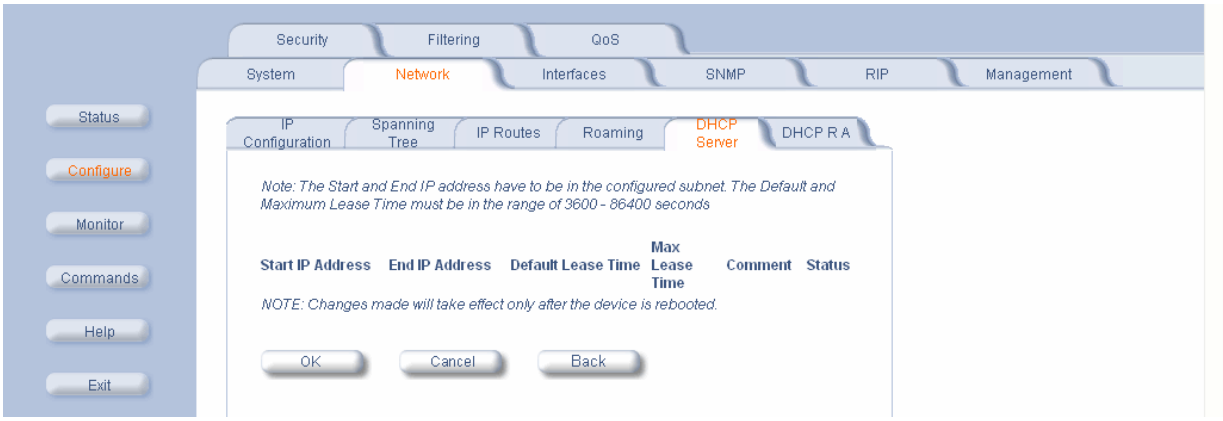
The maximum lease time for IP addresses in the address pool. The value is 3600-86400 seconds.

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**.



Note: The Start and End IP address have to be in the configured subnet. The Default and Maximum Lease Time must be in the range of 3600 - 86400 seconds

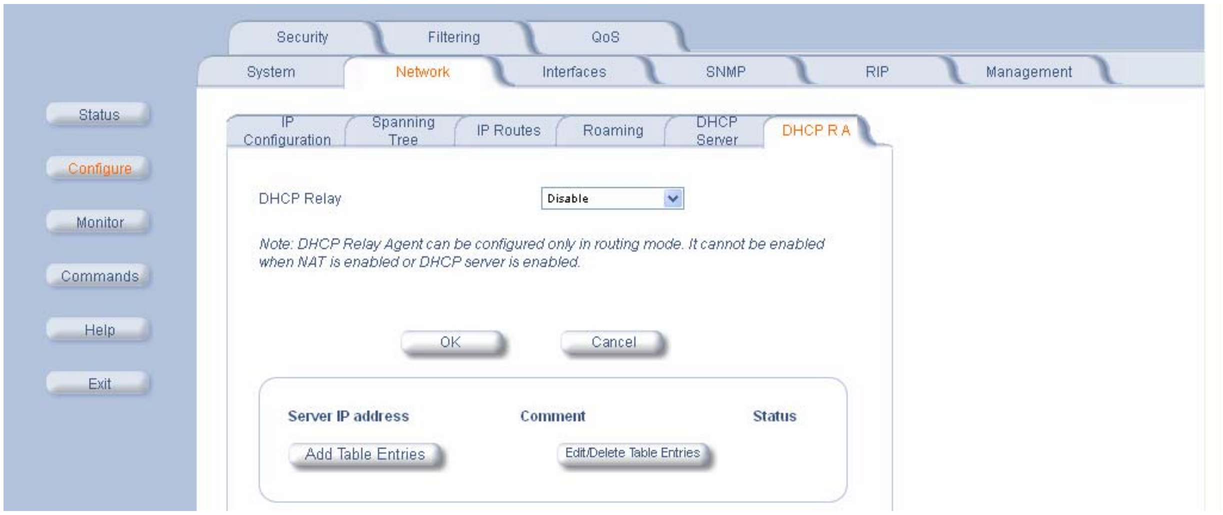
Start IP Address	End IP Address	Default Lease Time	Max Lease Time	Comment	Status

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

Enable the DHCP Relay Agent (Routing mode only)

Click the **Configure** button, the **Network** tab, and the **DHCP RA** sub-tab to enable the unit's DHCP Relay Agent. When enabled, the DHCP relay agent forwards DHCP requests to the set DHCP server.

Note that DHCP Relay Agent parameters are configurable only in **Routing** mode.



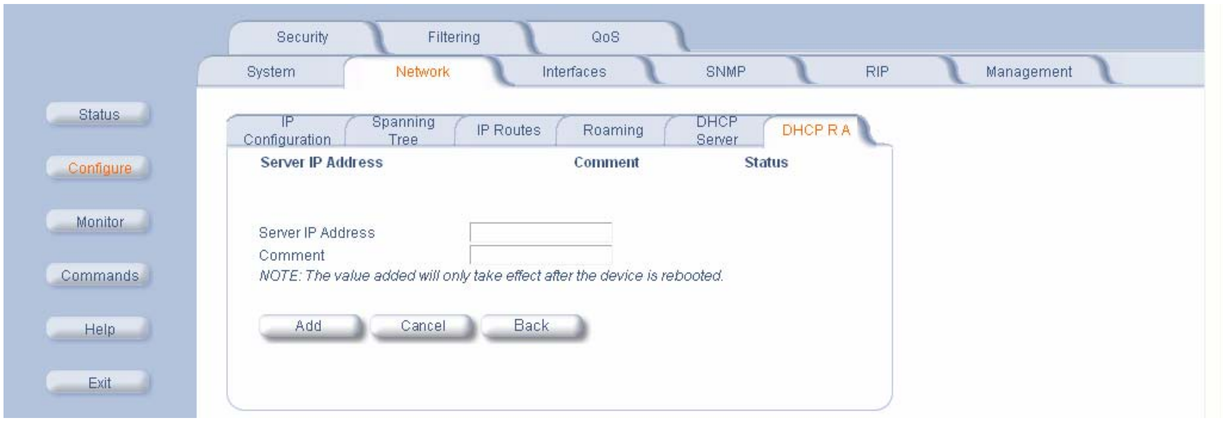
DHCP Relay: Disable

Note: DHCP Relay Agent can be configured only in routing mode. It cannot be enabled when NAT is enabled or DHCP server is enabled.

Server IP address	Comment	Status

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.



Server IP Address **Comment** **Status**

Server IP Address

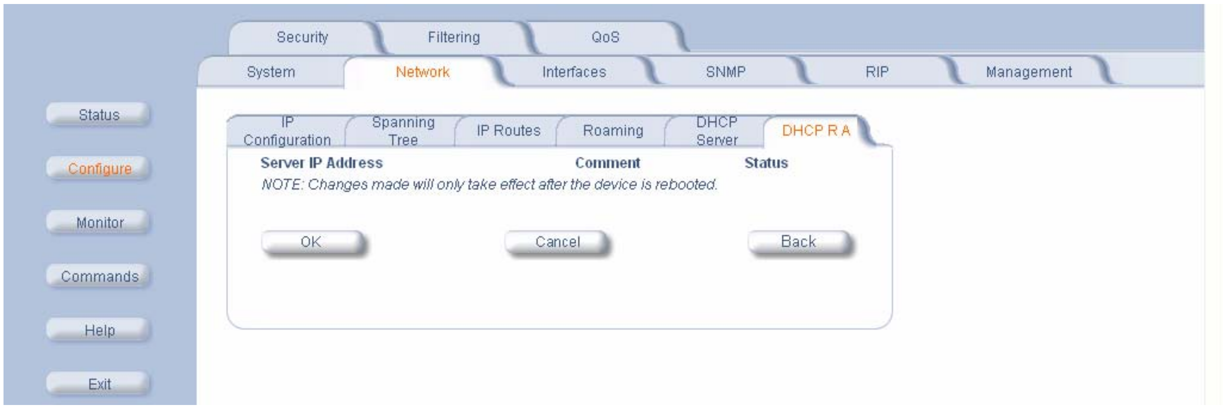
Comment

NOTE: The value added will only take effect after the device is rebooted.

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**.



Server IP Address **Comment** **Status**

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

3) Configure Interface Settings

Configure the Wireless Interface

To configure the wireless interface, click the **Configure** button followed by the **Interfaces** tab; then click the **Wireless** sub-tab.

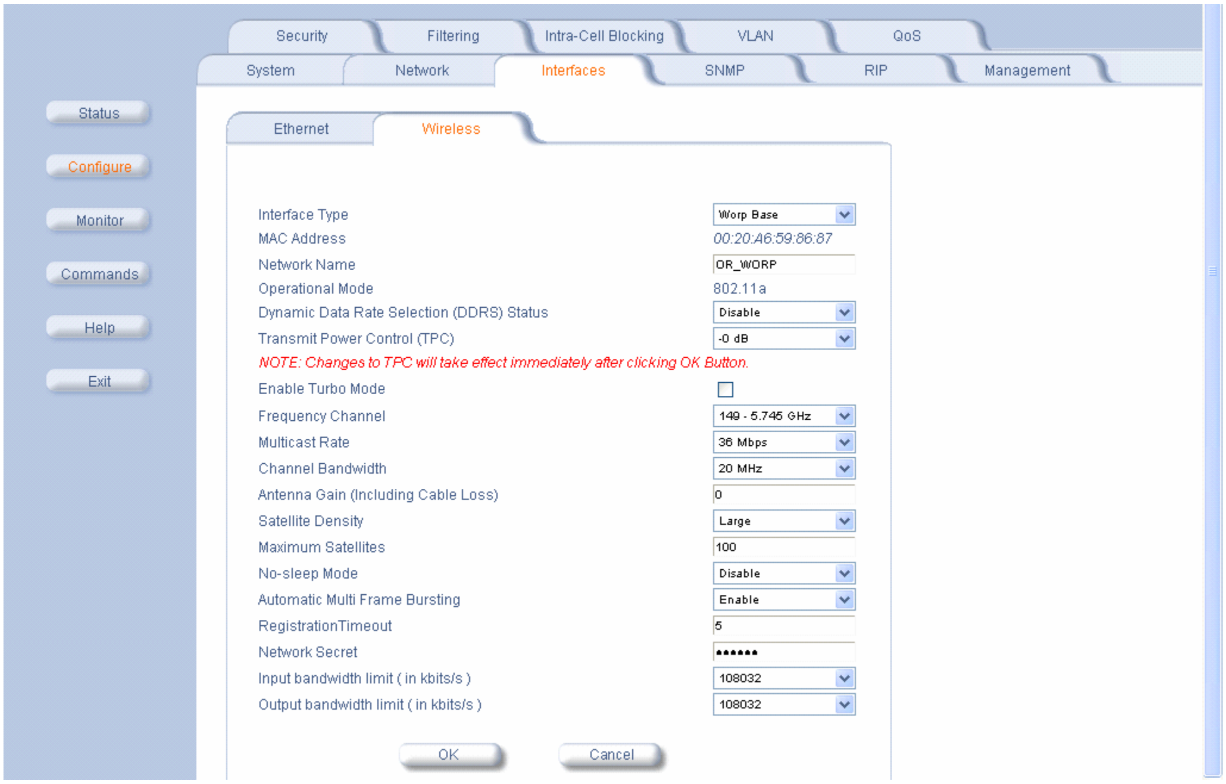
For Base Station units, the wireless interface can be placed in either **WORP Base** or **WORP Satellite** mode (selected from the **Interface Type** drop-down box). SUs can be placed only in WORP Satellite mode. The wireless interface settings depend upon whether the mode is Base or Satellite.

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 units send an RTS, if another unit 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, and for countries different than the US:

Base Mode – US Country



Interface Type	Worp Base
MAC Address	00:20:A6:59:86:87
Network Name	OR_WORP
Operational Mode	802.11a
Dynamic Data Rate Selection (DDRS) Status	Disable
Transmit Power Control (TPC)	-0 dB

NOTE: Changes to TPC will take effect immediately after clicking OK Button.

Enable Turbo Mode	□
Frequency Channel	149 - 5.745 GHz
Multicast Rate	36 Mbps
Channel Bandwidth	20 MHz
Antenna Gain (Including Cable Loss)	0
Satellite Density	Large
Maximum Satellites	100
No-sleep Mode	Disable
Automatic Multi Frame Bursting	Enable
RegistrationTimeout	5
Network Secret	••••••
Input bandwidth limit (in kbits/s)	108032
Output bandwidth limit (in kbits/s)	108032

Field Descriptions

Interface Type

The interface type can be **WORP Satellite** or **WORP Base**.

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 (not configurable)

This field indicates the operational mode of the unit – 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. For the 5054-R, this field shows 11a; for the 2454-R, this field shows 11g.

Dynamic Data Rate Selection (DDRS) Status

The WORP **Dynamic Data Rate Selection (DDRS)** lets the BSU and SUs monitor the remote average signal-to-noise ratio (SNR) and to adjust the data rate to an optimal value (to provide best possible throughput) according to the current communication conditions 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 signal to noise ratio (SNR) in dB. SNR is calculated then averaged:

SNR [dB] = signal level [dBm] – noise level [dBm]

This information lets the sender adjust the transmission data rate to the optimal level to provide the best possible throughput.

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

Note: DDRS threshold values must be configured in the BSU and SUs separately through the CLI or the SNMP interface.

Both the BSU and the SU 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.

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.

Transmit Power Control

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	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 5054-R. **Turbo Mode** uses three adjacent channels for wireless data transfer.

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 "Appendix A. Country Codes/Channels" on page 131 for channelization information.

For countries in which DFS is not enabled, the **Frequency Channel** list displays only the channels and frequencies allowed for the selected country.

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 rate than the BSU because timeouts will occur at the Base Station and communication will fail.

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

5 MHz	10 MHz	20 MHz
1.5	3	6
2.25	4,5	9
3	6	12
4.5	9	18
6	12	24
9	18	36
12	24	48
13.5	27	54

Channel Bandwidth

This field is used to change bandwidth; values are 5MHz, 10 MHz, or 20 MHz, as well as 40 MHz when Turbo mode is enabled (5054-R only). To change a BSU's channel bandwidth (for example from 20 MHz to 5 MHz), change the channel bandwidth of any SU connected to the BSU before changing the BSU's 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 Base Station 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” on page 96 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 “Disable” on the drop-down box of the **Configure**, **Network**, **Roaming** sub-tab (see “BSU Screen” on page 53). 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)” on page 30). This scenario is set by enabling Multi-Frame burst on the drop-down box of the **Configure**, **Network**, **Roaming** sub-tab (see “BSU Screen” on page 52) 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)” on page 30). This scenario is set by enabling Multi-Frame burst on the drop-down box of the **Configure**, **Network**, **Roaming** sub-tab (see “BSU Screen” on page 52) 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.

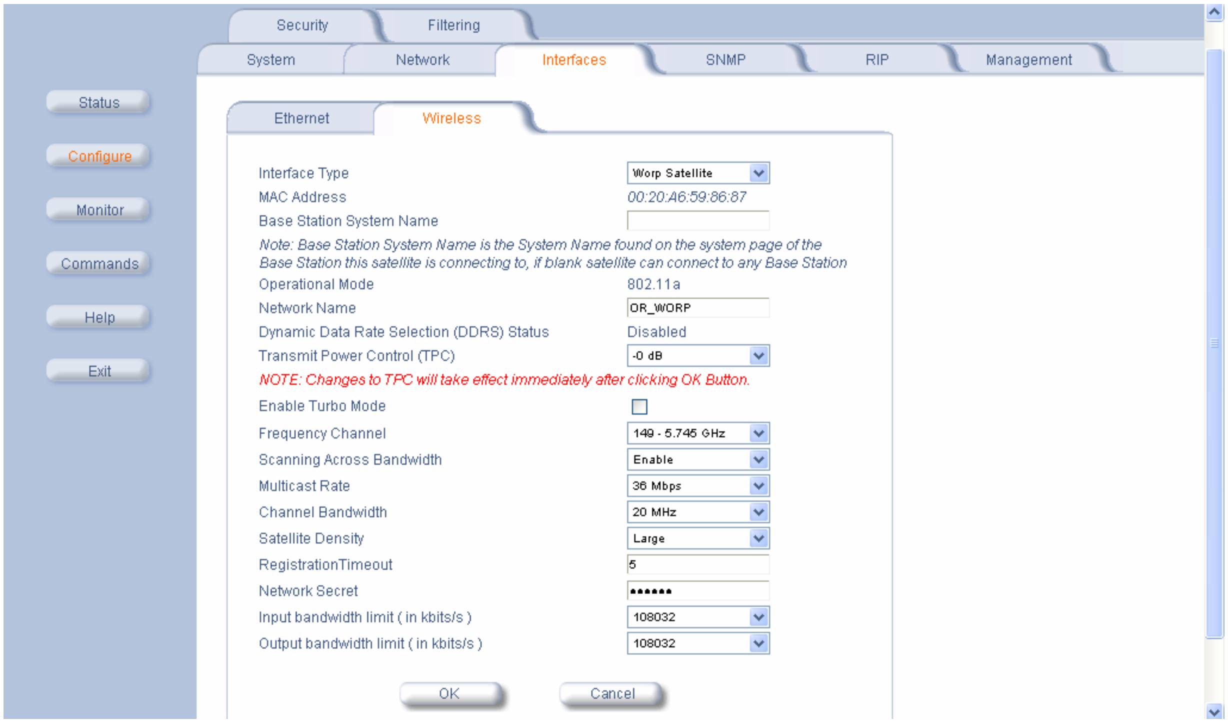
Network Secret

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 to 108,064 Kbps.

Satellite Mode – US Country



Interface Type	Worp Satellite
MAC Address	00:20:A6:59:86:87
Base Station System Name	

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

Operational Mode	802.11a
Network Name	OR_WORP
Dynamic Data Rate Selection (DDRS) Status	Disabled
Transmit Power Control (TPC)	-0 dB

NOTE: Changes to TPC will take effect immediately after clicking OK Button.

Enable Turbo Mode	□
Frequency Channel	149 - 5.745 GHz
Scanning Across Bandwidth	Enable
Multicast Rate	36 Mbps
Channel Bandwidth	20 MHz
Satellite Density	Large
RegistrationTimeout	5
Network Secret	••••••
Input bandwidth limit (in kbits/s)	108032
Output bandwidth limit (in kbits/s)	108032

Field Descriptions

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)

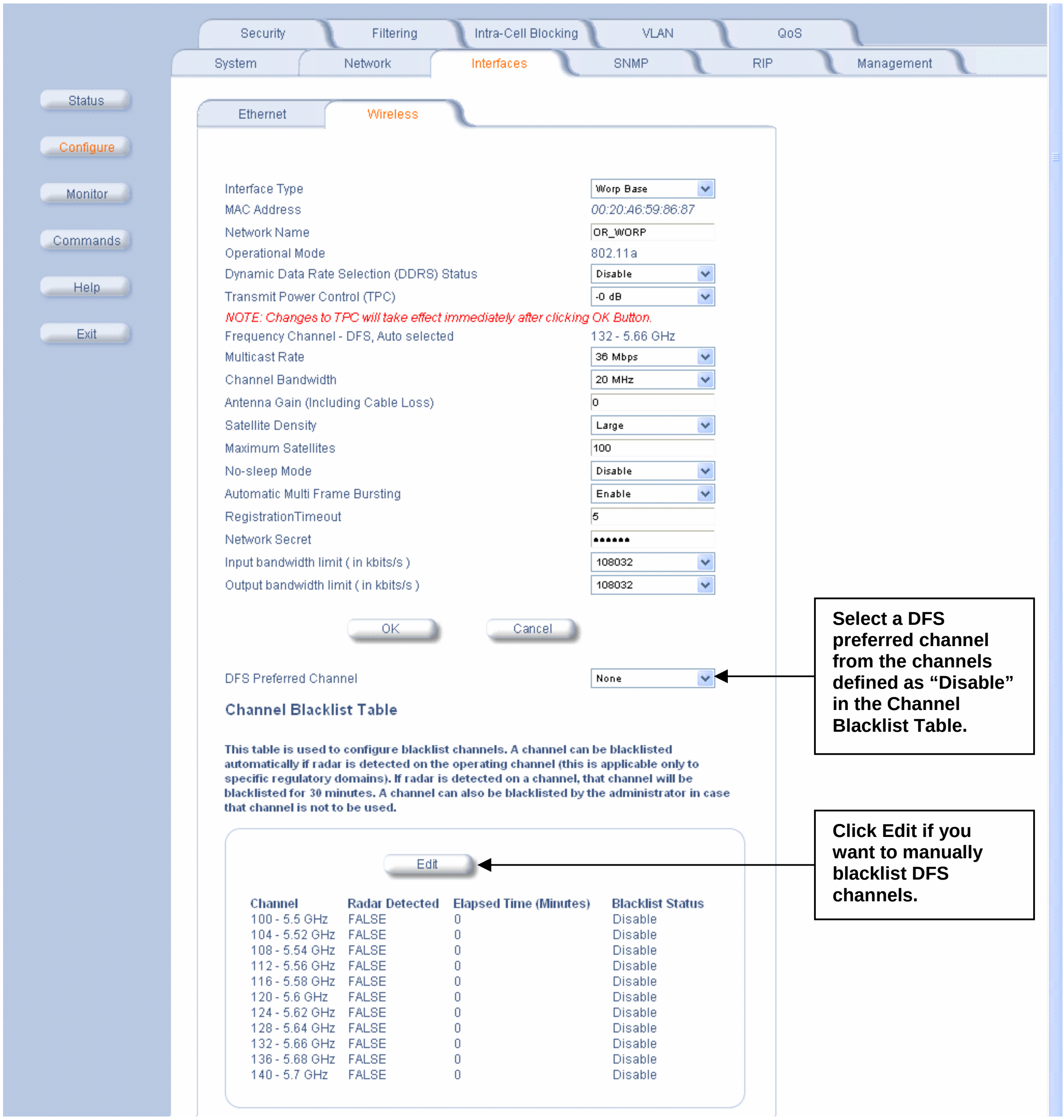
The name found on the system page of the BSU to which this SU is connecting. This parameter can be used as an added security measure, and when there are multiple BSUs in the network and you want an SU to register with only one when it may actually have adequate signal strength for either. The **System 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 Base Station 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.

Base Mode – Non-US Country



Interface Type	Worp Base
MAC Address	00:20:A6:59:86:87
Network Name	OR_WORP
Operational Mode	802.11a
Dynamic Data Rate Selection (DDRS) Status	Disable
Transmit Power Control (TPC)	-0 dB

NOTE: Changes to TPC will take effect immediately after clicking OK Button.

Frequency Channel - DFS, Auto selected	132 - 5.66 GHz
Multicast Rate	36 Mbps
Channel Bandwidth	20 MHz
Antenna Gain (Including Cable Loss)	0
Satellite Density	Large
Maximum Satellites	100
No-sleep Mode	Disable
Automatic Multi Frame Bursting	Enable
RegistrationTimeout	5
Network Secret	••••••
Input bandwidth limit (in kbits/s)	108032
Output bandwidth limit (in kbits/s)	108032

DFS Preferred Channel: None

Select a DFS preferred channel from the channels defined as “Disable” in the Channel Blacklist Table.

Channel Blacklist Table

This table is used to configure blacklist channels. A channel can be blacklisted automatically if radar is detected on the operating channel (this is applicable only to specific regulatory domains). If radar is detected on a channel, that channel will be blacklisted for 30 minutes. A channel can also be blacklisted by the administrator in case that channel is not to be used.

Click Edit if you want to manually blacklist DFS channels.

Channel	Radar Detected	Elapsed Time (Minutes)	Blacklist Status
100 - 5.5 GHz	FALSE	0	Disable
104 - 5.52 GHz	FALSE	0	Disable
108 - 5.54 GHz	FALSE	0	Disable
112 - 5.56 GHz	FALSE	0	Disable
116 - 5.58 GHz	FALSE	0	Disable
120 - 5.6 GHz	FALSE	0	Disable
124 - 5.62 GHz	FALSE	0	Disable
128 - 5.64 GHz	FALSE	0	Disable
132 - 5.66 GHz	FALSE	0	Disable
136 - 5.68 GHz	FALSE	0	Disable
140 - 5.7 GHz	FALSE	0	Disable

Field Descriptions

The differences between the BSU Wireless interface screen for a non-US country and the equivalent screen for the US are:

- There is no **Turbo Mode**.
- **Frequency Channel** is not configurable. Instead the channel is auto-selected by the DFS process.

All the other fields that appear in the US screen for the BSU are applicable. There are also these additional fields:

DFS Preferred Channel

A single DFS preferred frequency channel on the BSU is provided so that when the DFS process starts the BSU will first try the DFS preferred channel before scanning all the other active channels in the DFS channel list. The DFS preferred channel must be selected from those channels indicated as “Disable” in the DFS channel blacklist list. It is not possible to select the DFS preferred channel from those channels in the DFS channel blacklist list indicated as “Enable”.

Channel Blacklist Table

The DFS channel blacklist table shows all the channels in the current bandwidth and specifies the blacklist status of each channel as one of the following:

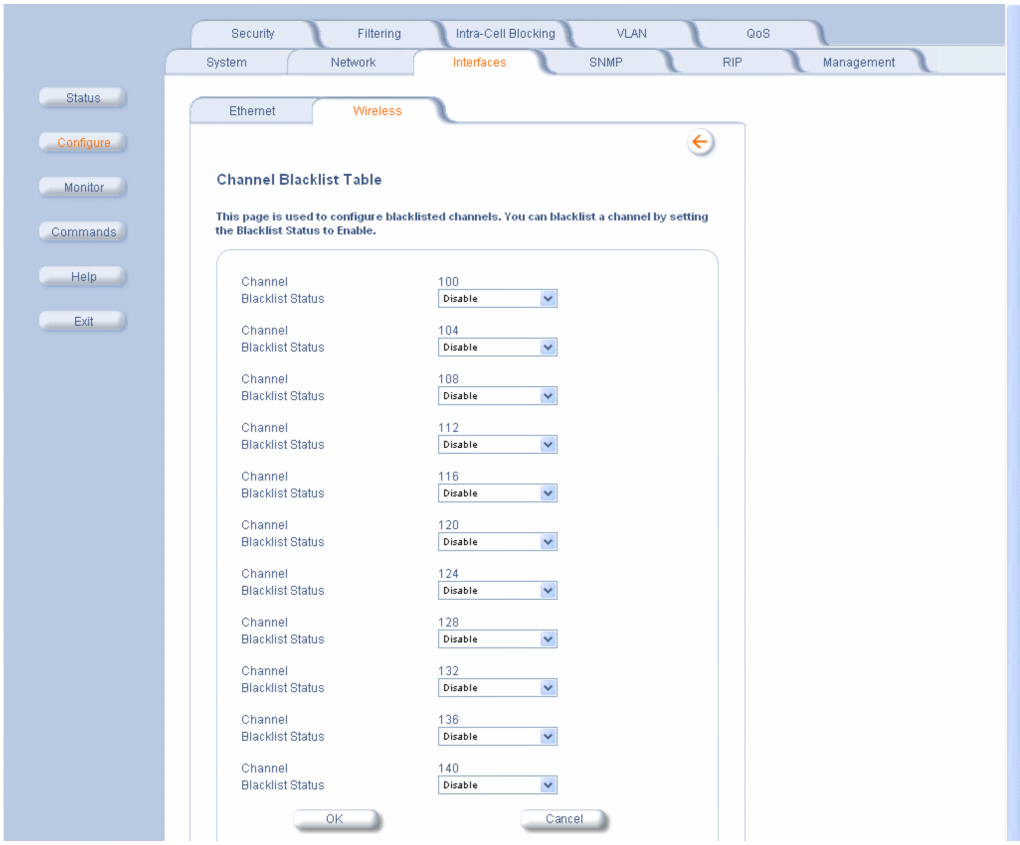
- Enable – Channels that are made unavailable either for a certain period of time upon detection of a radar signal, or permanently because the operator has configured them as blacklisted. These channels are skipped over during DFS channel selection.
- Disable – Channels that are to be scanned during DFS.

Edit Entries to the Channel Blacklist Table

In accordance to the EN301-893 non-occupancy rule, when a radar signal is detected on any active channel, the blacklist status of that channel will change to “Enable” and the Radar Detected status will change to TRUE (see previous figure). The channel will not be used for a period of 30 minutes after the radar signal has been detected. The elapsed time is also shown in the DFS channel blacklist table. When the elapsed time for a channel in the blacklist is greater than or equal to 30 minutes, the blacklist status of the channel will change to Disable and the Radar Detected and Elapsed Time fields will change accordingly.

If an operator knows in advance on which channels a radar signal is likely to exist, those channels can be blacklisted and hence they will be skipped during DFS. Similarly, if the operator knows of channels where a radar signal is unlikely to be detected, those channels can be defined as active and hence they will be scanned during DFS. This makes the whole process more efficient.

When you click **Edit** the channel blacklist table screen appears. Here you can manually configure each channel as “active” (Blacklist Status = Disable) or “blacklisted” (Blacklist Status = Enable). Enter your changes and click **OK**. To go back, click on the arrow button.

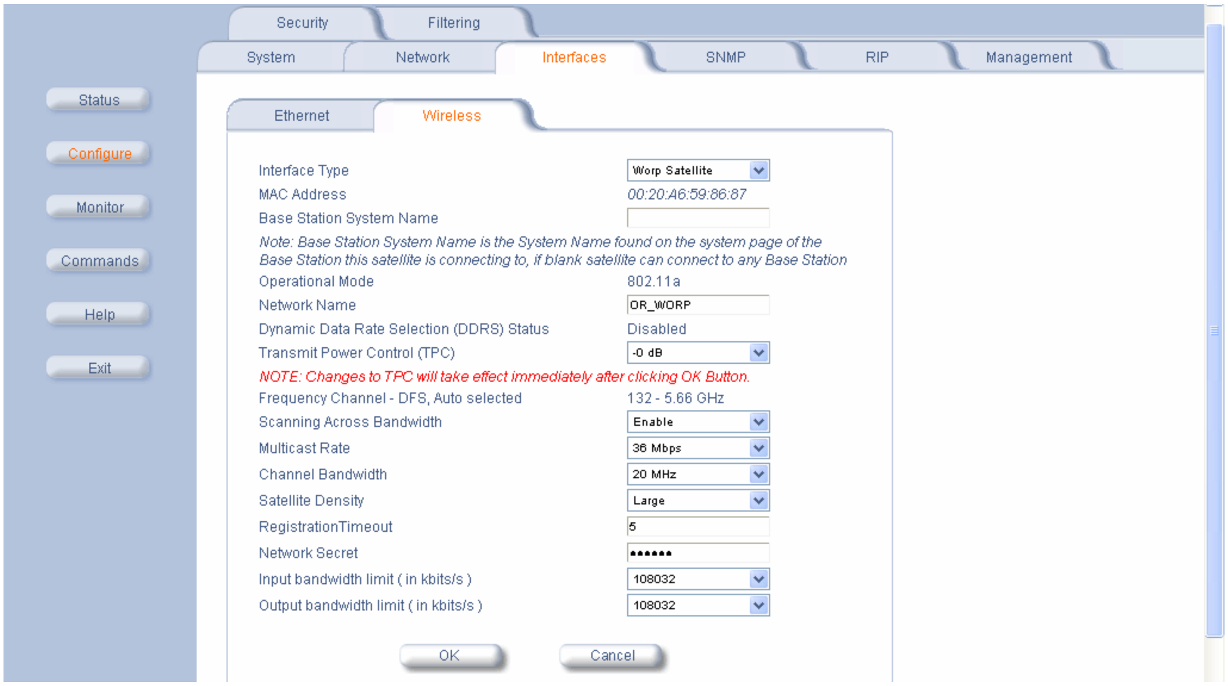


Channel Blacklist Table

This page is used to configure blacklisted channels. You can blacklist a channel by setting the Blacklist Status to Enable.

Channel	100
Blacklist Status	Disable
Channel	104
Blacklist Status	Disable
Channel	108
Blacklist Status	Disable
Channel	112
Blacklist Status	Disable
Channel	116
Blacklist Status	Disable
Channel	120
Blacklist Status	Disable
Channel	124
Blacklist Status	Disable
Channel	128
Blacklist Status	Disable
Channel	132
Blacklist Status	Disable
Channel	136
Blacklist Status	Disable
Channel	140
Blacklist Status	Disable

Satellite Mode – Non-US Country



Interface Type: Worp Satellite
MAC Address: 00:20:A6:59:86:87
Base Station System Name:
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
Operational Mode: 802.11a
Network Name: OR_WORP
Dynamic Data Rate Selection (DDRS) Status: Disabled
Transmit Power Control (TPC): -0 dB
NOTE: Changes to TPC will take effect immediately after clicking OK Button.
Frequency Channel - DFS, Auto selected: 132 - 5.66 GHz
Scanning Across Bandwidth: Enable
Multicast Rate: 36 Mbps
Channel Bandwidth: 20 MHz
Satellite Density: Large
RegistrationTimeout: 5
Network Secret: ••••••
Input bandwidth limit (in kbits/s): 108032
Output bandwidth limit (in kbits/s): 108032

Field Descriptions

The differences between the SU Wireless interface screen for a non-US country and the equivalent screen for the US are:

- There is no **Turbo Mode**.
- **Frequency Channel** is not configurable. Instead the channel is auto-selected by the DFS process.

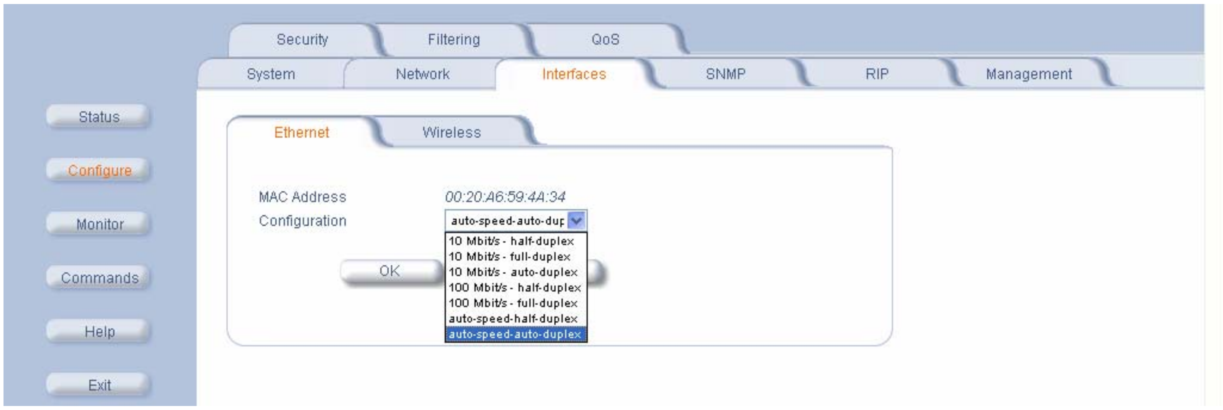
All the other fields that appear in the US screen for the SU are applicable.

Notes:

- Turbo mode is available only when the specified **Country** is US and only for the 5054-R.
- The list of parameters to configure for registration of the SU on a Base Station are:
  - Base Station System Name (when used)
  - Channel Frequency
  - Encryption (when used)
  - Network Secret

Configure the Ethernet Interface

To set the Ethernet speed, duplex mode, and input and output bandwidth limits, click the **Configure** button, the **Interfaces** tab, and the **Ethernet** sub-tab.



MAC Address 00:20:A6:59:44:34
Configuration auto-speed-auto-duplex

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**.

4) Configure SNMP Parameters

Click the **Configure** button and the **SNMP** tab 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.

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.

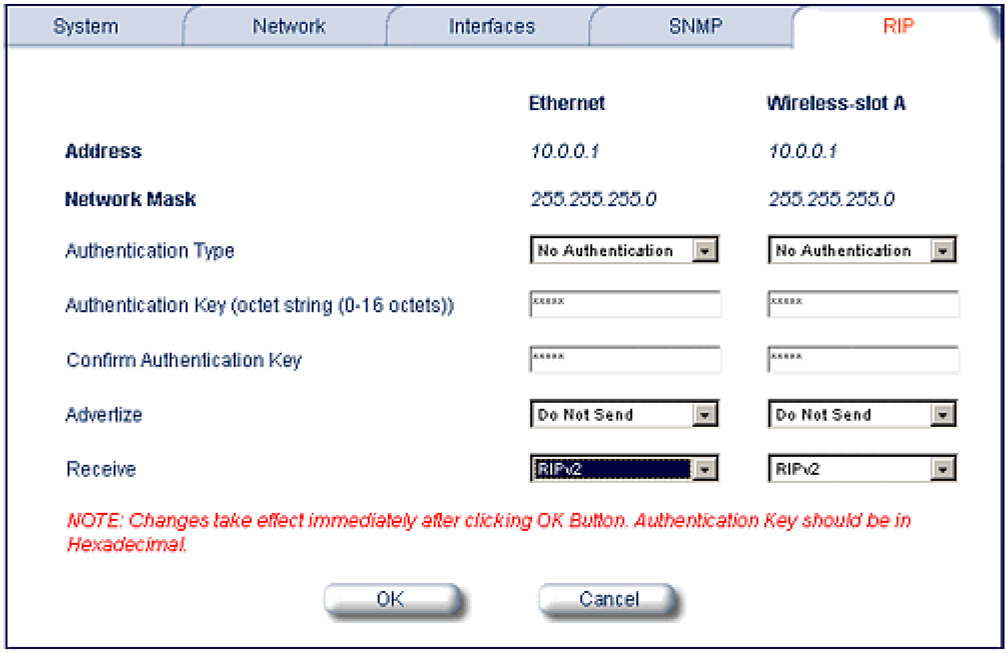
Edit/Delete Entries to the Trap Host Table

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

5) Configure 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 all 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.



	Ethernet	Wireless-slot A
Address	10.0.0.1	10.0.0.1
Network Mask	255.255.255.0	255.255.255.0
Authentication Type	No Authentication	No Authentication
Authentication Key (octet string (0-16 octets))	*****	*****
Confirm Authentication Key	*****	*****
Advertize	Do Not Send	Do Not Send
Receive	RIPv2	RIPv2

NOTE: Changes take effect immediately after clicking OK Button. Authentication Key should be in Hexadecimal.

Note the following:

- There is no option to turn off receiving RIP advertisements. Once the unit is in **Routing** mode, it receives RIP updates when there is another RIP-enabled device advertising on your network. Although it receives and processes these updates, it does not further propagate these updates unless configured to advertise RIP.
- 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
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

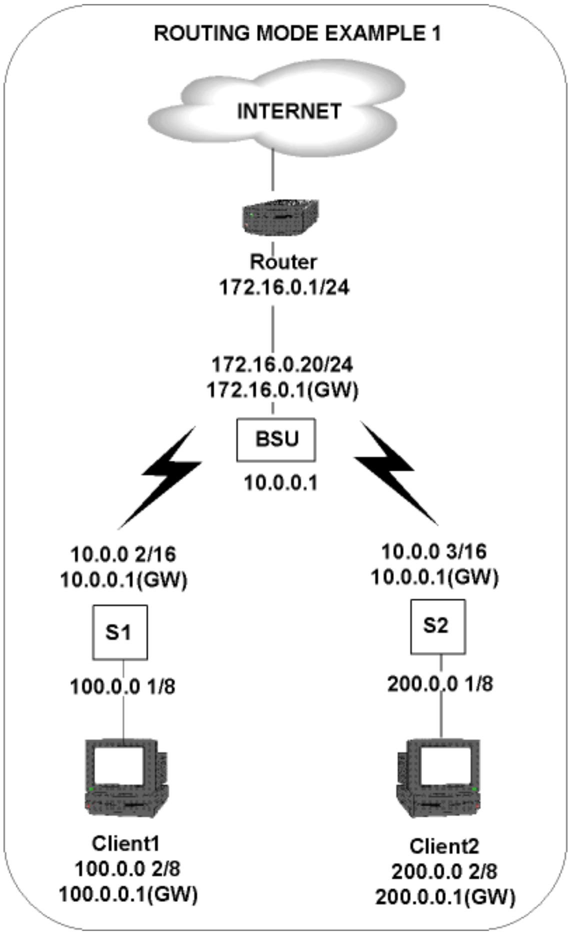
```
0.0.0.0       172.16.0.1    metric 1
172.16.0.0    172.16.0.20   metric 1
10.0.0.0      10.0.0.1      metric 1
100.0.0.0     10.0.0.2      metric 2
200.0.0.0     10.0.0.3      metric 2
```

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

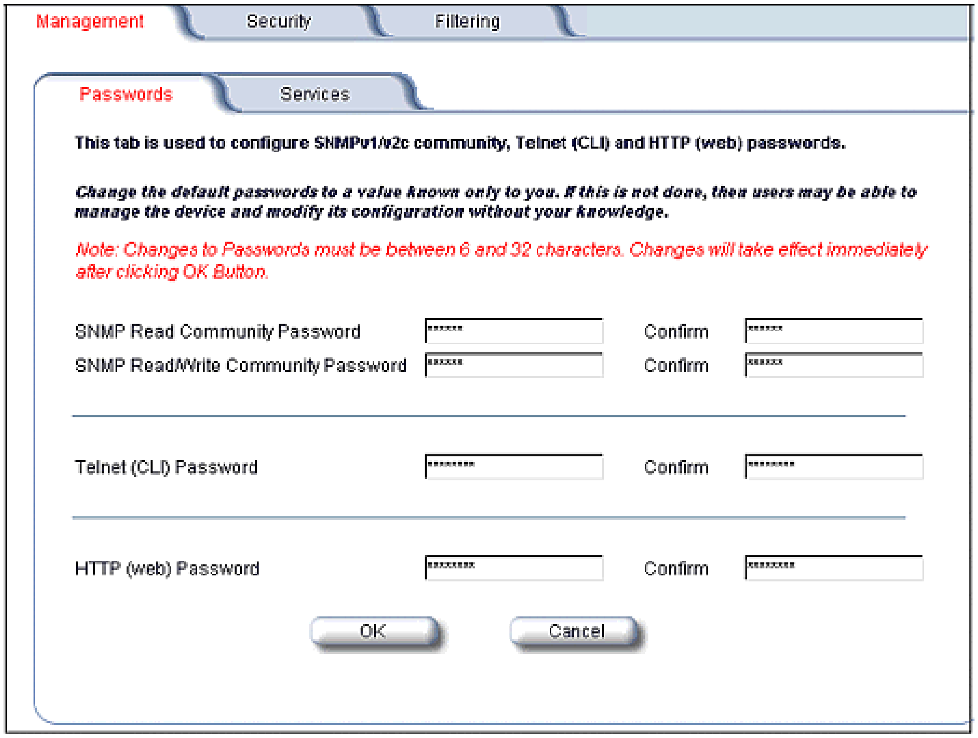
- Ensure that routers on the same physical network are configured to use the same version of RIP.
- Routing updates occur every 30 seconds. It may take up to 3 minutes for a route that has gone down to timeout in a routing table.
- RIP is limited to networks with 15 or fewer hops.

6) Configure Management Parameters

When you click the **Management** button, the **Passwords** tab 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.



This tab is used to configure SNMPv1/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	******	Confirm	******
SNMP Read/Write Community Password	******	Confirm	******
Telnet (CLI) Password	********	Confirm	********
HTTP (web) Password	********	Confirm	********

Field Descriptions

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

SNMP Read Community Password

The password for read access to the unit 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 to the unit using SNMP. Enter a password in both the **Password** field and the **Confirm** field. The default password is **public**.

Telnet (CLI) Password

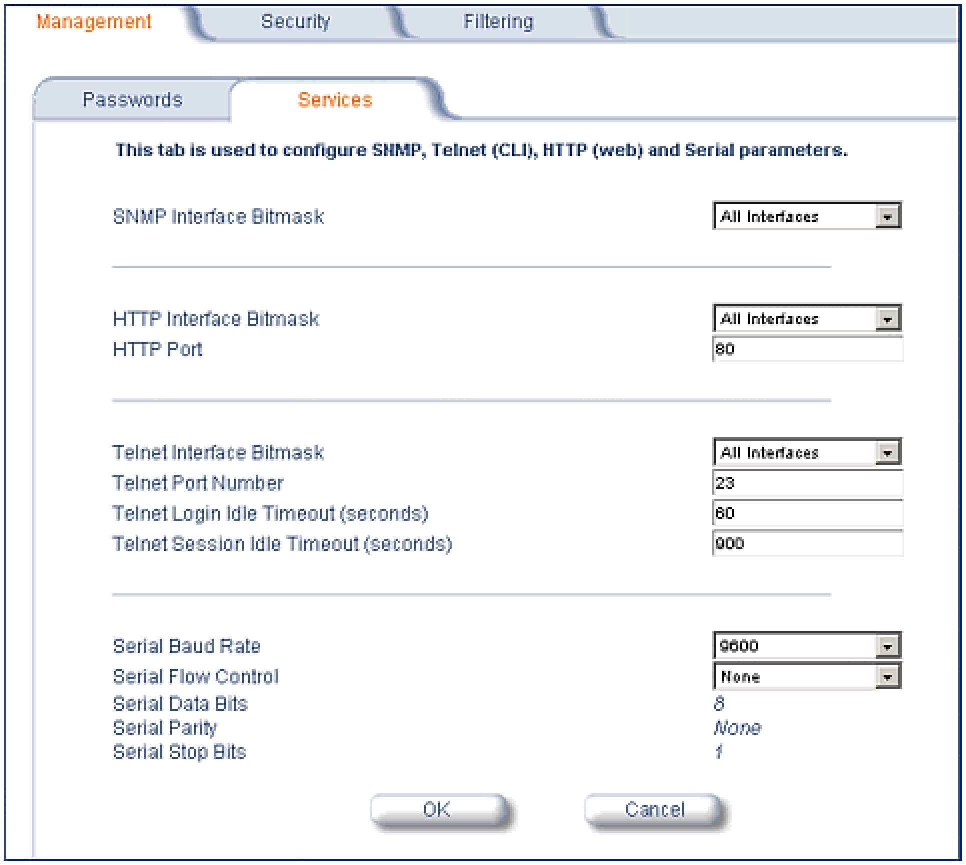
The password for the CLI interface (via serial or Telnet). Enter a password in both the **Password** field and the **Confirm** field. The default password is **public**.

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.



This tab is used to configure SNMP, Telnet (CLI), HTTP (web) and Serial parameters.

SNMP Interface Bitmask: All Interfaces

HTTP Interface Bitmask: All Interfaces
HTTP Port: 80

Telnet Interface Bitmask: All Interfaces
Telnet Port Number: 23
Telnet Login Idle Timeout (seconds): 60
Telnet Session Idle Timeout (seconds): 900

Serial Baud Rate: 9600
Serial Flow Control: None
Serial Data Bits: 8
Serial Parity: None
Serial Stop Bits: 1

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 (click **Properties** from the HyperTerminal window; select **Setup**, then **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).

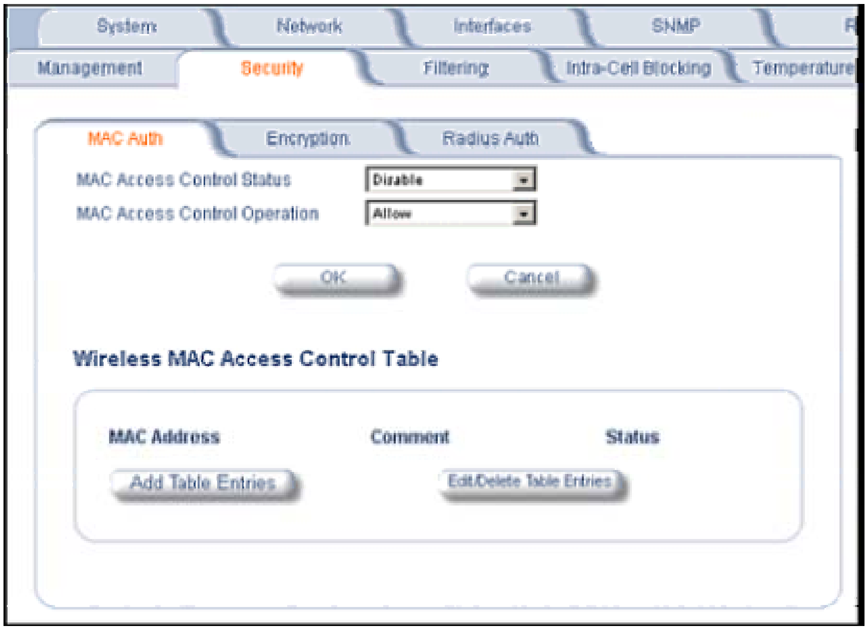
The serial port bit configuration is commonly referred to as 8N1.

7) Configure Security Parameters

Configure MAC Authentication

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

MAC authentication is available only for Base Station units.



MAC Access Control Status: Disable

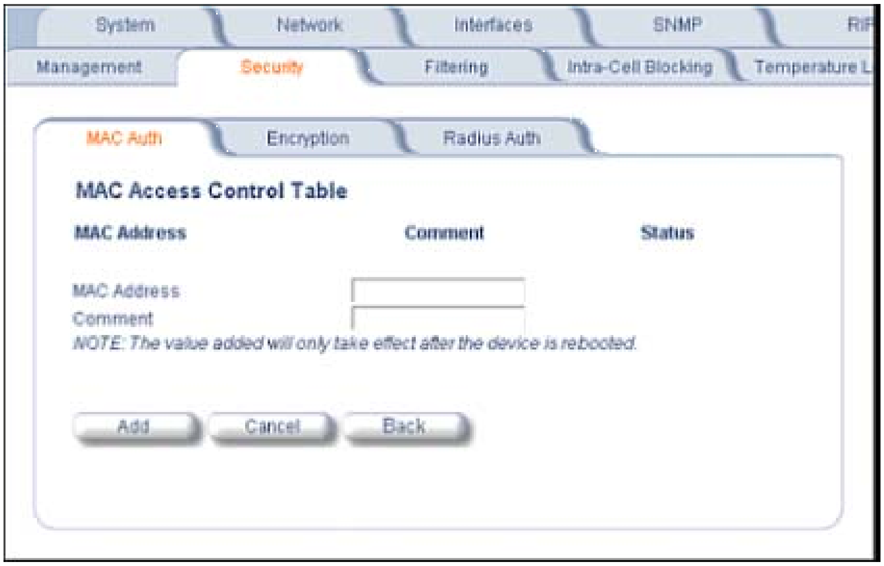
MAC Access Control Operation: Allow

Wireless MAC Access Control Table

MAC Address	Comment	Status

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:



MAC Access Control Table

MAC Address	Comment	Status

MAC Address:

Comment:

NOTE: The value added will only take effect after the device is rebooted.

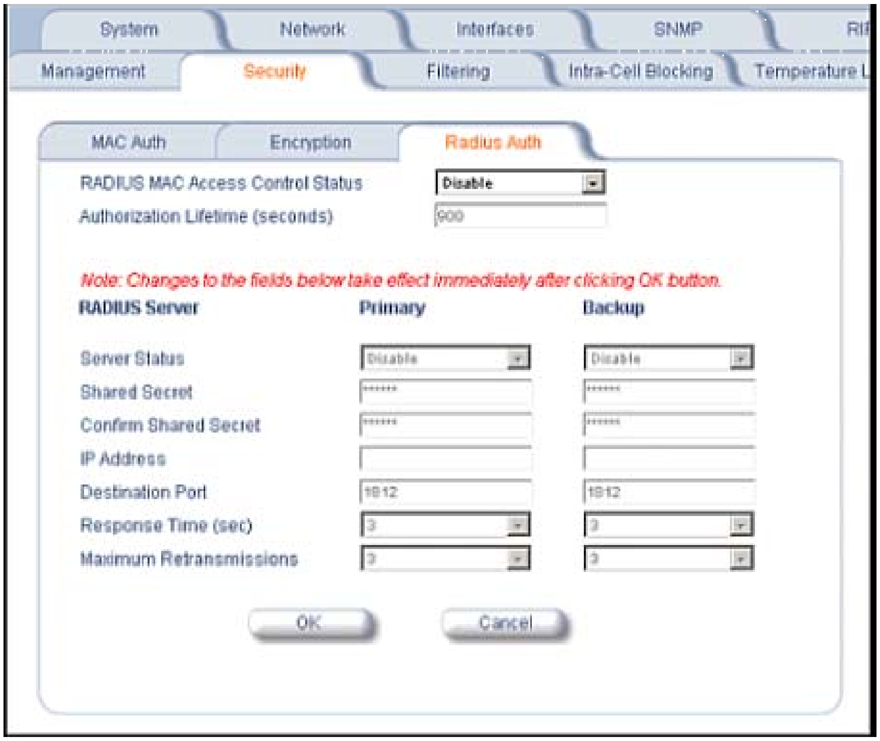
Enter the MAC address and any comment, then click **Add**. The maximum number of MAC addresses that can be entered is 250.

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

Configure RADIUS Authentication

Click the **Configure** button, the **Security** tab, and the **Radius Auth** sub-tab 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.



RADIUS MAC Access Control Status	Disable
Authorization Lifetime (seconds)	900

Note: Changes to the fields below take effect immediately after clicking OK button.

RADIUS Server	Primary	Backup
Server Status	Disable	Disable
Shared Secret	******	******
Confirm Shared Secret	******	******
IP Address		
Destination Port	1812	1812
Response Time (sec)	3	3
Maximum Retransmissions	3	3

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.

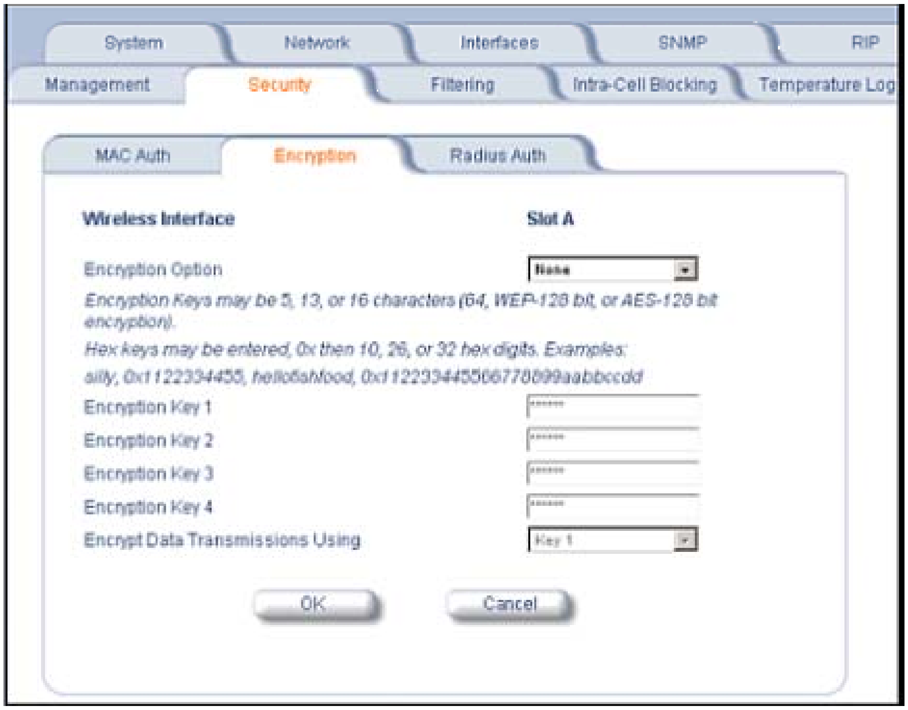
Configure Encryption Parameters

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 the **Configure** button, the **Security** tab, and the **Encryption** sub-tab 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.



Wireless Interface — Slot A

Encryption Option: None

Encryption Keys may be 5, 13, or 16 characters (64, WEP-128 bit, or AES-128 bit encryption).

Hex keys may be entered, 0x then 10, 26, or 32 hex digits. Examples:

silly, 0x1122334455, hellofishfood, 0x112233445566778899aabbccdd

Encryption Key 1: ******

Encryption Key 2: ******

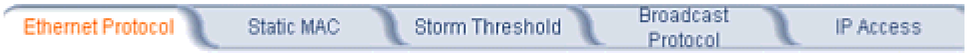
Encryption Key 3: ******

Encryption Key 4: ******

Encrypt Data Transmissions Using: Key 1

8) Configure Packet Filtering

Click the **Configure** button and the **Filtering** tab to configure packet filtering. Packet filtering can be used to control and optimize network performance. Filtering sub-tabs are as follows:



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 to (administrator) the MP.11, Proxim recommends that IP (0x0800) and ARP (0x0806) protocols are always passed through.

Sample Use and Validation

Configure the protocol filter to let only IP and ARP traffic pass through the MP.11 (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 RangeLAN2 device may have the MAC address of 00:20:A6:33:ED:45.

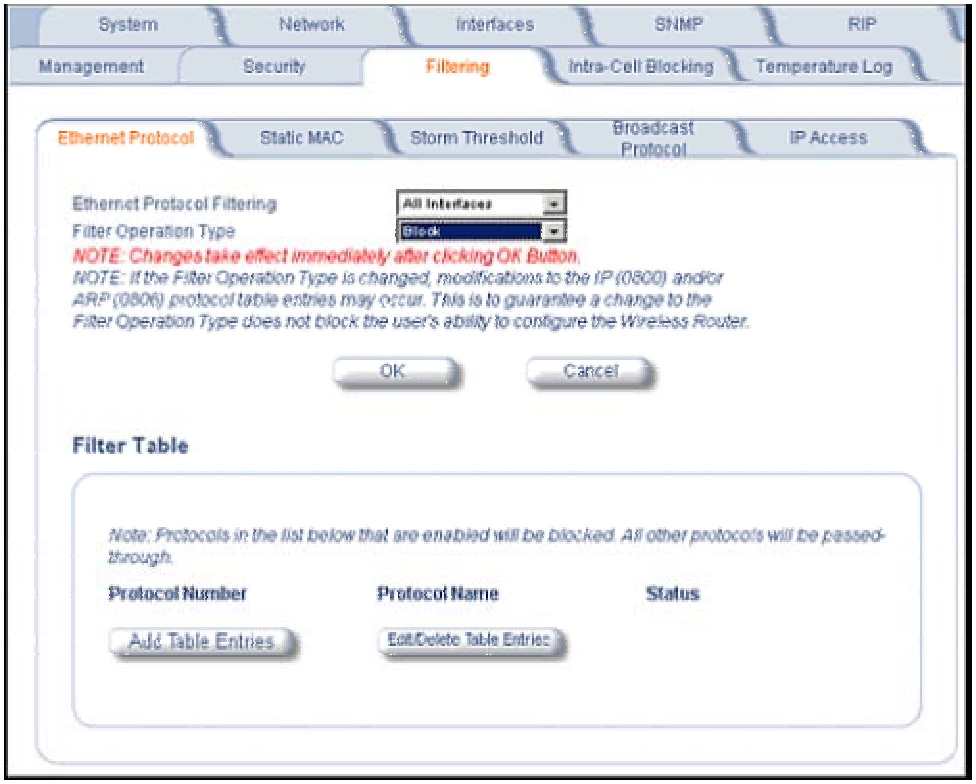
When devices send data over the network (Ethernet, Token Ring, or wireless), they use the MAC address to identify a packet's source and destination. Therefore, an IP address must be mapped to a MAC address in order for a device to send a packet to particular IP address. In order to resolve a remote node's 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 on the Ethernet protocols they support. Click the **Configure** button, the **Filtering** tab, and the **Ethernet Protocol** sub-tab to enable or disable certain protocols in the table. Entries can be selected from a drop-down box.



Ethernet Protocol Filtering: All Interfaces

Filter Operation Type: Block

NOTE: Changes take effect immediately after clicking OK Button.

NOTE: If the Filter Operation Type is changed, modifications to the IP (0800) and/or ARP (0806) protocol table entries may occur. This is to guarantee a change to the Filter Operation Type does not block the user's ability to configure the Wireless Router.

Filter Table

Note: Protocols in the list below that are enabled will be blocked. All other protocols will be passed-through.

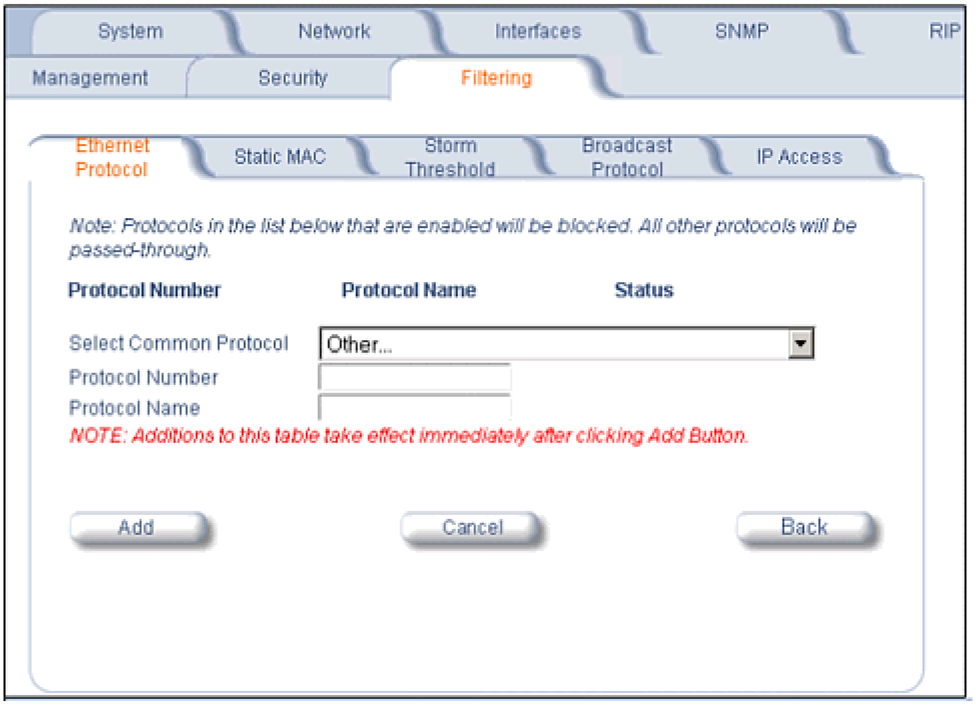
Protocol Number	Protocol Name	Status

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 **Passthru**, only the enabled Ethernet Protocols listed in the Filter Table pass through the bridge.
   - If set to **Block**, the bridge blocks enabled Ethernet Protocols listed in the Filter Table.
3. Configure the **Ethernet Protocol Filter Table**. This table is pre-populated with existing Ethernet Protocol Filters, however, you may enter additional filters by specifying the appropriate parameters.
   - To add an entry, click **Add**, and then specify the **Protocol Number** and a **Protocol Name**.
   - **Protocol Number:** Enter the protocol number. See http://www.iana.org/assignments/ethernet-numbers for a list of protocol numbers.
   - **Protocol Name:** Enter related information, typically the protocol name.
   - To edit or delete an entry, click **Edit** and change the information, or select **Enable**, **Disable**, or **Delete** from the **Status** drop-down menu.
   - An entry's status must be enabled in order for the protocol to be subject to the filter.

Add Entries to the Ethernet Protocol Filter Table

To add an entry to the table, click **Add Table Entries**, select the protocol name from the drop-down box and click the **Add** button.



Note: Protocols in the list below that are enabled will be blocked. All other protocols will be passed-through.

Protocol Number **Protocol Name** **Status**

Select Common Protocol: Other...
Protocol Number:
Protocol Name:

NOTE: Additions to this table take effect immediately after clicking Add Button.

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

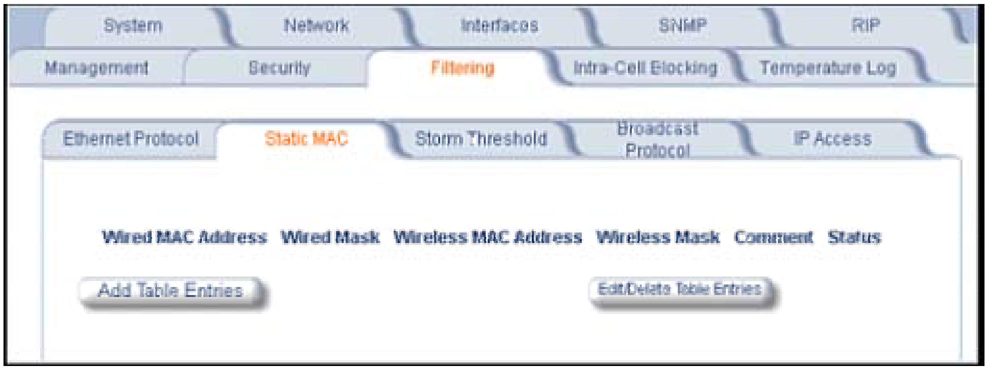
Configure Static MAC Pair Filtering

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 only thing important is the MAC address in the packets arriving at the wireless interface.

This 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 the **Configure** button, the **Filtering** tab, and the **Static MAC** sub-tab to access the Static MAC Address filter.



Wired MAC Address	Wired Mask	Wireless MAC Address	Wireless Mask	Comment	Status

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 (each bit represents the value 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 allows any value and F allows only 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:FF:FF applies only to the specified MAC address.

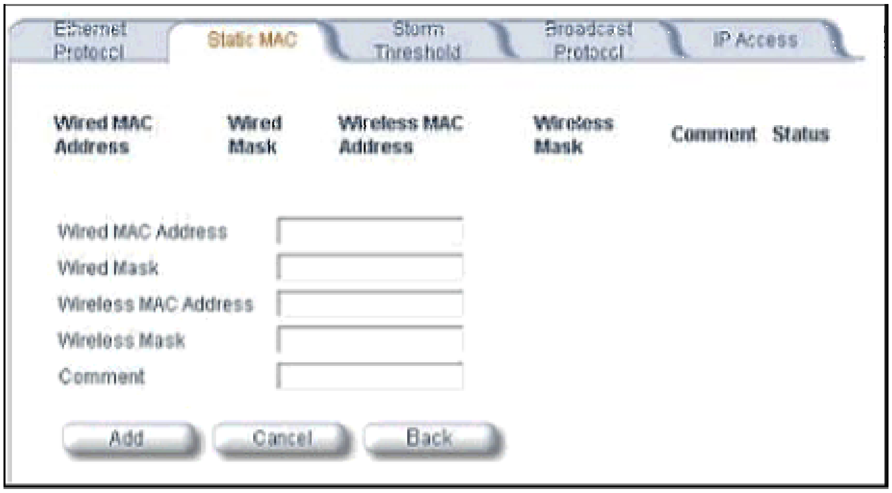
For example, if the MAC address is 00:20:A6:12:54:C3 and the mask is FF;FF;FF;00:00:00, the unit examines the source and destination addresses of each packet looking for any MAC address starting with 00:20:A6. If the mask is FF;FF;FF;FF;FF;FF, the unit looks only for the specific MAC address (in this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

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**.

Field Descriptions

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 1:

- **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 Wired Server 1 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.