

TECHNICAL MANUAL

TRIMAR 802.11a/b/g AP/REPEATER



Introduction

The TRIMAR is a multiple-band, multiple-data-rate, multiple-role wireless data radio that meets many of the challenges faced by today's wireless networking applications.

Compliant with both 802.11b/g and 802.11a standards and operating in either the 2.4 GHz or 5 GHz bands, TRIMAR offers great flexibility in the trade-offs between data speed, link distance and frequency planning for adjacent coverage or linkages.

The TRIMAR can be configured to function as an access point or as a repeater. Designed for both Indoors and Outdoor uses, it comes with a weatherproof enclosure and is powered over the Ethernet cable, making the product extremely easy to install. Its built-in RF connector allows different types of antennas to be attached, allowing for great flexibility in terms of deployment coverage and link distance requirements.

Whether used as an access point in a retail hotspot application for Internet access or as an office wireless LAN (WLAN) for interconnecting mobile computers, TRIMAR's multiple SSID and VLAN features provide service providers and network managers with great versatility in customizing access control and classes of service for different user groups.

For connecting computer networks in different locations miles apart, TRIMAR's capability of working as a repeater, affords network designers, integrators and contractors great flexibility in constructing point-to-point, point-to-multiple point, multiple point-to-multiple point networks, as well as wireless backbones.

The TRIMAR has built-in intelligence capable of automatically forming a layer-two mesh network and discovering optimal paths. In case of node failures, it automatically searches out alternative paths, making the network self-healing and fault tolerant.

In addition, the TRIMAR's ability to support the latest wireless networking security standards: WPA, WPA2, WEP, AES, TKIP and 802.11i authentication provides for maximum security deployment options for your network and securing your data.

Copyright

Information in this document is subject to change without notice. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of the seller. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

The seller provides this documentation without warranty, term, or condition of any kind. The seller may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

Other product and company names herein may be trademarks of their respective owners.

Copyright © 2006, Pegasus Wireless Corporation. All rights reserved.

Notes:

1. OTC Wireless, Inc. is a wholly owned subsidiary of Pegasus Wireless Corporation.
2. The term TRIMAR and TRIMAR AP are used interchangeably throughout this document.

Table of Contents

Section	Title	Page	Description
	Features	3	
	Specifications	4	
1	Equipment Installation	5	Instructions and considerations for wiring and installing TRIMAR radios including manufacturer's recommended practices.
2	Configuring the TRIMAR	9	Basic procedures for working with the TRIMAR web-based administration utility.
3	Information Tab	11	An explanation on how to obtain the current operational status of the TRIMAR.
4	Administration Tab	12	An explanation of the controls for the basic administrative functions of the TRIMAR including setting a TRIMAR's IP address or IP addressing mode.
5	Basic Wireless Tab	15	An explanation of the Basic wireless operation controls including controls used to control the visibility of SSIDs and configuring the controls for channel selection and turbo mode operations.
6	Advanced Tab	17	An explanation of the Advance wireless operation controls.
7	SSID Admin Tab	19	An explanation of how to configure the eight SSIDs that a TRIMAR radio can support including instructions on setting up each SSIDs security policies (WPA/WEP).
8	WEP Security Tab	23	An explanation on how to configure the WEP controls.
9	Access Control Tab	24	An explanation of the control that are used to restrict wireless access based on device MAC addresses.
10	WDS Tab	25	An explanation on how to set the controls to enable TRIMARs to become participants in a WDS mesh deployment.
11	DHCP Server Tab	27	An explanation on setting the controls that will allow the TRIMARs to function as DHCP servers.
12	Stations Tab	28	An explanation on viewing information on stations that have associated with the TRIMAR.
13	Save Tab	29	An explanation on how to create, save and upload a configuration/settings template.
14	Help Tab	31	Where to get Technical support and additional information.
	Appendix	32	

Features

GENERAL:

- ❑ Enterprise-class wireless LAN capable of supporting up to 48 infrastructure stations/users.
- ❑ Power-Over-Ethernet system (POE) allows individual radios to be powered over the same cable used to carry data.

SSID:

- ❑ Supports multiple SSIDs. Up to eight simultaneous virtual APs can be supported by each TRIMAR radio.
- ❑ Each SSID can have its own individual security and authentication configuration that supports WEP, WPA or WPA2 (802.11i).
- ❑ One of the custom configured SSIDs can be selected as the visible SSID that will be broadcasted in the beacon. The station users can scan and only see this visible SSID.
- ❑ The visible SSID can be reserved for guest users. All of the other SSIDs can be reserved for use by company employees.
- ❑ TRIMARs can also be configured with none of their SSIDs being visible.

WIRELESS:

- ❑ Supports 802.11a and 802.11b/g. A TRIMAR radio can be used in either 802.11a mode or 802.11b/g mode; but not in both modes simultaneously.
- ❑ Supports Atheros SuperA/G turbo mode to boost data rates up to 108Mbps.
- ❑ Dynamic turbo mode.
- ❑ Auto-channel setting to allow the radio to select the best channel automatically during system boot-up.
- ❑ All APs that are wirelessly linked together need to share the same channel but can use different SSIDs.

WIRELESS MESH:

- ❑ Supports WDS (Wireless Distribution System) with STP (Spanning Tree Protocol) to link with other APs to form a large wireless mesh network.
- ❑ The WDS connection supports unsecured as well as WEP encrypted deployments.

SECURITY:

- ❑ WPA/WPA2 support for TKIP and AES cipher type with personal (PSK) and enterprise authentication (through 802.1x with RADIUS server).
- ❑ Two RADIUS servers setup per each virtual AP to provide flexible and redundant deployment.
- ❑ Supports four WEP keys (64-bits/128-bits) and authentication type (open / shared key) is shared by each virtual AP and WDS services.
- ❑ Individual local bridging enable/disable. When disabled, even stations assigned with the same SSID cannot communicate with each other.
- ❑ WEP key is shared with other virtual APs in the same BSS network.

NETWORK:

- ❑ Supports VLAN (Virtual Local Area Network) tags on each virtual AP. (This function requires a VLAN capable switch or router).
- ❑ VLAN tagging can be enabled/disabled for each individual SSID.
- ❑ Each virtual AP can be assigned a unique VLAN ID (1 to 4095). The VLAN ID determines to which VLAN a station belongs when the station associated with the SSID.
- ❑ VLAN support provides more secure network deployment.
- ❑ Traffic for each individual VLAN ID is separated from each other.

NETWORK MANAGEMENT:

- ❑ SNMP v1 and v2 with OTC enterprise MIB for total wireless management.

Specifications

- RF
 - Operating Frequency Range: 2.4 –2.4835 GHz, 5.15 – 5.85 GHz
 - Data Rate: 54, 48, 36, 24, 18,12, 11, 9, 6, 5.5, 2 and 1 Mbps
 - Turbo mode: 108 Mbps
 - Modulation: OFDM/CCK/DQPSK/DBPSK
 - Antenna Connector: Type N Female
 - Transmission Power: 14dBm typical at antenna port
 - Receiving Sensitivity: 65dBm @ 54 Mbps, -80dBm @11Mbps, at 10-5 BER
- Network Interface: 10/100BaseT RJ-45
- Security: WPA, WPA2, WEP, TKIP, AES, 802.11i
- Management: WEB, SNMP
- Environment:
 - Operating Temperature: -10° to 65°C
 - Operating Humidity: 5% -100%. Rain proof
- Physical Dimension:
 - 5.375 inches x 4.75 inches x 2 inches
- Certification: FCC, CE

TRIMAR FCC label:

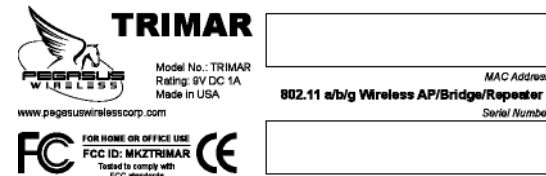


Figure 1: TRIMAR FCC label

This label is located on the back of all official TRIMAR products. The unit's unique hardware MAC address and serial number are affixed on this label.

Hardware MAC address: This is separately indicated from within the TRIMAR's web-based administration utility. The hardware MAC address on the label should match the web-based administration utility's reported MAC address (unless this has been subsequently modified by the user).

Product Serial Number: This number is needed for product verification should the unit ever require servicing by Pegasus Wireless Corporation.

1. Equipment Installation

Manufacturer's Recommended Practices

Tip: Place a UPS battery back-up unit or as a minimum, a surge protector between the power supply outlet and AC-DC adapter.

Applying Power and network connections to your TRIMAR Radio

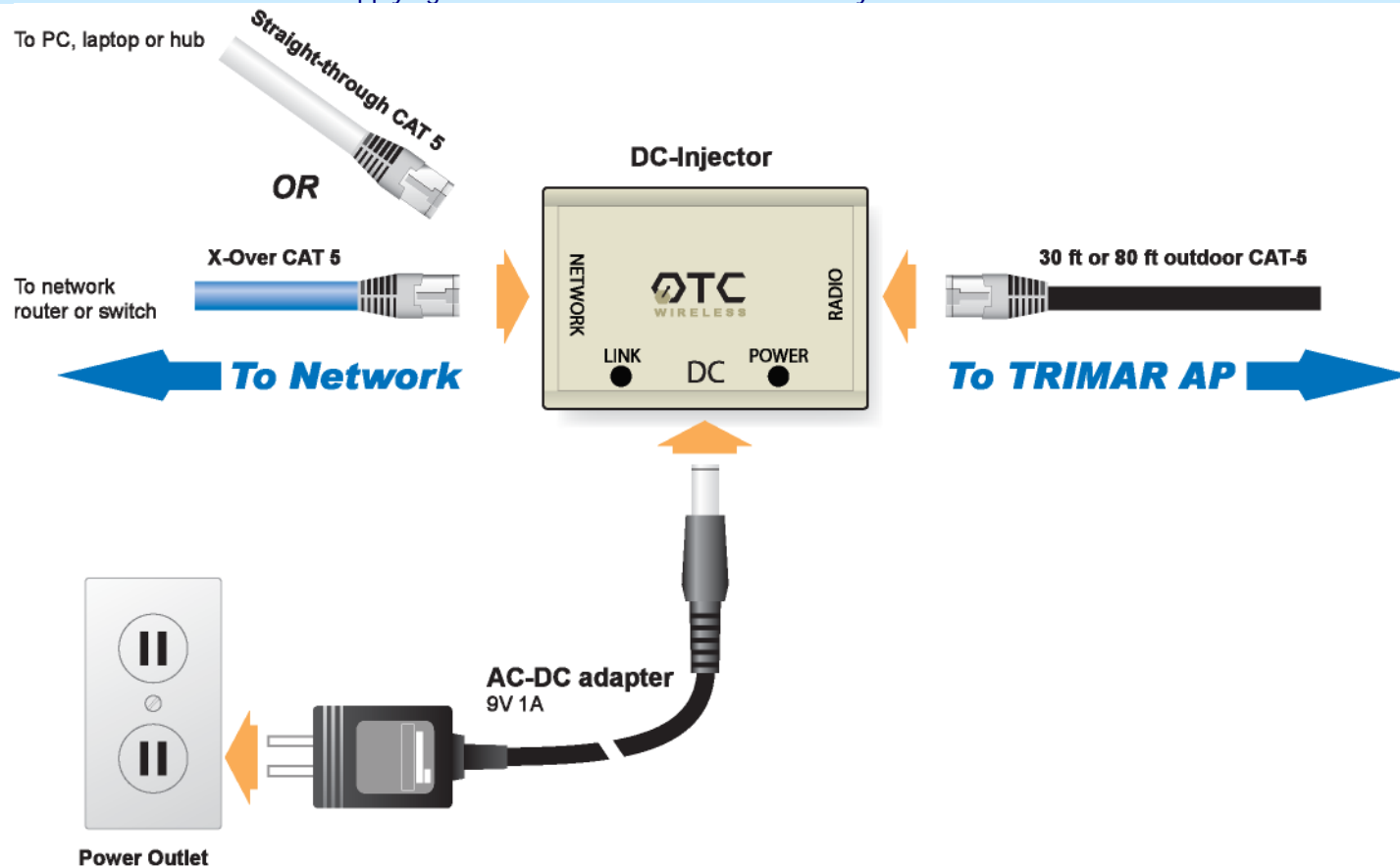


Figure 2: Hooking up the DC-Injector

Safety Statement:

Use only the power adapter provided with this product or other Pegasus Wireless Corporation authorized replacement power adapter. Connect the power adapter to a properly grounded electrical outlet that is near the product and easily accessible.

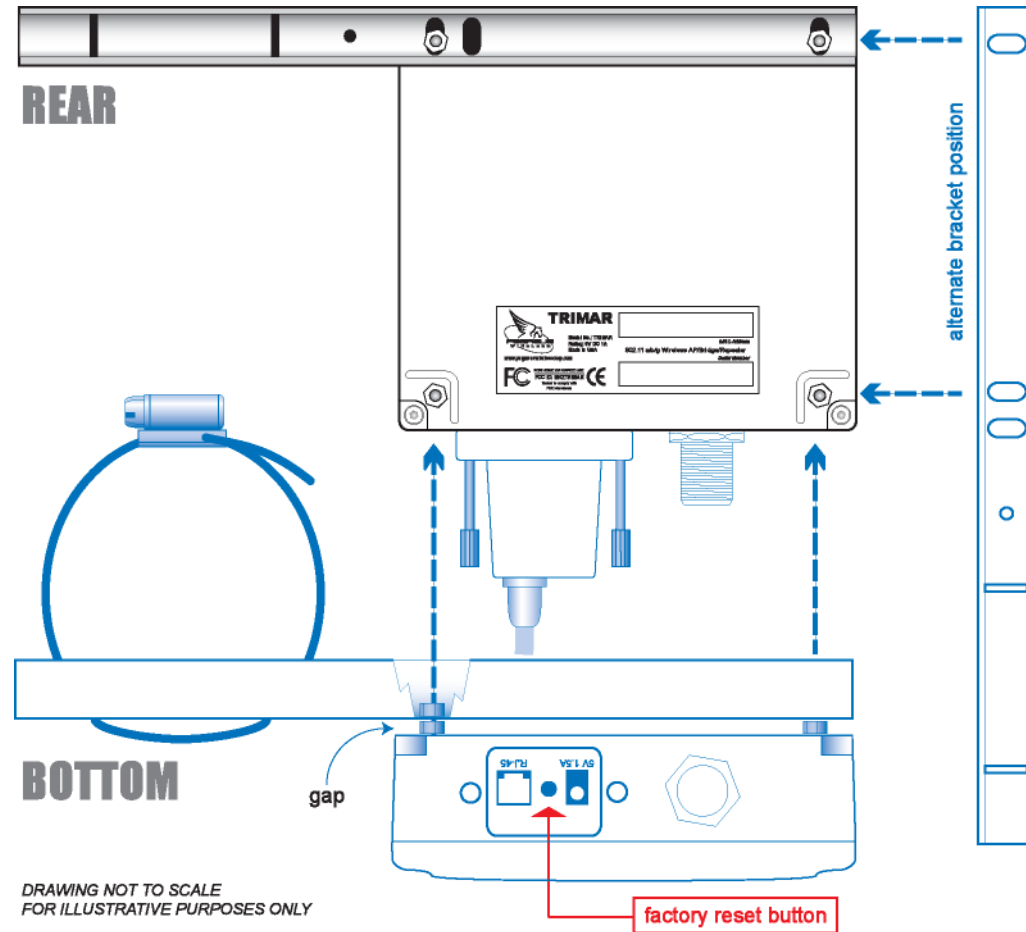
Refer service or repairs to a professional service person.

WARNING: The DC-injector and the power adapter are not intended for outdoor use. These should be protected from the elements and damp at all times.

Equipment Installation

(.. /continued)

Installing the TRIMAR Radio



DRAWING NOT TO SCALE
FOR ILLUSTRATIVE PURPOSES ONLY

Figure 3: Bracket assembly details

RECOMMENDATIONS:

1. **Do not mount the radio upside down or sideways.** The type N-connector must face downwards towards the ground.
2. Strap down the external CAT 5 cable leading from the radio to the antenna mast or other suitable fixture.

HOW TO RESET THE RADIO TO FACTORY DEFAULTS:

Should it become necessary to do a hardware reset of the TRIMAR AP to factory default settings, follow the steps below. Refer to Figure 3 for the location of the reset button:

1. Unscrew and remove the cable cover and *gently* pull assembly away from the main case.
2. To reset the unit the radio needs to be powered.
3. Press firmly on the reset button and watch the indication of the LED lamps.
4. When the reset is successfully performed, the LED lamps will dim and then light up again as the unit reboots.
5. After resetting, reconnect the CAT 5 cable and replace the cable cover taking care to ensure that this is replaced correctly to avoid moisture from getting into the unit.

DO NOT UNDER ANY CIRCUMSTANCE OPEN THE PRIMARY CASE OF THE RADIO. DOING SO WILL BREAK THE SPECIAL WEATHER SEAL BETWEEN THE CASE COVER AND MAIN CASING AND WILL AUTOMATICALLY VOID THE WARRANTY ON THE UNIT.

THERE ARE NO USER SERVICABLE PARTS INSIDE THE CASE.

WARNING: After fixing and testing the radio at its final location, **use the weather sealant provided to protect the antenna and N-connector from the elements.** Failure to do so could cause water to corrode the connection or allow water seepage to penetrate the weather casing and causing catastrophic damage to the radio circuitry.

Equipment Installation

(.. /continued)

DC-Injector LED indicators

LED	Color	State
Power	Amber	OFF when there is no power. Steady ON when power is supplied to the unit.
Network	Amber	OFF when network connection is absent. Steady ON when network connection is successfully established. BLINKING if the network connection is unstable – check or replace cable; make sure all plug connections are snug.

TRIMAR-AP LED indicators

LED	Color	State
NW (network)	Amber	Steady ON when network connection is successfully established.
RX (receive)	Green	BLINKING when receiving data. OFF when radio is idle or unable to receive data.
TX (transmit)	Red	BLINKING when transmitting data. OFF when radio is idle or unable to transmit data.
ON (power)	Red	Steady ON when there is power.

Use the correct cable to connect with the network!

Rule of Thumb:

Use the white UTP straight-through CAT-5 when connecting directly to a PC, laptop or hub.

Use the blue UTP crossover CAT-5 when connecting to a network router or switch.

Note: If one type of cable does not work, try using the other type of cable.

Many contemporary laptops and some routers will accept either type of cables.

Check to make sure all connections are snug. Do not use damaged cables or ones with broken or damaged connectors.

USE THE CORRECT VOLTAGE POWER SUPPLY.

For normal operations, power the TRIMAR AP with the 9V AC-DC adapter. This power supply is rated 9V DC ~ 1A and will provided the correct POE voltage to the radio via the 30-foot or 80-foot external CAT 5 cable supplied.

For testing and configuration purposes a 5V DC ~ 1.5A power socket is located on the radio underneath the CAT-5 cable cover (see Figure 3). The radio is not designed for long-term operations when powered in this manner. Doing so may lead to unpredictable or undesirable results, including, but not limited to data loss or hardware damage.

Absolutely DO NOT use the 9V AC-DC adapter to power the radio at the 5V DC socket as this will overload the unit's circuitry and render the radio completely inoperative.

Equipment Installation

(.. /continued)

Tip: Always test all equipment at the workbench before installing them at their final positions.

Example Installations

STANDARD AP SETUP

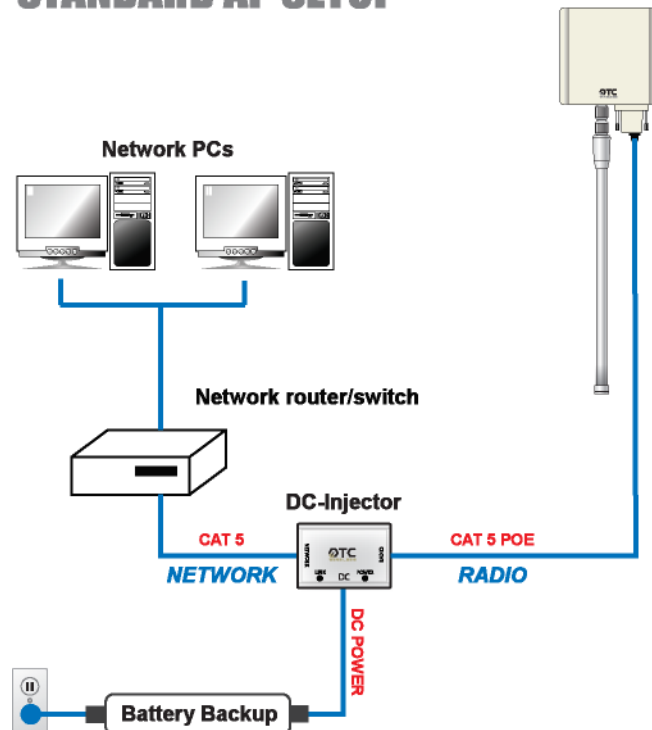


Figure 4: Typical TRIMAR deployment schematic

Figure 4 above illustrates a common wiring scheme for a TRIMAR radio unit that is physically connected to the network.

A set up like this can be used to connect with another TRIMAR radio in a separate building that is wired similarly to form the basis of a wireless point-to-point bridge. Alternatively, it can be connected wirelessly with TRIMAR repeaters (as shown in Figure 5) to form a larger wireless mesh. In both of these types of operations, the TRIMAR APs need to be configured to operate in WDS mode.

REPEATER SETUP

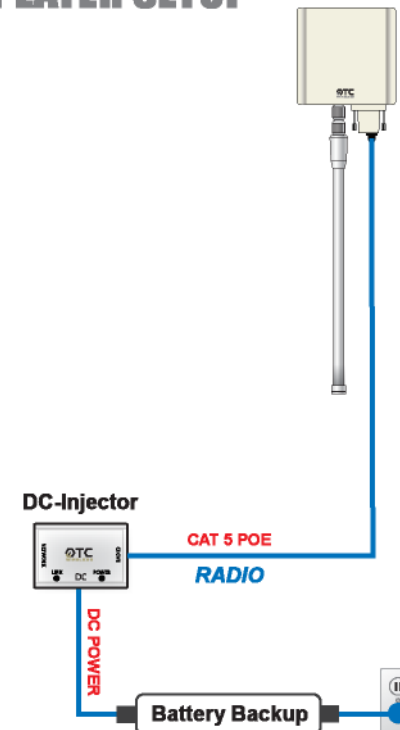


Figure 5: TRIMAR repeater mode schematic

Figure 5 illustrates a TRIMAR radio used as a repeater. In this type of deployment, no physical connection to the network is necessary, all communications is done via the 802.11 wireless connections.

To work in this mode, the TRIMAR radio must be configured using WDS and connected wirelessly to at least one radio that is physically connected to the network being serviced.

2. Configuring the TRIMAR AP

Basic Procedure

The TRIMAR AP uses a web-based administration utility. To access this utility you will need to use Microsoft © Internet Explorer, Mozilla Firefox or a compatible web-browser.

Accessing the web-based administration utility:

1. Connect a PC either directly to the TRIMAR radio. If the radio is already configured for operation on an established network, connect to it via a network route.
2. The PC connecting with a TRIMAR radio's web-based administration utility *must* be on the same IP subnet as the radio. (See insets at right).
3. Enter the IP address of the TRIMAR into the web-browser window and click "Go".

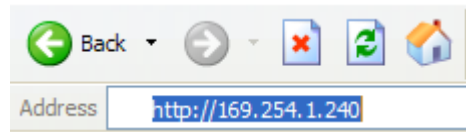


Figure 6: Enter the TRIMAR's IP address into the browser's address bar

4. Enter the correct account and password when security dialog panel appears.



Figure 7: Web-based administration password challenge dialog box

Preset Factory Defaults:

IP address:	169.254.1.240	User name:	admin
Subnet Mask:	255.255.0.0	Password:	public
Default Gateway:	169.254.1.1		

Using the OTC Device Locator:

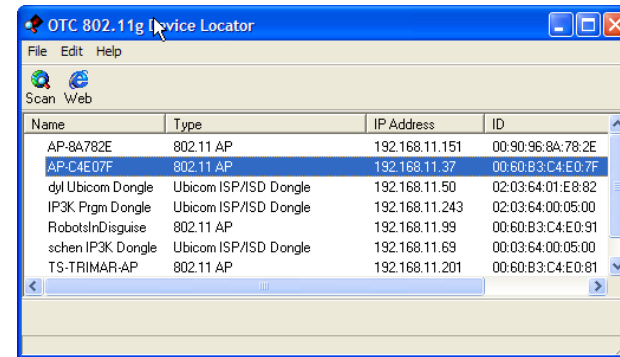


Figure 8: OTC 802.11g Device Locator GUI

The OTC Device Locator program can be found on the CD that is distributed with the TRIMAR AP. Install it on to the PC by creating a folder for it and copying the .exe and .dll file into the new folder.

The Locator will locate all OTC AVCW and TRIMAR radios within the same network. Its primary use is to identify the IP and MAC addresses of the radios.

The PC running the program needs to have a wireless card; be connected to the same network; or directly with at least one OTC 802.11g radio. To use the program, simply click the "Scan" button and wait for the program to report its findings. If the PC and the radio being accessed are already on the same IP subnet, clicking on the "Web" button will open the default web-browser, which will proceed to connect directly with the selected product's web-based administration utility.

Configuring the TRIMAR AP

(.. /continued)

Navigating and using the web-based administration utility

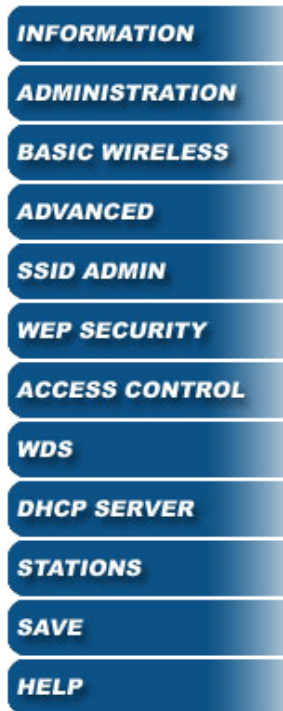


Figure 9: TRIMAR web-based administration navigation tabs

The different pages of the web-based administration utility can be accessed by clicking on the buttons located on the left side of the web-based administration screen.

Make all the desired changes under each tab and “Save” the changes before moving to the next tab. If the only changes that are being made are under the same tab, simply click “Reboot” to apply the settings. Otherwise, proceed to other pages to make (and save) other changes and only reboot the unit after all configuration tasks have been completed.

SAVE CHANGES BEFORE SWITCHING PAGES:

- ❑ If changes are not saved before switching to another page, the changes will be lost.
- ❑ Clicking on the Cancel button will abandon all changes made and will reset the fields to their previous values.

REBOOT THE TRIMAR AP AFTER ALL CHANGES HAVE BEEN MADE:

- ❑ If the TRIMAR AP is not rebooted after all changes have been made, closing the web-based administration utility will cause all newly enter custom settings to be lost.

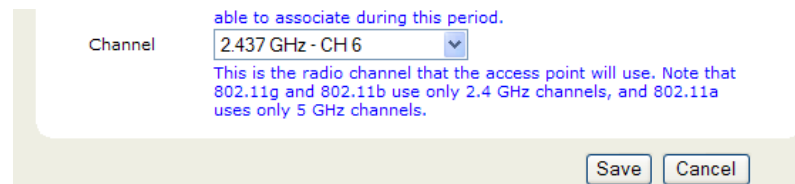


Figure 10: Save changes before changing pages

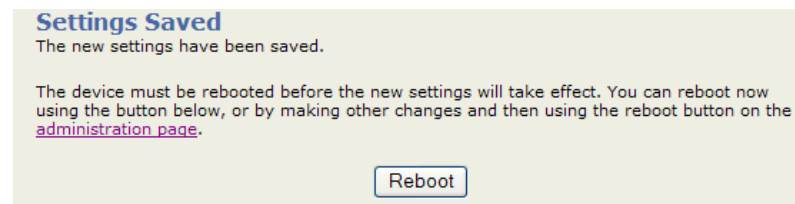


Figure 11: Reboot the unit to apply changes

IMPORTANT: If you change the IP address of the TRIMAR AP, and this puts it on a different IP subnet from the PC used to configure the settings, the web-based administration utility may be unreachable until the PC itself is set to operate within the same IP subnet.

3. Information Tab

This is the “home page” of the TRIMAR’s web-based administration utility. It will be displayed when the utility is first accessed and whenever the TRIMAR AP has been rebooted after configuration changes have been made.

The information on this page gives various readings polled directly from the TRIMAR AP. This data is a “capture” of its current operational status.

Note that it may be necessary to refresh the page to re-poll the TRIMAR AP to update the displayed information.

	Field	Definition/Meaning
1	Access Point Name:	The units assigned name/label
2	Radio MAC Address:	The units factory assigned MAC address
3	IP address:	The units IP address and IP addressing scheme
4	AP firmware version:	The units software firmware version number
5	Radio firmware version:	The units hardware firmware version number
6	SSID:	The units (primary) assigned SSIDs
7	Cell ID:	<i>Used for load balancing – see TRIMAR Controller Manual</i>
8	Current transmit rate:	The units data transmission rate
9	Current channel:	The unit’s current operating channel
10	Operational radio profile:	The unit’s assigned radio operation mode
11	Security:	The unit’s configured security schemes
12	Region:	The unit’s operating geographic region
13	Associated station count:	The number of radios currently associated with the unit
14	Number of stations allowed to associate:	The number of radios allowed to associate with the unit
15	Ethernet MAC Address:	Same as 2. above unless user reconfigured
16	Total packets received:	Total of all packets received or transmitted
17	Total packets transmitted:	
18	Packets received to host:	Total of packets received or transmitted by the host
19	Packets transmitted from host:	
20	Ethernet port rx packets:	Total of packets received, transmitted or broadcasted via LAN port
21	Ethernet port tx packets:	
22	Ethernet port broadcast packets:	
23	WLAN port rx packets:	Total of packets received, transmitted or broadcasted via WLAN port
24	WLAN port tx packets:	
25	WLAN port broadcast packets:	
26	WDS port rx packets:	Total of packets received, transmitted or broadcasted via WDS port
27	WDS port tx packets:	
28	WDS port broadcast packets:	

Table 1: System status definitions

4. Administration Tab

Device Control:

(See Figure 12)

Reboot: Clicking on this button causes the unit to be rebooted. This is normally used in conjunction with configuring the TRIMAR AP.

Reset Configuration: Clicking on this button causes the unit to reboot and will reset the unit's configuration back to its original factory default settings. Use with caution as this will cause all custom user settings to be lost.

Firmware Upgrade:

(See Figure 13)

These controls are used to upload firmware and patches into the TRIMAR AP.

Browse: Use the "Browse" button to select a patch to upload.

Upload: Use the "Upload" button to apply a selected patch to the unit.

Once a patch has been successfully uploaded, the TRIMAR AP will automatically reboot.

Important: Use only official firmware patches supplied by Pegasus Wireless Corporation or an authorized dealer/reseller.

Device Name:

(See Figure 14)

This field is used to give a TRIMAR AP a custom label/name to help more easily identify the unit for administrative purposes. The label will be displayed in the OTC Device Locator panel together with the unit's IP address.

The value entered into this field has no other impact on the TRIMAR AP's operational characteristics.



Figure 12: Device Control

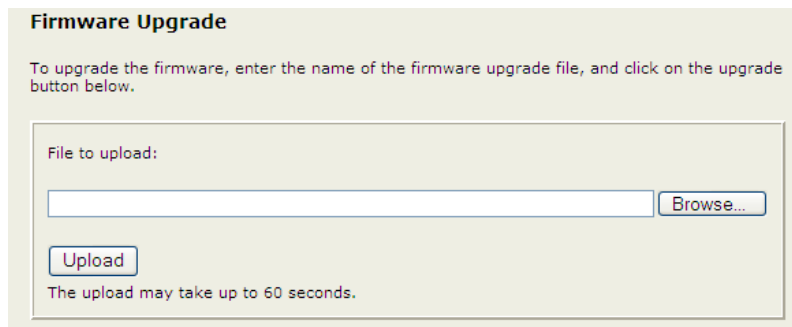


Figure 13: Firmware Upgrade

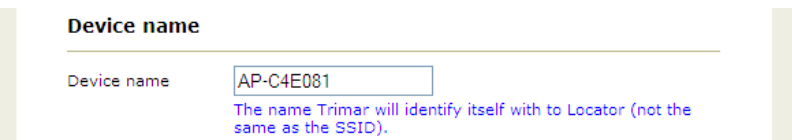


Figure 14: Device Name

Administration Tab

(.. /continued)

IP settings:

(See Figure 15)

These controls are used to assign the TRIMAR AP with its custom IP addressing scheme.

- IP Addressing Mode:** **Static** – select this control if a static/fixed IP address is to be used.
- DHCP** – select this control if the IP address is to be assigned by an external DHCP server.

Default IP address: Use this field to enter a valid IP address.

Default subnet mask: Use this field to enter a valid subnet mask.

Default gateway: Use this field to enter the default gateway (router IP address) for the subnet on which the TRIMAR is located.

Factory Defaults:

IP address: 169.254.1.240
 Subnet mask: 255.255.0.0
 Default gateway: 169.254.1.1

Security:

(See Figure 16)

These controls are used to set the account name and password used to access the web-based administration utility. If these are changed, these should be properly documented as the only way to re-access a unit's administrative controls should the password be lost is to perform a hard reset on the unit which may be extremely difficult if the radio is located in a hard to access location.

Factory Defaults:

User name: admin
 Password: public

IP settings

IP Address Mode Static DHCP
Select 'DHCP' to get the IP settings from a DHCP server on your network. Select 'Static' to use the IP settings specified on this page.

Default IP address
The Trimar's IP address.

Default subnet mask
The subnet mask specifies the network number portion of an IP address.

Default gateway
This is the IP address of the gateway that connects you to the internet.

Figure 15: IP settings

Security

User name
User name for web configuration access.

Administrator password

Password for web configuration access. You must enter the same password into both boxes, for confirmation

Figure 16: Security

Administration Tab

(.. /continued)

SNMP Setting:

(See Figure 17)

These controls are used to enable SNMP control of the TRIMAR AP.

- SNMP enabled:** Check this box to enable SNMP management.
- SNMP server IP address:** This field is used to direct the TRIMAR AP to the network location of the SNMP server.
- Read community:** SNMP read community string
- Write community:** SNMP write community string

Load Control & Balance Setting:

(See Figure 18)

These controls are normally used to allow managed load-balancing of the TRIMAR AP and requires the use of the **TRIMAR Controller** for full functionality.

- Controller IP address:** This field is used to direct the TRIMAR AP to the network location of the TRIMAR Controller.
- Load Limit:** By default, the TRIMAR AP is factory set to allow support to a maximum of 48 stations. This can be manually overridden by entering another value. Restricting the number of stations that are permitted to associate with the unit may help improve service in deployments where a few specific individual stations demand a large percentage of the overall available bandwidth capacity.

If the **TRIMAR Controller** is used to control the load-balancing of the TRIMAR AP, the value entered into this field may be superseded by administrative directives.

SNMP Setting

SNMP enabled Check this box to enable SNMP..

SNMP Server IP Address Enter IP address of the SNMP server this unit sends TRAP packets to.

Read community SNMP read only community.

Write community SNMP read/write community.

Figure 17: SNMP Setting

Load Control & Balance Setting

Load Balance Controller IP address IP address of the Load Balance Controller. A valid address enables load balancing.

Load Limit Maximum number of stations allowed for this AP - a value between 1 and 48. If Load Balance is enabled, then this value is trivial.

Figure 18: Load Control & Balance Setting

TRIMAR CONTROLLER

The TRIMAR Controller is sold separately and is usually required in wireless deployments where the load capacity of the TRIMAR wireless system needs to be managed for optimum network performance.

The use of the TRIMAR Controller allows network managers to fine tune their systems and provides complete monitoring and administration functions of the entire TRIMAR system.

Please contact Pegasus Wireless Corporation or authorized dealer/reseller for additional information on the TRIMAR Controller.

5. Basic Wireless Tab

(See Figure 19)

Wireless On/Off: This control allows a TRIMAR AP to be switched On or Off. This is not the same as an on/off switch. It simply allows the wireless functions of the radio to be switched off for maintenance or other contingencies.

Visible SSID: The TRIMAR AP can support up to eight SSIDs simultaneously. Only one can be visible. This control is used to specify which SSID is to be made visible. Alternatively, the same control is used to make all the SSIDs invisible (choose "None").

Transmission Rate: This control allows users to specify a data transmission rate. It is recommended that this should be left at the factory preset - **Best (automatic)**. When turbo modes are enabled, transmission rates are doubled.

The following controls are inter-related:

802.11 Mode: This control sets the TRIMAR AP's 802.11 operation mode. Note that if 802.11a is selected, an antenna in the 5 GHz range is required. All other modes require that the TRIMAR AP be equipped with a 2.4 Ghz antenna.

Adaptive Radio Selection: This box is checked by default and this enables the TRIMAR AP's Adaptive Radio feature. This control enables the use of the TRIMAR's Super A/G with Dynamic Turbo mode. It needs to be unchecked if the turbo mode is disabled or if other turbo modes are selected.

Super mode: This control determines which type of turbo mode the TRIMAR AP will use. See Table 2 for a full explanation of the choices. Turbo modes always use preset default channels.



Figure 19: Basic wireless controls

Basic Wireless Tab

(.. /continued)

(See Figure 19 on previous page)

Auto Channel Select: This control allows the TRIMAR AP to automatically select what it determines is the best channel to use. This occurs during the radio's boot up process. The channel it selects can be seen under the Information Tab.

Channel: This control is used to set a channel manually. Channels cannot be manually set when Super modes are enabled or if the radio has been set to automatically select a channel when it boots up.

To manually set a channel it is necessary to uncheck both the [Adaptive Radio Selection](#) and the [Auto Channel Select](#) check boxes. Additionally, the super modes must be disabled.

Super Mode Options

Disabled	Super mode operation is disabled.
Super A/G without Turbo	These modes are based on
Super A/G with Static Turbo	Atheros A/G cognitive radio
Super A/G with Dynamic Turbo	technology.
(AR enabled)	

This is the Factory default. If in doubt, leave the TRIMAR AP in this mode. The cognitive radio technology will optimize all wireless operations automatically.

Requires all WLAN equipment or computers to be Atheros A/G enabled for full benefits.

When used with standard WLAN equipment, there should be at least a 10%-20% performance gain, depending on factors present in the local operational environment.

Table 2: Super mode options defined

6. Advanced Tab

(See Figure 20)

Fragmentation Threshold: This determines the maximum size of a data package in bytes. Packages larger than the set value will be broken up for transmission purposes. Reducing the package size in a noisy wireless environment should maintain overall performance.

Factory default: 3200 bytes

RTS/CTS Threshold: Reducing the preset value will enable RTS/CTS and may maintain overall performance in a noisy wireless environment.

Factory default: 3200 bytes

Beacon Period: This value determines the number of milliseconds between AP beacon periods. This controls the frequency that the AP will broadcast its presence to other radios on the network.


Factory default: 100 milliseconds.

Burst Time: This value controls the number of microseconds that the radio will occupy its assigned channel for transmission purposes. Increasing this value can help increase the data throughput rate.

Factory default: 0 microseconds (disabled)

Power Saving: By default, the TRIMAR AP will go into standby mode if it has been idle for a preset period. It will fully activate immediately if it needs to send or receive data.

Factory default: Enabled



Advanced wireless

Fragmentation threshold: 3200
Transmitted wireless packets larger than this size will be fragmented to maintain performance in noisy wireless networks. Valid range is 256..65535. Values larger than ~1560 will prevent fragmentation from taking place.

RTS threshold: 3200
Transmitted wireless packets larger than this size will use the RTS/CTS protocol to maintain performance in noisy wireless networks and prevent hidden nodes from degrading performance. Valid range is 1..65535. Values larger than ~1560 will prevent RTS/CTS from taking place.

Beacon period: 100
The number of milliseconds between each AP beacon. Valid range is 1..65535.

Burst time: 0
Time duration for transmission burst mode, in microseconds. Valid range is 0..65535 (0 to disable). Burst mode increases data throughput by occupying the channel for an extended duration. Typical value is in the 3000 microsecond range.

Power saving:
Check this box to enable support for stations that want to use the power saving mode.

DTIM interval: 1
The rate at which broadcast and multicast packets are delivered to stations in power save mode. Valid range of once every 1..255 beacons.

802.11d:
Check this box to enable support for sending regional information to the stations.

Transmit Power: High
Select Antenna Transmit Power.

WLAN MAC address:
Enter unique MAC address of radio port. If the value is all zeros then hardware MAC address will be used.

Save Cancel

Figure 20: Advanced wireless

Advanced Tab

(.. /continued)

(See on previous page Figure 20)

DTIM Interval: This value determines the frequency when the radio will send broadcast/multicast packets to stations in power save mode. This function is associated with the Beacon Period.

Factory default: 1 (each beacon period or once every 100 milliseconds)

802.11d Global Harmonization control.

Factory default: Disabled.

Transmit Power: This controls the power output permitted to the antenna. If the radio is causing interference to another device, reducing the antenna's output may help alleviate the problem. Do not reduce the power level for any other reasons.

Factory default: High

WLAN MAC address: The MAC address of the wireless port. If left blank, the factory preset MAC address will be used. The factory default MAC address is reported on the Information tab report screen.

Factory default: blank (hardware MAC address is used)

Note about the TRIMAR MAC address options:

The TRIMAR AP supports 2 MAC addresses, one used to address the Ethernet port and the other the Wireless port. By default, these are set to a particular unit's hardware and are unique to the unit.

It is possible to manually enter and override the hardware MAC address by entering the new MAC address information into the following areas:

WLAN MAC address field - Advanced Tab
Ethernet MAC address field - WDS Tab

7. SSID Admin Tab

SSID CONTROLS

(See Figure 21)

SSID #: Selecting an item in this dropdown menu allows configuration to be performed on the SSID selected. **All** the settings on this page are the exclusive properties of the selected SSID. Note the SSID number at the top of the frame – this indicates exactly which of the eight-supported SSID is currently being configured.

The TRIMAR AP is designed to be able to support up to 8 SSIDs simultaneously. Each SSID can be assigned unique security policies and can individually be assigned to a separate VLAN. Only one SSID can be made visible; the other seven will be invisible. The TRIMAR AP can also be configured so that none of the SSIDs is visible. All created SSIDs will share the same WEP keys (for those SSIDs configured to use WEP) as well as the same channel assignment as set under the [Basic Wireless Tab](#). Additionally, the total number of stations that the TRIMAR AP can simultaneously support remains at 48 stations over all created SSIDs.

Enable this SSID: Check this box to enable the selected SSID.

Factory default: Only SSID 1 is enabled by default.

Wireless Network Name (SSID) Enter the desired SSID into this field. (up to 32 characters)

Factory default: TRIMAR

Disable Local: By default, all stations connected to the TRIMAR AP

Bridging are able to see and communicate with each other. Checking this box will stop associated stations from being able to see each other.

This is useful for SSIDs that are used to service “hot-spots” or “Guests accounts”. In these types of deployments, it may not be desirable for PCs connected to the same TRIMAR AP to be aware of each others’ presence.

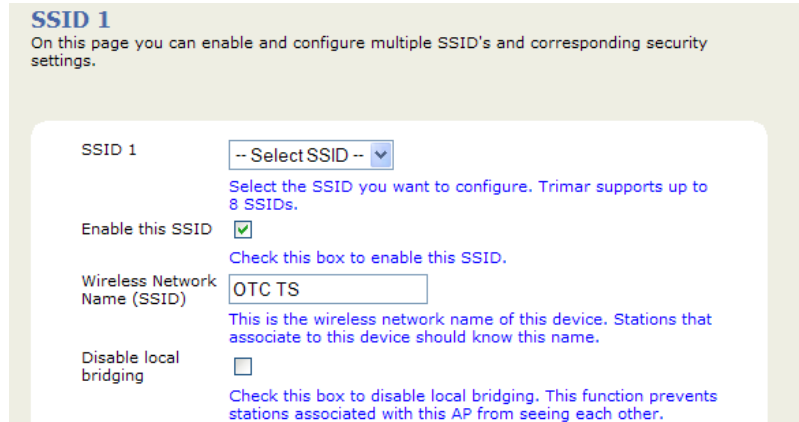


Figure 21: SSID controls

SSID Admin Tab

(.. /continued)

WPA configuration

(See Figure 22)

Each configured SSID can support its own unique WPA configuration, which it does not need to share with the other SSIDs in the configuration set.

WPA Enable: Check this box if WPA is to be used to secure this SSID's wireless access and transmissions.

WPA Mode: Select the desired WPA mode. The following choices are available under the dropdown menu:

- WPA
- WPA2
- WPA2 only

Cipher Type: Select between the following:

- TKIP
- AES
- TKIP and AES

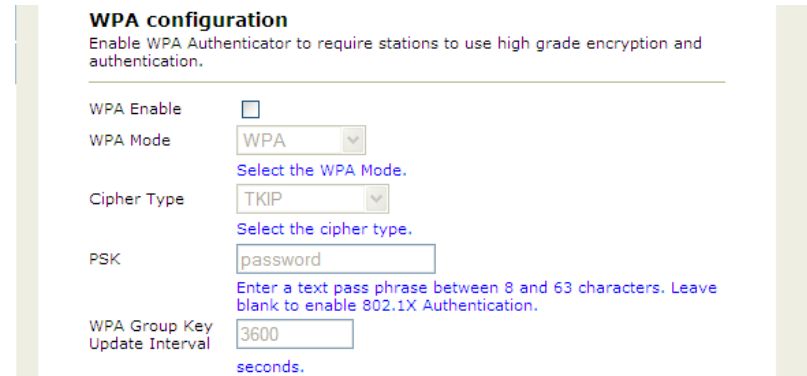
PSK: Enter a valid PSK Pass phrase. Minimum 8 characters to a maximum of 63 characters.

WPA Group Key: Update Interval Value in seconds after which the Group Key will be refreshed.

Factory default: 3600 seconds (one every hour)

Note: WPA-PSK with a TKIP/AES cipher can use for WPA security without the presence of an 802.1X authentication service. With this type of implementation, the associated radios will authenticate amongst themselves.

This type of WPA implementation is ideal for static wireless deployment such as point-to-point, building-to-building wireless bridges as they offer maximum wireless security without the cost and complexity associated with setting up a full 802.1X authentication service.



The screenshot shows the WPA configuration interface. At the top, it says 'WPA configuration' and 'Enable WPA Authenticator to require stations to use high grade encryption and authentication.' Below this, there are several fields: 'WPA Enable' with an unchecked checkbox, 'WPA Mode' with a dropdown menu set to 'WPA', 'Cipher Type' with a dropdown menu set to 'TKIP', 'PSK' with a text input field containing 'password', and 'WPA Group Key Update Interval' with a text input field containing '3600'. There are also blue links: 'Select the WPA Mode.' and 'Select the cipher type.'.

Figure 22: WPA configuration

WPA and TRIMAR APs in WDS mode

TRIMAR APs deployed in a WDS mesh cannot use WPA. All that is needed to configure TRIMAR AP to work within a mesh is that the WDS function be enabled and the MAC addresses of the other units in the same WDS mesh be made known to all radios operating within the same mesh.

SSIDs serves no function in a TRIMAR AP WDS deployment. This means that the individual TRIMAR APs within the WDS mesh can still use WPA security policies associated with the individual SSIDs. These SSIDs can be used with station units that are not immediate members of the WDS mesh.

TRIMAR APs set up as repeaters without a direct Ethernet connection with the network should not use WPA with an 802.1X authentication service.

SSID Admin Tab

(.. /continued)

802.1X configuration

(See Figure 23)

If WPA is used in conjunction with a RADIUS Server, these controls are used to activate this service. The TRIMAR AP can support two RADIUS servers. The first RADIUS server entered is the “preferred” server, and the second RADIUS server entered is the “backup” server that will be accessed if, for whatever reason, the first server cannot be located.

Authentication Timeout: By default the 802.1X service will re-authenticate an associated station once every 60 minutes.

RADIUS Server IP address: The IP address of the Radius Server.

RADIUS Server Port number: The port used by the 802.1X service.

RADIUS Server shared secret: For enhanced security purposes the shared secret password should not be a word found in a dictionary and be at least 16 characters long.

MAC Address Authentication: Check this box if the 802.1X authentication service requires MAC address verification of associating stations.

802.1X configuration

When 802.1X authentication is enabled then the AP will authenticate clients via a remote RADIUS server.

802.1X enabled	<input type="checkbox"/>
Authentication timeout (mins)	<input type="text" value="60"/>
RADIUS server IP address	<input type="text" value="0.0.0.0"/>
RADIUS server port number	<input type="text" value="1812"/>
RADIUS server shared secret	<input type="text" value="radius_shared"/>
MAC Address Authentication	<input checked="" type="checkbox"/>
RADIUS server IP address	<input type="text" value="0.0.0.0"/>
RADIUS server port number	<input type="text" value="1812"/>
RADIUS server shared secret	<input type="text" value="radius_shared"/>
MAC Address Authentication	<input checked="" type="checkbox"/>

Figure 23: 802.1X configuration

SSID Admin Tab

(.. /continued)

WEP configuration

(See Figure 24)

The same WEP keys are used by all SSIDs using WEP encryption on the TRIMAR AP. TRIMAR APs deployed in WDS mode are limited to using WEP.

Enable WEP: Check this box if the selected SSID will implement WEP as a component of its security policy.

VLAN configuration

(See Figure 25)

Each of the TRIMAR AP's eight SSIDs can support a separate VLAN.

Enable VLAN for: This SSID Check this box if the selected SSID is a component of a specific VLAN.

VLAN tag: Enter the correct VLAN tag number.

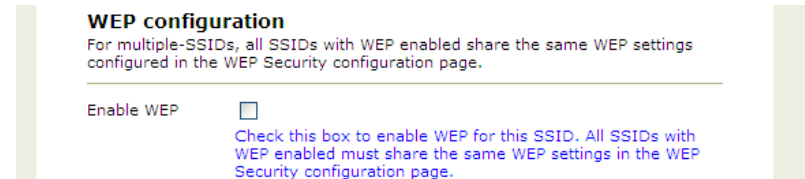


Figure 24: WEP configuration

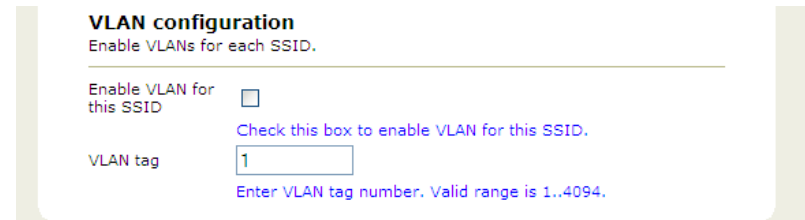


Figure 25: VLAN configuration

8. WEP Security Tab

WEP configuration

(See Figure 26)

The WEP settings configured under this tab are shared by all SSIDs configured to use WEP. TRIMAR APs used in WDS mode are limited to using WEP encryption only.

Enable WEP: Check this box to enable WEP. Each SSID using WEP must also have its [WEP configuration](#) box checked.

Default WEP Key: Select the default WEP transmission key (1-4). The radio will use this key for transmissions only. It will be able to receive data encrypted using the other three keys.

Authentication: Open and Shared authentication is supported.

Factory default: Open

WEP key length: Both 64-bit and 128-bit key lengths are supported.

WEP key 1-4: Enter the WEP keys using hexadecimal characters. (1-9 and A-F)

WEP pass phrase generator

This is a feature and should not be confused with a standard pass phase field entry. To use this feature enter the desired pass phase into the pass phrase field. Click on the "Generate WEP keys" function and all 4 keys will be automatically generated and populate the WEP key fields above.

The generated WEP keys are not viewable. To use corresponding keys to allow other TRIMAR radios to authenticate, use the exact same pass phrase in their respective pass phrase generators.

Warning: Other pass phrase generators may not be compatible with the TRIMAR WEP key generator.

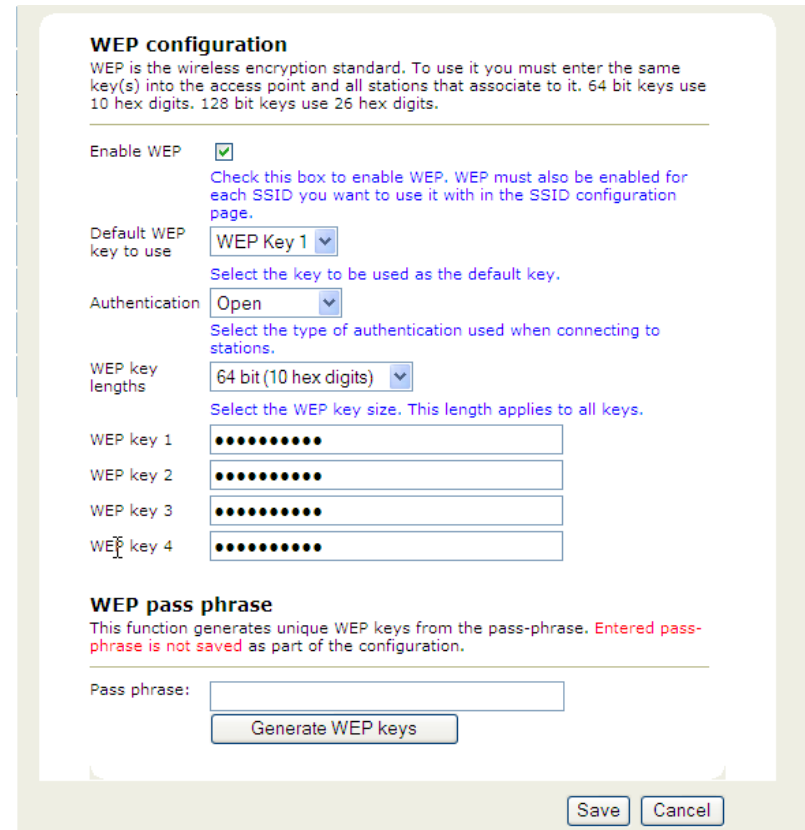


Figure 26: WEP configuration

9. Access Control Tab

Access Control

(See Figure 27)

These controls allow administrators to specifically allow stations to associate with the access point. This is accomplished by entering the allowed stations' unique MAC addresses into the MAC address fields. Stations whose MAC addresses are not entered into the list will not be able to authenticate with the TRIMAR AP.

Access Control is also commonly referred to as **MAC address filtering**.

Enable access control: Check this box if Access Controls are to be used.

MAC address 1-48: 48 MAC address fields are available, one slot for each of the 48 stations that the TRIMAR AP can simultaneously support.

The MAC address needs to be entered as hexadecimal numbers without delimiters. (A valid MAC address entry has 12 characters).

Example: 0011F5910E06

Access Control

On this page you can enable Access Control. If enabled, only the MAC addresses entered into the 'MAC address' boxes are allowed to associate to this AP. Note that you can cut and paste the addresses from the 'Station List' page into the MAC address boxes. Any new settings will not take effect until the device is rebooted.

Enable access control (Check this box to enable access control.)

MAC address 1	<input type="text"/>
MAC address 2	<input type="text"/>
MAC address 3	<input type="text"/>
MAC address 4	<input type="text"/>
MAC address 5	<input type="text"/>
MAC address 6	<input type="text"/>
MAC address 7	<input type="text"/>
MAC address 8	<input type="text"/>
MAC address 9	<input type="text"/>
MAC address 10	<input type="text"/>
MAC address 11	<input type="text"/>
MAC address 12	<input type="text"/>
MAC address 13	<input type="text"/>
MAC address 14	<input type="text"/>
MAC address 15	<input type="text"/>
MAC address 16	<input type="text"/>
MAC address 17	<input type="text"/>
MAC address 18	<input type="text"/>
MAC address 19	<input type="text"/>
MAC address 20	<input type="text"/>
MAC address 21	<input type="text"/>
MAC address 22	<input type="text"/>
MAC address 23	<input type="text"/>

Figure 27: Access Control

10. WDS Tab

Wireless Distribution System

(See Figure 28)

WDS is one of the most important TRIMAR AP features. It allows TRIMAR APs to communicate with each other as well as other makes of APs to create radial and linear wireless meshes. Each TRIMAR AP can be linked with up to six other WDS capable APs. This combination can be the basic component of much larger mesh networks as meshes can easily be linked with other meshes.

TRIMARs APs in WDS mode must be on the same channel, but they can use completely separate SSIDs.

Enable WDS: Check this box to enable the TRIMAR AP's WDS feature.

AP MAC address 1-6: Enter the MAC addresses in hexadecimal characters of all other APs that will be a part of the same mesh.

Enable STP: The Spanning Tree Protocol (STP) must be enabled for all TRIMAR APs that have a physical (Ethernet) connection as well as a wireless connection with the same network. This will prevent network loops from occurring due to the multiple paths to the same network.

Enable WEP for WDS: Check this box to enable WEP encryption to be used. The WEP keys need to be entered under the WEP Security Tab.

Use separate MAC: For administrative purposes it may be desirable to manually assign the Ethernet port a different MAC address. Check this box to enable this feature.

Ethernet MAC address: Enter in hexadecimal characters a new MAC address for the Ethernet port.

WDS table: This button is used to access the WDS table. WDS must be enabled to use this feature.

For load-balance management and other network administrative functions, use a [TRIMAR Controller](#) to manage all aspects of a TRIMAR WDS mesh.

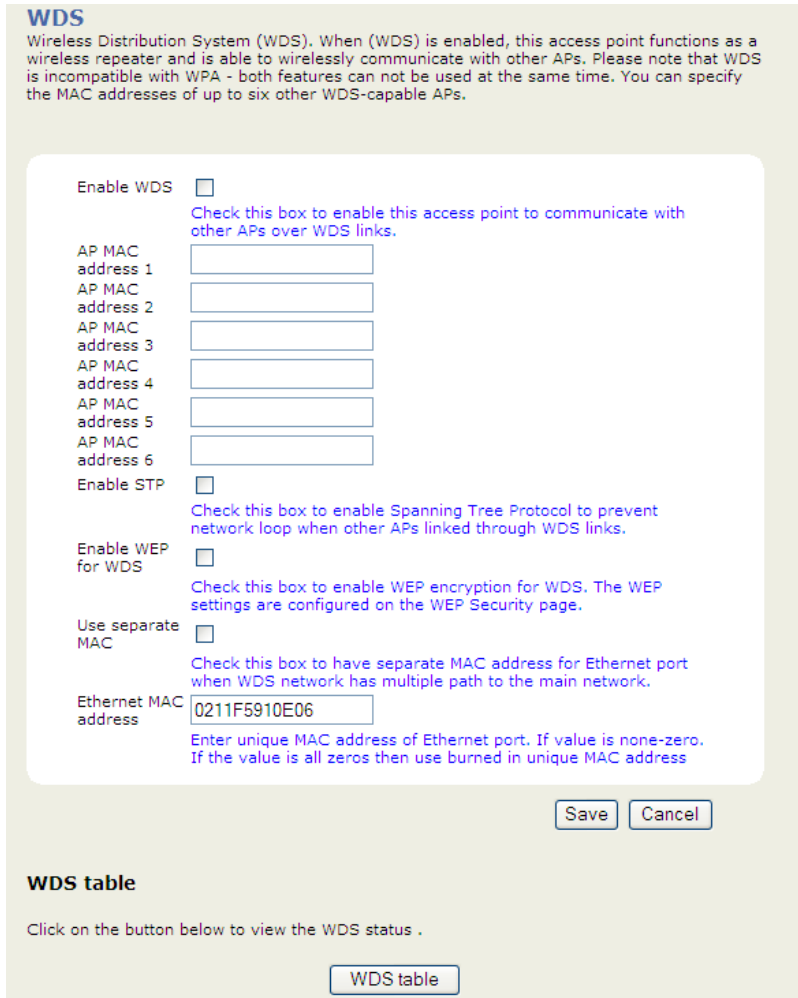


Figure 28: WDS configuration

WDS Tab

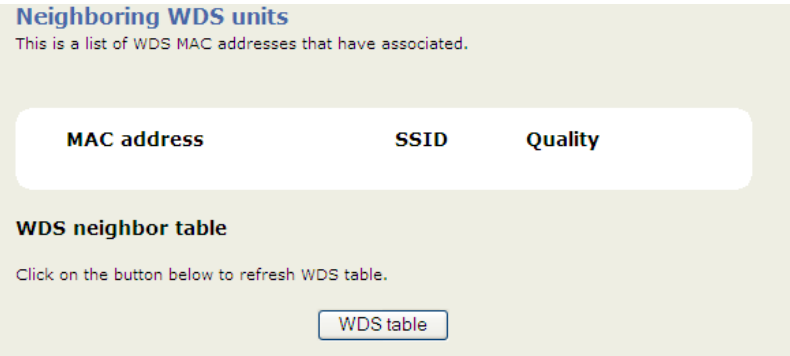
(.. /continued)

WDS neighbor table

(See Figure 29)

This display reports on the radios that are a part of the same mesh and includes information such as the associating units MAC address, SSID and the wireless signal quality.

WDS table: This button refreshes the display.



The screenshot shows a web interface for the WDS neighbor table. At the top, it says "Neighboring WDS units" and "This is a list of WDS MAC addresses that have associated." Below this is a table with three columns: "MAC address", "SSID", and "Quality". Underneath the table, there is a section titled "WDS neighbor table" with the instruction "Click on the button below to refresh WDS table." and a button labeled "WDS table".

Figure 29: WDS Table

11. DHCP Server Tab

DHCP Server Configuration

(See Figure 30 and Figure 31)

The TRIMAR AP can be configured to function as a DHCP server. To use this feature, since the TRIMAR AP can only issue IP addresses within its own IP subnet, **the TRIMAR AP must be given an IP address in the same IP subnet as the IP addresses it will be assigning.**

DHCP server: Check this box to enable the TRIMAR AP's DHCP functions.

DHCP address range start: Enter the first number of the fourth octet in the range of IP addresses to be assigned.

DHCP address range end: Enter the last number of the fourth octet in the range of IP addresses to be assigned.

DHCP timeout: Enter the number of minutes that an issued IP address will remain valid.

Preferred DNS server: IP address of the primary DNS server.

Alternate DNS server: IP address of the alternate DNS server.

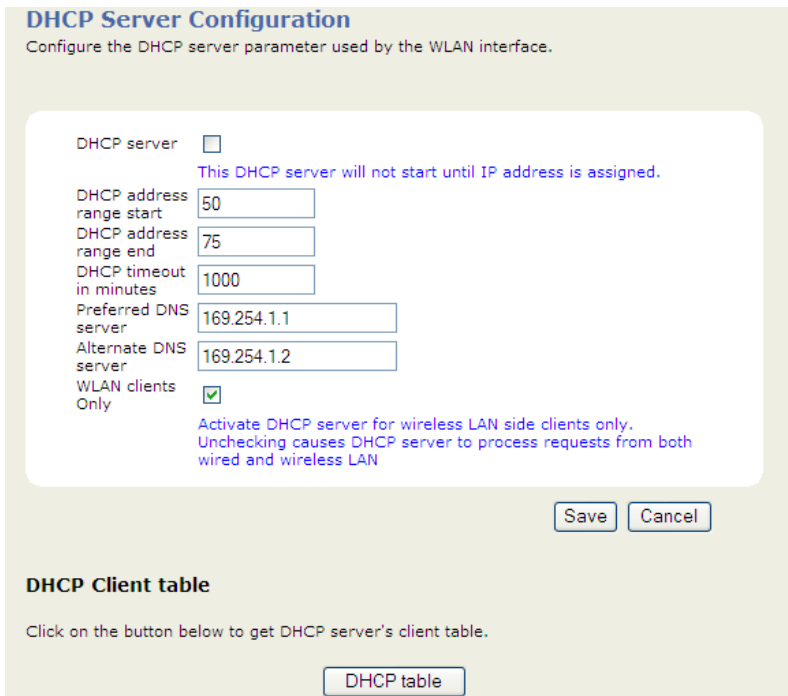
WLAN client only: Optionally, the TRIMAR AP can be instructed to offer IP addresses only to wireless clients. Check this box to enable this feature. This function may be mandatory in some network situations.

DHCP table: On this tab, use this button to **access** the DHCP server client table (Figure 30).

DHCP server client table

This report shows information as to which PCs have been assigned DHCP IP addresses by the TRIMAR AP.

DHCP table: On this tab, use this button to **refresh** the DHCP server client table (Figure 31).



DHCP Server Configuration
Configure the DHCP server parameter used by the WLAN interface.

DHCP server This DHCP server will not start until IP address is assigned.

DHCP address range start

DHCP address range end

DHCP timeout in minutes

Preferred DNS server

Alternate DNS server

WLAN clients Only

Activate DHCP server for wireless LAN side clients only. Unchecking causes DHCP server to process requests from both wired and wireless LAN

DHCP Client table

Click on the button below to get DHCP server's client table.

Figure 30: DHCP Server Configuration



DHCP server client table
Information.

NOTE: DHCP client list

Host name	MAC address	IP address	lease

DHCP Client table

Click on the button below to refresh DHCP table.

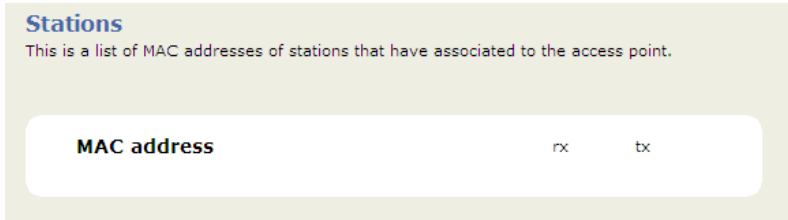
Figure 31: DHCP server client table

12. Stations Tab

Stations

(See Figure 32)

The stations tab display shows information about all stations that have associated with the TRIMAR AP. Information polled from the associated stations include the individual stations' MAC addresses as well as the number of packets sent and received.



MAC address	rx	tx
-------------	----	----

Figure 32: Associated stations display

13. Save Tab

Save Configuration

(See Figure 33, Figure 34 and Figure 35)

A TRIMAR AP's configuration can be saved to a template and reapplied to other TRIMAR APs. This feature makes it easy to configure and deploy multiple units quickly and without having to re-type the configuration information into every unit. In most instances, all that needs to be changed are the individual unit's IP addresses and adjustments to the WDS settings so that units do not refer to themselves.

Before creating the template, the TRIMAR AP's IP address needs to be added to the PC's Local Intranet zone. (See below for instructions).

Create Template: Click on this button to create the template. Another window will open advising that a wait may be necessary whilst the computer creates the file. Once the file is created, a file navigation window will open allowing an opportunity to choose where to save the file and renaming it.

Default name is: **settings.htm**

TURN OFF THE WEB-BROWSER'S POP-UP BLOCKER OR THE TEMPLATE FILE WILL NOT BE CREATED

Assigning the TRIMAR AP to the Local Intranet Zone

1. Go to the Microsoft® Windows **Control Panel**.
2. Find the **Internet Options** icon and double click to open the application.
3. Select the "**Security**" tab.
4. Select the **Local Intranet** icon. The "**Sites**" button will become available.
5. Click on the "**Sites**" button. In the panel that appears select "**advanced**".
6. Enter the IP address of the TRIMAR AP, include the "http://". (Example: **http://169.254.1.240**)
7. Click "**Add**". This will add the TRIMAR AP's IP address to the list.
8. Click the "**OK**" buttons to close all the windows.

Save Template

NOTE: This page allows the user to create a save template. This template can be used to restore previous settings or to program multiple devices with identical settings. In order to create the template, the Trimar IP address needs to be added to your local intranet zone. Please see the Technical Manual for additional details.

Create Template

Click this button to save the current Access Point settings to a file. Open the template file from your computer to upload the settings back to the device.

Figure 33: Save Configuration

Saving Trimar Settings

Saving Trimar settings to file...

NOTE: This may take up to one minute.

Please do not close this window until the file has been saved.

The settings can be loaded onto any Trimar AP by opening the saved file from your computer.

Figure 34: Saving TRIMAR Settings

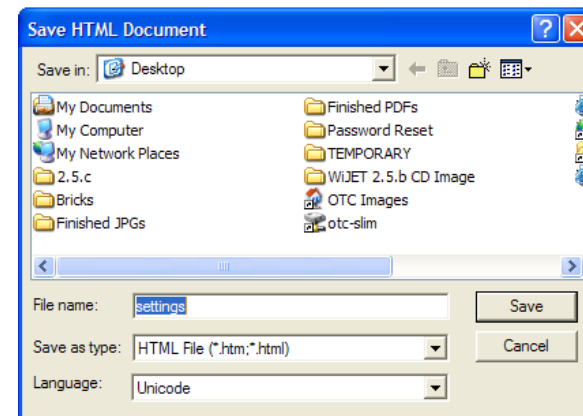


Figure 35: Save the template file

Save Tab

(.. /continued)

Uploading a template

(See Figure 36)

To upload a template file into a TRIMAR AP open the **settings.htm** file using a web-browser.

Target AP: Enter the IP address of the TRIMAR AP to which the template is to be applied.

Upload Settings: Click on this button to upload the template file. This can take several minutes.

Once the template has fully uploaded, the web-based administration utility for the target TRIMAR AP will be automatically started. Negotiate the password challenge screen when it appears. **Wait until the progress bar stops**, then reboot the TRIMAR AP so that the uploaded configurations can be applied.

Once it restarts, review the uploaded configurations. In particular, there may be some fields that needs to be altered (such as its IP address or custom MAC address settings).

TURN OFF THE WEB-BROWSER'S POP-UP BLOCKER OR THE TEMPLATE FILE WILL NOT BE UPLOADED

Note: In particular, be aware that the template is an exact copy of the settings of the TRIMAR AP on which the template was created. If this unit has a static IP address, all subsequent TRIMAR APs to which the template has been applied will be given the same identical IP address.

Target AP:

Upload Settings

Device name

Device name

The name Trimar will identify itself with to Locator (not the same as the SSID).

IP settings

IP Address Mode Static DHCP

Select 'DHCP' to get the IP settings from a DHCP server on your network. Select 'Static' to use the IP settings specified on this page.

Default IP address

Type the IP address of your device

Default subnet mask

The subnet mask specifies the network number portion of an IP address. The factory default is 255.255.255.0.

Default gateway

This is the IP address of the gateway that connects you to the internet. The factory default is 192.168.1.1.

Security

User name

User name for web configuration access.

Administrator password

Password for web configuration access. You must enter the same password into both boxes, for confirmation

SNMP Setting

SNMP enabled

Figure 36: Uploading a template

14. Help Tab

Contact our Technical Support department for additional technical assistance for configuring and deploying your TRIMAR AP.

OTC Wireless Technical Support Department can be contacted by either email, phone or the web-mail form on the [Pegasus Wireless Corporation](http://www.otcwireless.com) web site:

Email: support@otcwireless.com
Website: <http://www.otcwireless.com/support/technicalsupport.html>
Phone: (510) 490-8288 ext 244
Fax: (510) 440-7046



Help

For additional information about the operation of this unit, please consult the Technical Manual.

Support and Service information can be found on our Web site: <http://www.otcwireless.com/support/support.htm>.

You can find useful FAQ and downloadable articles from this site.

Our telephone support number is:

510-490-8288.

Telephone support is available 9 AM to 5 PM, Pacific Time, Monday through Friday.

Figure 37: Help

Appendix

Limited Warranty

The seller warrants to the end user ("Customer") that this product will be free from defects in workmanship and materials, under normal use and service, for one (1) year from the date of purchase. The seller's sole obligation under this express warranty shall be, at the seller's option and expense, to repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item.

All returns must be authorized by Pegasus Wireless Corporation and accompanied by a Return Materials Authorization (RMA).

All products that are replaced will become the property of the seller. Replacement products may be new or reconditioned.

FCC Rules and Regulations - Part 15

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by unplugging the equipment and then plugging it back in, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Changes or modifications not expressly approved by OTC Wireless could void the user's authority to operate the equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Compliance Information Statement

FCC Part 15 Declaration of Conformity (DoC)

The following equipment:

Product Name: **TRIMAR 802.11 a/b/g Wireless AP/BRIDGE/REPEATER**
Model Number: **TRIMAR** is herewith confirmed to comply with the requirements of FCC Part 15 rules. The operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

FCC ID: MKZTRIMAR

A declaration of conformity with the requirements of the directives is available from: Pegasus Wireless Corporation, 48499 Milmont Drive, Fremont, California 94538, USA

Exposure to Radio Frequency Radiation

Caution: The radiated output power of this device is far below the FCC radio frequency exposure limits. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, a minimum separation of 20 cm (8 inches) is recommended between the antenna and any persons.