Broadband Wireless Access 4.9GHz Outdoor Subscriber

User Manual

Includes install, configuration and trouble shooting information for the broadband wireless access outdoor radio.

Version 1.0.4

Website: www.wnint.com
Address : 2146 Bering Drive, San Jose, CA 95131, USA
TEL : +1-408-432-8892
FAX : +1-408-432-8896

Nov, 2008

Copyright

Copyright © 2007 all rights reserved. No part of this publication may be reproduced, adapted, stored in a retrieval system, translated into any language, or transmitted in any form or by any means without the written permission of the supplier.

About This Manual

This manual includes install, configuration and trouble shooting for the 4.9GHz outdoor subscriber. It can help you in avoiding the unforeseen problems and use the outdoor radio correctly.

Technical Support

If you have difficulty resolving the problem while installing or using the wireless bridge, Please contact the supplier for support.

IMPORTANT NOTE: To comply with the FCC RF exposure compliance requirements, no change to the antenna or the device is permitted. Any change to the antenna or the device could result in the device exceeding the RF exposure requirements and void user's authority to operate the device.

FCC Notice

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. 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 turning the equipment off and on, 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 technician for help.

Warning : Please attach the proper antenna to the external antenna type and ensure the total EIRP comply with the rules which defined by the local government organization.

Table of Contents

Conventions

This publication uses the following conventions to convey instructions and information:

NOTE	This symbol means ***reader take note.*** Notes contain helpful suggestions or references to materials not contained in this manual.
CAUTION	This symbol means ***reader be careful.*** In this situation, you might do something that could result in equipment damage or loss of data.
WARNING	This warning symbol means ***danger***. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

Chapter 1 Introduction

Broadband Wireless Access (BWA) 4.9GHz outdoor subscriber is a cost-effective point-to-point / point-to-multipoint (CPE) solution for ISM band wireless backhaul deployment and could be equipped with Ethernet interface.

New adding Vlan functionality allows a single network AP to behave as “8” number of virtual network APs. This does away with the limitation by the sheer number of Ethernet connections that need APs acting as a proxy.

This ISM band radio provides customers with the greatest flexibility to deploy applications due to customers’ need and would be easily upgraded or switched to another interface with the lowest cost.

This radio is incorporated with Time Division Duplex technology that they could be operated on a single channel. The Ethernet products are primarily designed to provide standard Ethernet interface in a wireless link between distant sites.

1-1 Features and Benefits

■ EFFECTIVE SPECTRUM UTILITY

This Wireless Bridge uses advanced technology to narrow the channel into smaller bandwidths than other wireless radios, better serving the needs of the operator.

■ FLEXIBILITY

Detachable antennas allow operators to select the optimum antenna for specific environments.

■ MANAGEABILITY

Through the Web-based utility, the Wireless Bridge is fully manageable locally and remotely. In addition, built-in SNMP support lets the operator, whether ISP or enterprise, expand the network infrastructure with ease.

■ FETURES

- ➢ Provides the easy installation and high performance outdoor PTP / PTMP wireless bridge up to 30 KM.
- ➢ With a data rate up to 5.5Mbps / 10Mbps / 20Mbps (with different bandwidth: 5MHz / 10MHz and 20MHz), the system is much faster than an E1/T1 data link. Customer can select the suitable bandwidth via the software.
- ➢ Regatta mode increase the performance up to 35%.

  Unique technology called regatta mode can enhance the performance of the radio up to 25~35%
- ➢ VAPs (VLAN)

  Assign Multi-SSIDs on your radio (one SSID per VAP) to differentiate policies and services among users forming a wide variety of VLANs.
- ➢ Technique operating in the 4.9GHz.

- Versatile Quality of Service / Time-Division Multiplexing technique. TDM tech can avoid the packets collision and send the packets more efficient and stable to improve the quality of voice and data transmission. The data rate of the CPE radio can be set in fractional (nx64 Kbps).
- Transmit Power Control :

  Supports settable transmit power levels to adjust coverage cell size, ranging f from full, half(50%), quarter(25%) eighth(12.5%) and min
- Multiple security settings per VLAN with up to 8 VLANs

  Security settings for multiple groups; so employees, guests and contractors now easily and securely share the same infrastructure
- Provides WEP 64 bit / 128 bit / 152 bit, WPA-PSK and WPA2(AES) as well as MAC access control to increase security.
- Provides Web-based configuration utility, user friendly interface.
- IP-68 rated weatherproof housing

Chapter 2 Hardware Installation

This chapter describes initial setup of the Wireless Bridge.

Warnings

WARNING

In order to comply with international radio frequency (RF) exposure limits, panel antennas should be placed at a minimum of 23.6 inches (60 cm) from the bodies of all persons.

WARNING

Do not work on the system or connect or disconnect cables during periods of lightning activity.

WARNING

This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

WARNING

Ultimate disposal of this product should be handled according to all national laws and regulations.

WARNING

Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.:NFPA 70, National Electrical Code, Article 810, in Canada: Canadian Electrical Code, Section 54).

WARNING

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

WARNING

To meet regulatory restrictions, the radio and the external antenna must be professionally installed. The network administrator or other IT professional responsible for installing and configuring the unit is a suitable professional installer. Following installation, access to the unit should be password protected by the network administrator to maintain regulatory compliance.

CAUTION

The 4.9GHz outdoor subscriber and POE injector can be damaged by incorrect power application. Read and carefully follow the installation instructions before connecing the system to its power source.

Follow the guidelines in this chapter to ensure correct operation and safe use of the ISM band radio.

2-1 Product Kit

Before installation, make sure that you the following items:

◆ **4.9GHz outdoor subscriber**	x 1
◆ **Power over Ethernet**	x 1
◆ **Power Adapter**	x 1
◆ **Power Cord**	x 1
◆ **Mounting kit**	x 1
◆ **Button head socket cap screw 4*6 iso for reset button**	x 2
◆ **Product CD**	x 1
◆ **Quick Installation Guide**	x 1

NOTE: If any of the above items are missing or damaged, please contact your local dealer for support.

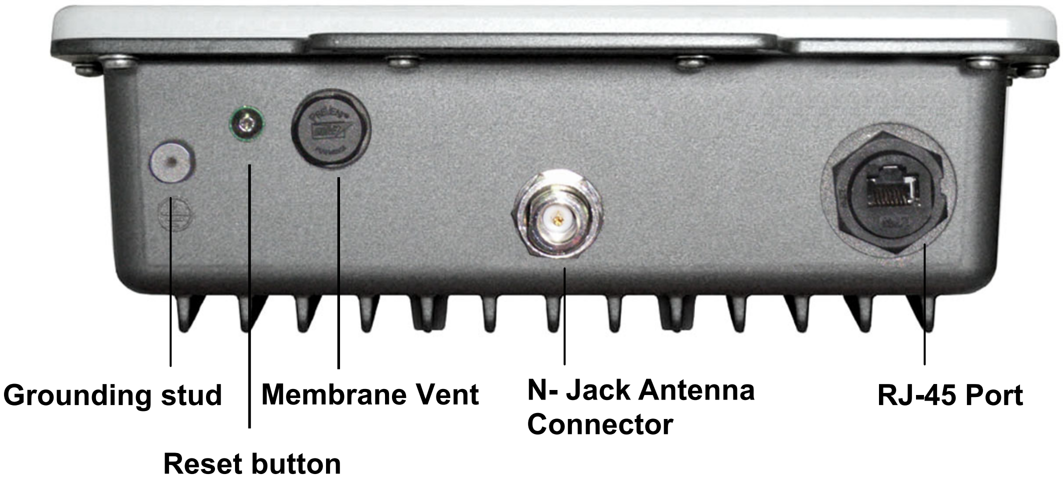
2-2 System Requirements

Before installing the 4.9GHz outdoor subscriber, please make sure that these equirements have been met:

- A 10/100 Mbps Local Area Network device such as a hub or switch. (optional)
- Category 5 UTP or STP networking cable. (From the PC to POE)
- Category 5 SSTP or SFTP networking cable. (From the radio to POE)
- A Web browser for configuration: Microsoft IE 5.0 or later, or Netscape Navigator 5.0 or later version.
- Installing TCP/IP protocol to the computer.

2-3 Mechanical Description

Please refer to the following table for the meaning of each feature.

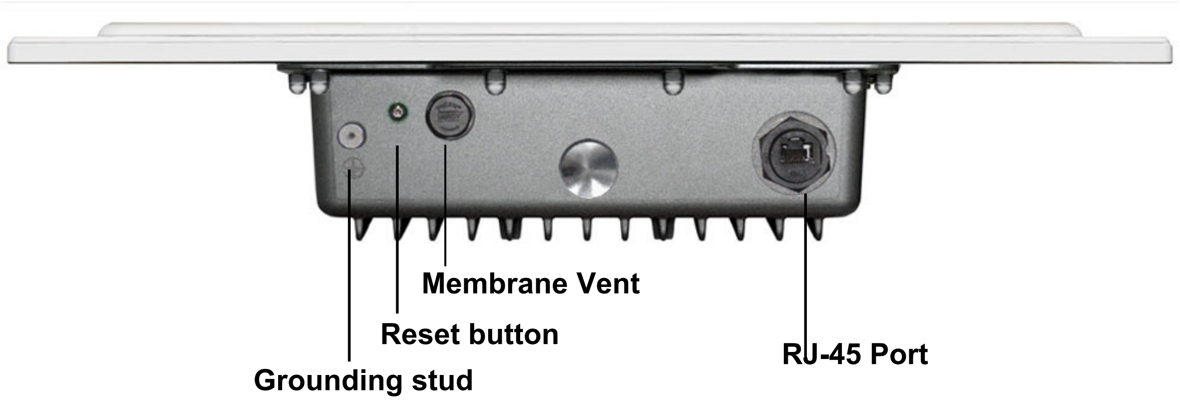


Outdoor Multi-function Radio Figure

1	**RJ-45 Port**	Use the SFTP cat.5 cable with weatherproof connector to connect to the "To ODU" side of the POE injector.
2	**N- Jack Antenna Connector**	Here you can attach the proper antenna with the outdoor radio to wirelessly connect to the networks. In order to improve the RF signal radiation of your antenna, proper antenna installation is necessary.
3	**Grounding stud**	Connect to the ground conductor with the ground wire.
4	**Reset button**	Revolve the screw and insert a stick to press in and hold the reset button for 5~10 seconds, the radio will back to factory default settings. PS. The spec of the screw is "Button head socket cap screw 4*6 iso".
5	**Membrane Vent**	1. Moisture vapor permeable to help aid in condensation and fogging reduction in the ODU. 2. High airflow allows pressure equalization to prevent stress on enclosure seals

WARNING

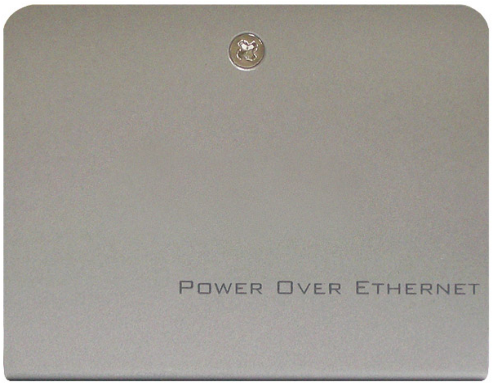
This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

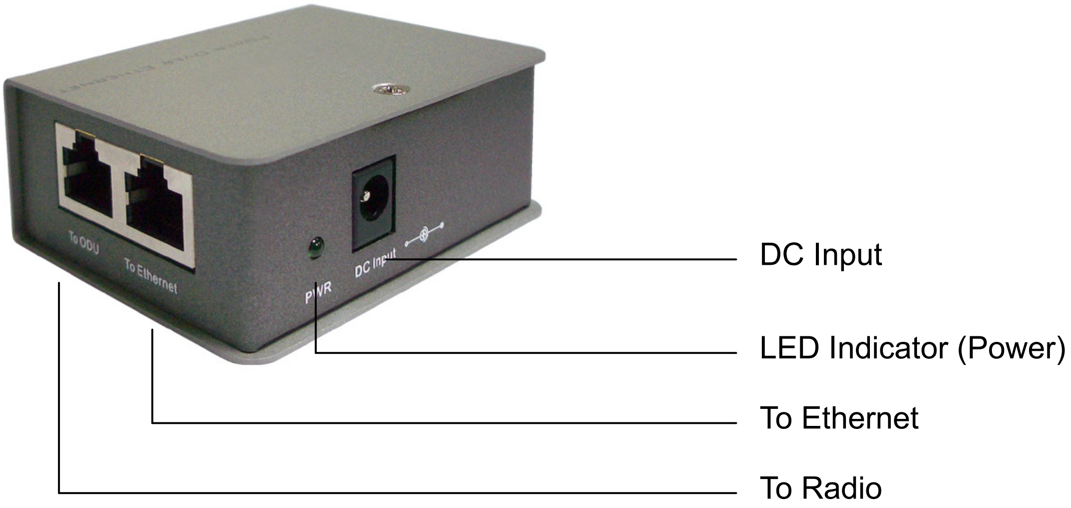


Outdoor Subscriber Figure

1	**RJ-45 Port**	Use the SFTP cat.5 cable with weatherproof connector to connect to the “To ODU” side of the POE injector.
2	**Grounding stud**	Connect to the ground conductor with the ground wire.
3	**Reset button**	Screw off this screw and insert a stick to press in and hold the reset button for 5~10 seconds, the radio will back to factory default settings. PS. The spec of the screw is “Button head socket cap screw 4*6 iso”.
4	**Membrane Vent**	1. Moisture vapor permeable to help aid in condensation and fogging reduction in the ODU. 2. High airflow allows pressure equalization to prevent stress on enclosure seals

POE





Power Over Ethernet Injector Figure

1	**To Ethernet**	This RJ-45 port is used to connect to the 10/100 Base T complied device such as switch, router or PC.
2	**To ODU**	This RJ-45 port is used to connect to the ODU.
3	**DC Input**	Connect to the Power adaptor for DC input.
4	**LED Indicator**	Power LED

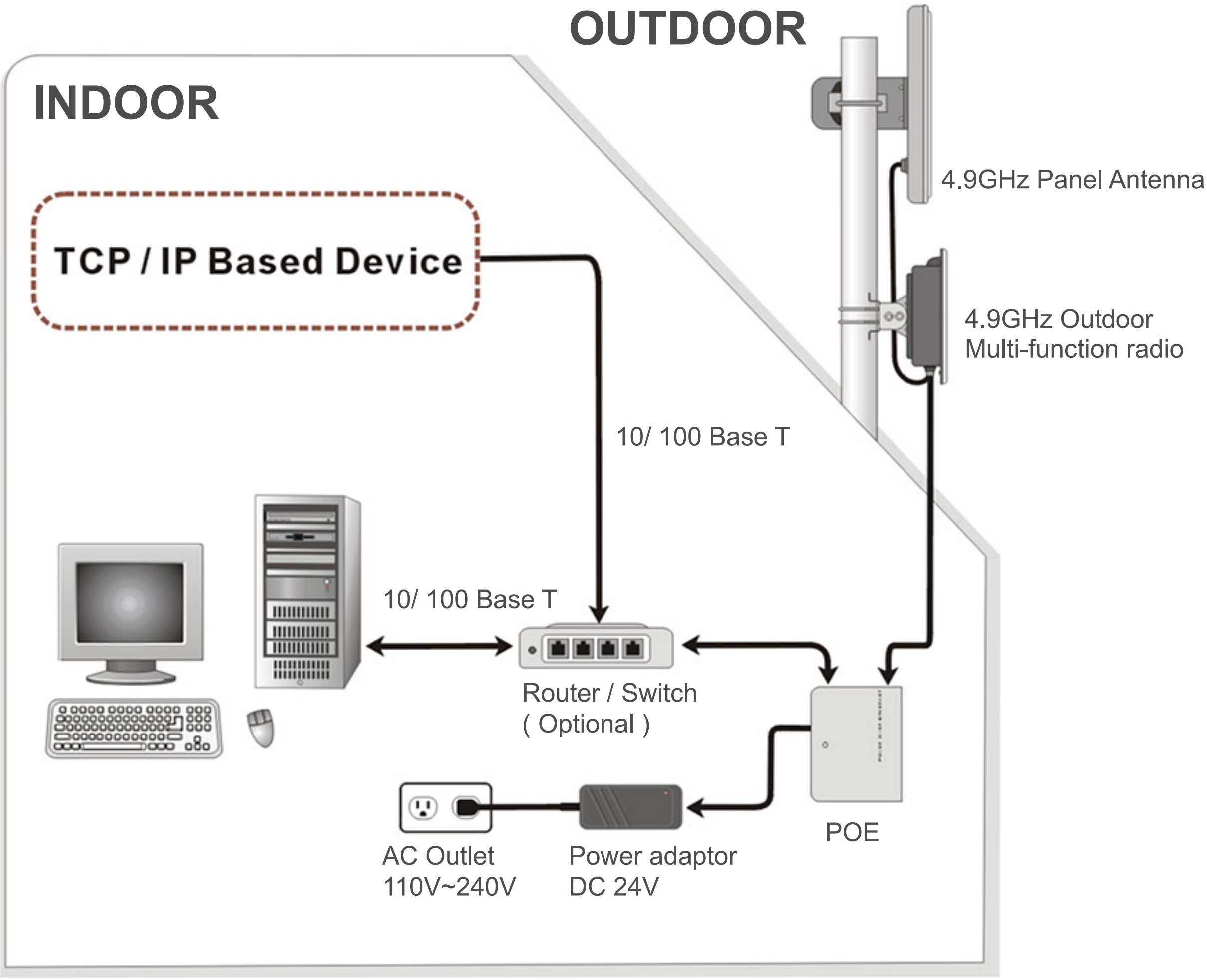
2-4 Hardware Installation

The 4.9GHz outdoor subscriber is a radio device, so it is susceptible to common causes of interference that can reduce throughput and range. Follow these basic guidelines to ensure the best possible performance:

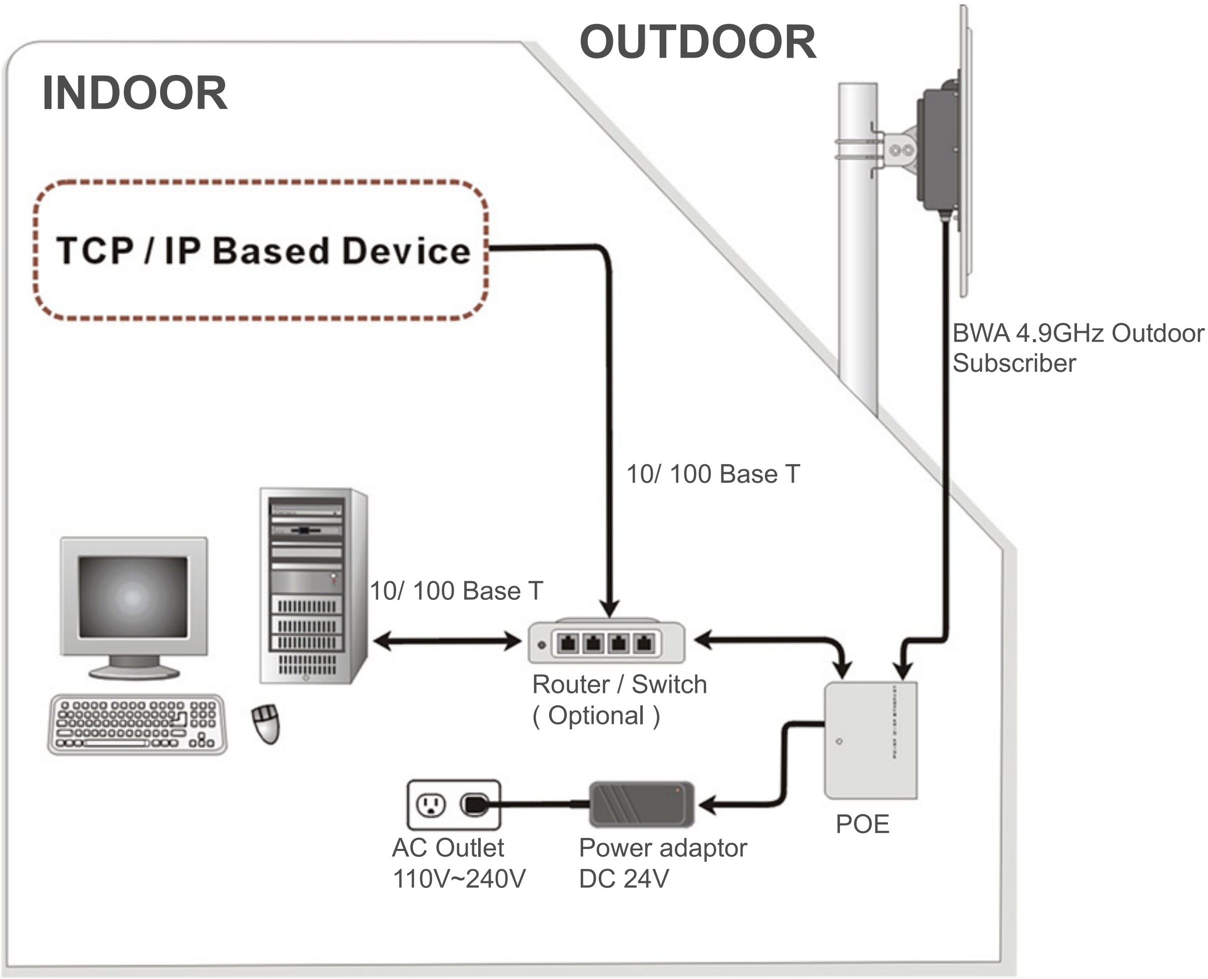
- IF there is any other 4.9GHz RF device deployed around the outdoor radio, try to set the channel to the non-overlapping one.
- Install the bridge at a height sufficient place where structures, trees, or hills do not obstruct radio signals to and from the unit. A clear line-of-sight path can guarantee the performance of the RF link.

Site Surveys

Clear and flat area provide better RF range and data rate, on the contrary, physical obstructions such as trees, electric tower, hills or buildings can reduce the performance of RF devices. Do not deploy your radios in the location where there is any obstacle between the antennas.



Hardware Installation Figure (external antenna type)



Hardware Installation Figure (integrated antenna type)

Configure and verify the 4.9GHz outdoor subscriber operations first before you mount the radio in a remote location.

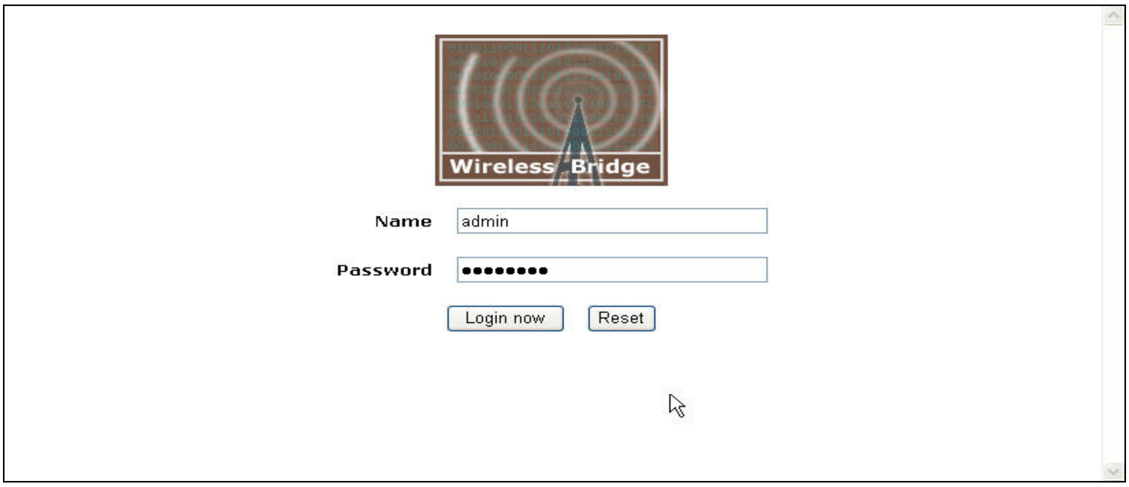
Power Over Ethernet Injector is not a waterproof unit, should not be exposed to outdoor without any protection.

Chapter 3   Configuration

3-1 Start-up and Log in

In order to configure the Wireless Bridge, use the web browser and please do the following:

1. Type the IP address **http://192.168.1.1** of this ISM band radio in the Location (for IE) or Address field and press Enter.
2. Enter the system name (the default setting is **"admin"**) and password (the default setting is **"password"**).
3. Click on the **"Login now"** button.
4. The main page will appear.



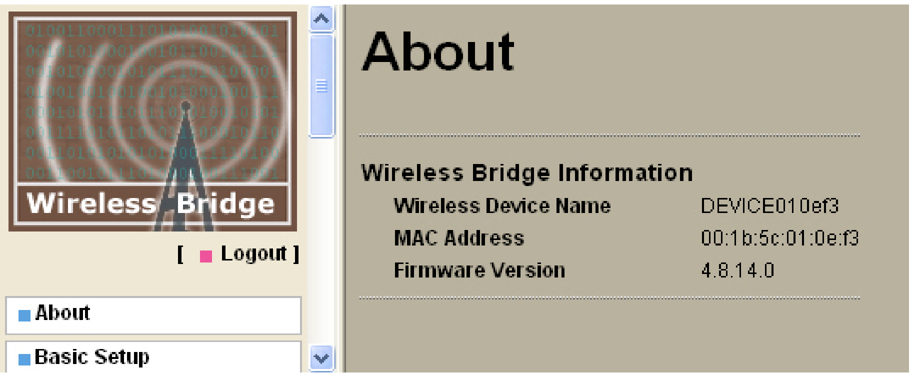
Name admin

Password ●●●●●●●●●

After you have logged-in the main page, the **About**, **Basic Setup**, **Wireless Setup, Tools, Status**, **Management** buttons will be shown. The main menu provides links to the whole sections of the web configuration interface.

About

The About screen describes the product information briefly. Information of the radio includes **Wireless Bridge Name**, **MAC Address**, and **Firmware Version**.

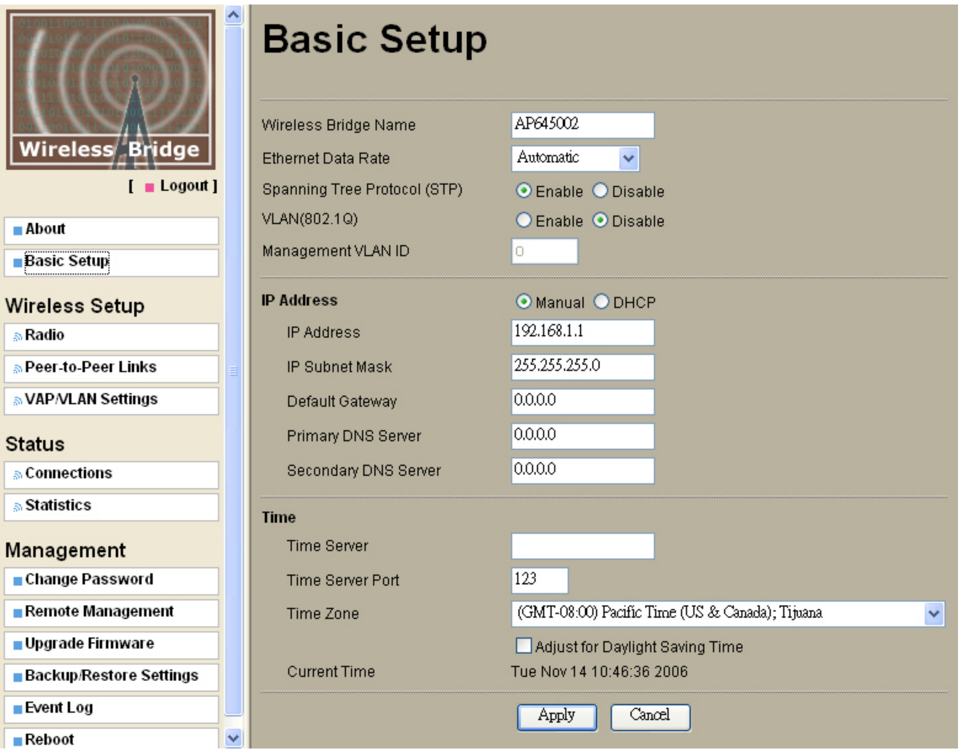


About

Wireless Bridge Information

Wireless Device Name	DEVICE010ef3
MAC Address	00:1b:5c:01:0e:f3
Firmware Version	4.8.14.0

Basic Setup

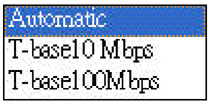


Basic Setup

Wireless Bridge Name	AP645002
Ethernet Data Rate	Automatic
Spanning Tree Protocol (STP)	● Enable ○ Disable
VLAN(802.1Q)	○ Enable ● Disable
Management VLAN ID	0
IP Address	● Manual ○ DHCP
IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Time	
Time Server	
Time Server Port	123
Time Zone	(GMT-08:00) Pacific Time (US & Canada); Tijuana
	□ Adjust for Daylight Saving Time
Current Time	Tue Nov 14 10:46:36 2006

The **Wireless Bridge Name** is used to give a name to your Wireless Bridge. This will enable you to manage your Wireless Bridge more easily if you have multiple radios on your network.

Ethernet Data Rate: you can choose the Ethernet data rate you need



Automatic
T-base10 Mbps
T-base100Mbps

Spanning tree protocol (STP): You may Enable or Disable the Spanning Tree Protocol used in this Wireless Bridge.

IP Address: Type the IP address you want to set to your Wireless Bridge. (Default: 192.168.1.1).

IP Subnet Mask: The Wireless Bridge's Subnet Mask must be the same as your Ethernet network. We recommended that you do NOT change the value. (Default: 255.255.255.0).

Default Gateway: The Wireless Bridge will use this value for default Gateway.

Primary DNS Server: The Wireless Bridge will use this value for primary Domain Name Server.

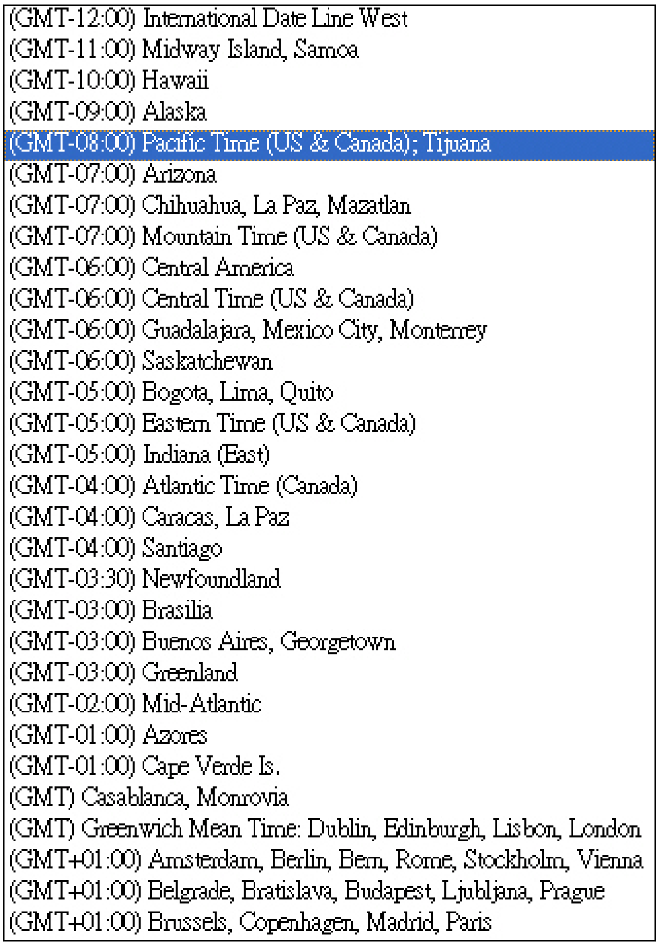
Secondary DNS Server: The Wireless Bridge will use this value for secondary Domain Name Server.

Time: While you connect this Wireless Bridge to Internet, it could automatically synchronize the current time with the Time Server that you have set.

Time Server: the central time of the Time Server.

Time Server Port: the port of the Time Server.

Time Zone: You may select the appropriate local time zone for your radio from a list of all available time zones. Default: GMT.

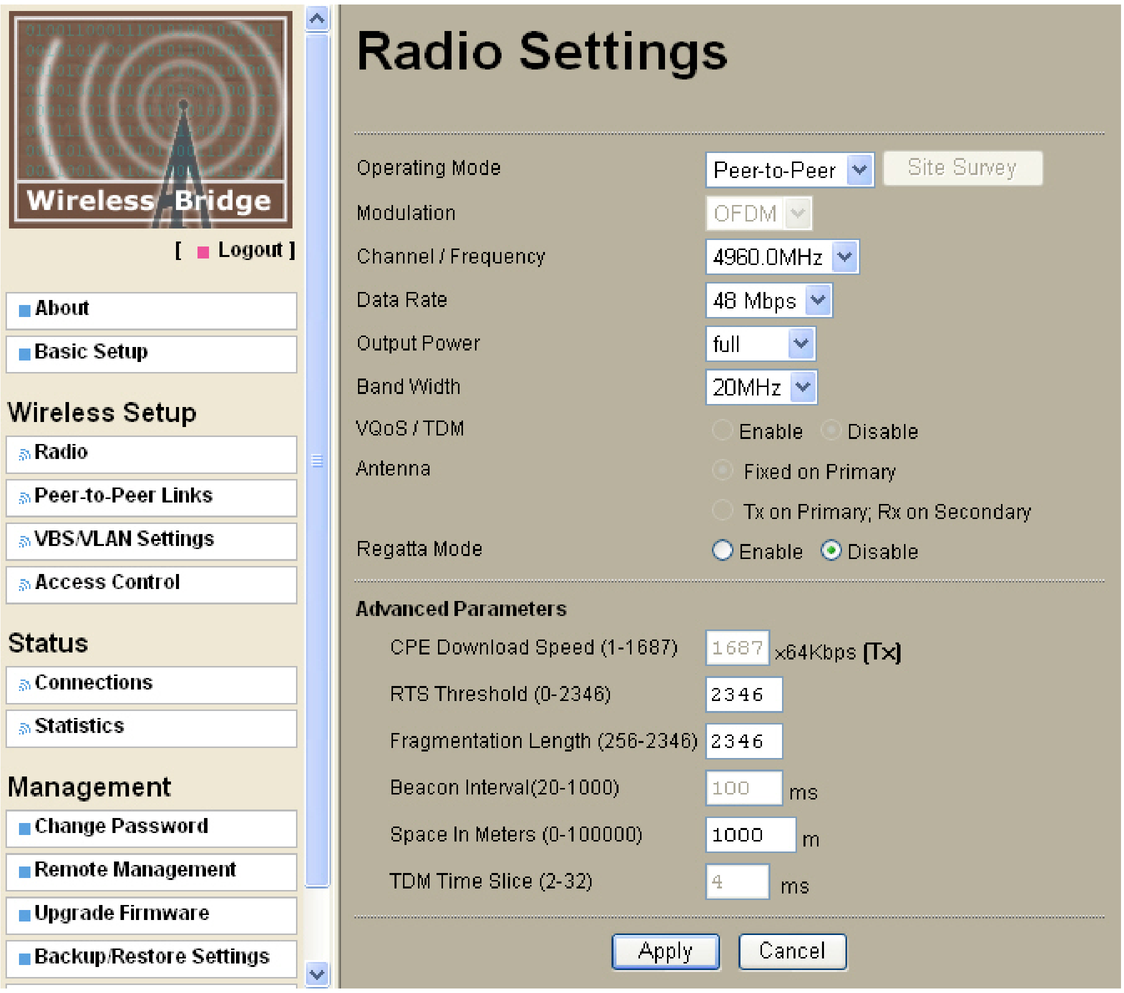


(GMT-12:00) International Date Line West
(GMT-11:00) Midway Island, Samoa
(GMT-10:00) Hawaii
(GMT-09:00) Alaska
(GMT-08:00) Pacific Time (US & Canada); Tijuana
(GMT-07:00) Arizona
(GMT-07:00) Chihuahua, La Paz, Mazatlan
(GMT-07:00) Mountain Time (US & Canada)
(GMT-06:00) Central America
(GMT-06:00) Central Time (US & Canada)
(GMT-06:00) Guadalajara, Mexico City, Monterrey
(GMT-06:00) Saskatchewan
(GMT-05:00) Bogota, Lima, Quito
(GMT-05:00) Eastern Time (US & Canada)
(GMT-05:00) Indiana (East)
(GMT-04:00) Atlantic Time (Canada)
(GMT-04:00) Caracas, La Paz
(GMT-04:00) Santiago
(GMT-03:30) Newfoundland
(GMT-03:00) Brasilia
(GMT-03:00) Buenos Aires, Georgetown
(GMT-03:00) Greenland
(GMT-02:00) Mid-Atlantic
(GMT-01:00) Azores
(GMT-01:00) Cape Verde Is.
(GMT) Casablanca, Monrovia
(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
(GMT+01:00) Brussels, Copenhagen, Madrid, Paris

Note: If you complete the settings, please click on "Apply" for changes to take effect.

3-2 Wireless Setup

Wireless Setup / Radio Settings



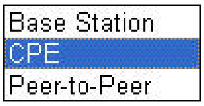
Radio Settings

Operating Mode	Peer-to-Peer ▾ Site Survey
Modulation	OFDM ▾
Channel / Frequency	4960.0MHz ▾
Data Rate	48 Mbps ▾
Output Power	full ▾
Band Width	20MHz ▾
VQoS / TDM	○ Enable ○ Disable
Antenna	● Fixed on Primary ○ Tx on Primary; Rx on Secondary
Regatta Mode	○ Enable ● Disable

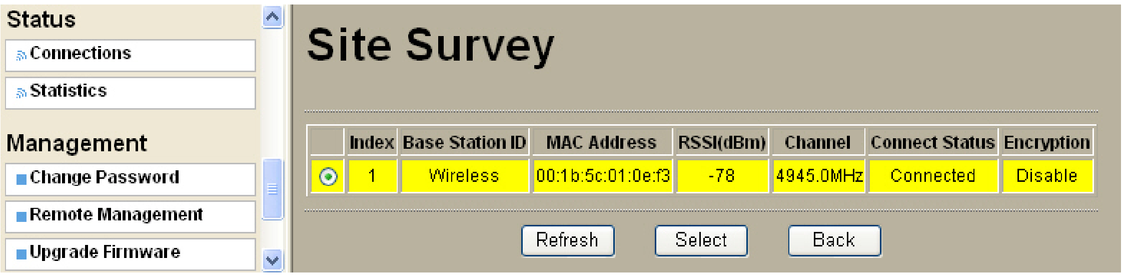
Advanced Parameters

CPE Download Speed (1-1687)	1687 x64Kbps [Tx]
RTS Threshold (0-2346)	2346
Fragmentation Length (256-2346)	2346
Beacon Interval(20-1000)	100 ms
Space In Meters (0-100000)	1000 m
TDM Time Slice (2-32)	4 ms

Operating mode: There are 3 kinds operating modes can be selected in this field.



Site Survey: Site survey only works under the CPE mode, which can scan the Base stations in the environment.



Site Survey

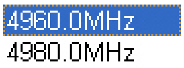
	Index	Base Station ID	MAC Address	RSSI(dBm)	Channel	Connect Status	Encryption
●	1	Wireless	00:1b:5c:01:0e:f3	-78	4945.0MHz	Connected	Disable

Base Station ID: only act in Base Station mode and CPE mode. Before you link the CPE to the Base station, make sure the Base Station ID is the same.

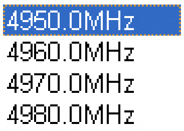
BSSID: Basic Service Set Identifier, only works at CPE mode.

Broadcast Base Station ID: You can decide broadcast the Base station ID or not.

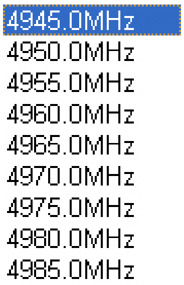
Channel / Frequency: Select the appropriate channel/Frequency from the list (from 4920MHz~ 5860MHz) provided to correspond with your network settings.



20MHz Channel bandwidth

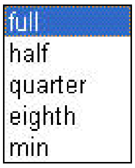


10MHz Channel bandwidth



5MHz Channel bandwidth

Output Power: Set the transmit signal strength of the radio. The options are full, half, quarter, eighth and min. Decrease the transmit power if necessary. The default is “full”.



Band Width: Set the Band width of the radio. The options are 20MHz / 10MHz / 5MHz. Different bandwidth has different throughput. Below is the list.

Bandwidth	**Throughput**
5MHz	5.5Mbps
10MHz	10Mbps
20MHz	20Mbps

VQOS / TDM: Versatile Quality of Service / Time-Division Multiplexing technique. TDM tech can avoid the packets collision and send the packets with more efficient way. You can set the data rate fractional (nx64 Kbps). This function is only available in CPE to Base station mode.

Antenna: Please set to "Fixed on primary"

Regatta mode: To shorten the header length of the fragmentation, enable this mode may make the throughput

Advanced Parameters

RTS Threshold: RTS Threshold is a mechanism implemented to prevent the "Hidden Node" problem. If the size of the packet transmitted is larger than the value you set, the RTS will be enabled. When the RTS is activated, the Wireless Bridge will use a (RTS/CTS) mechanism for data transmission. The setting range is 0-2346.

Fragmentation Length: Fragmentation mechanism is used for improving the efficiency when there is high traffic within the wireless network. If you transmit large files in a wireless network, you can enable the Fragmentation Threshold and specify the packet size. This specifies the maximum size a data packet will be before splitting and creating a new packet. The setting range is 256-2346. For example: If you set value as 256, it means the packet will be fragmented into "256" bytes while transmitting.

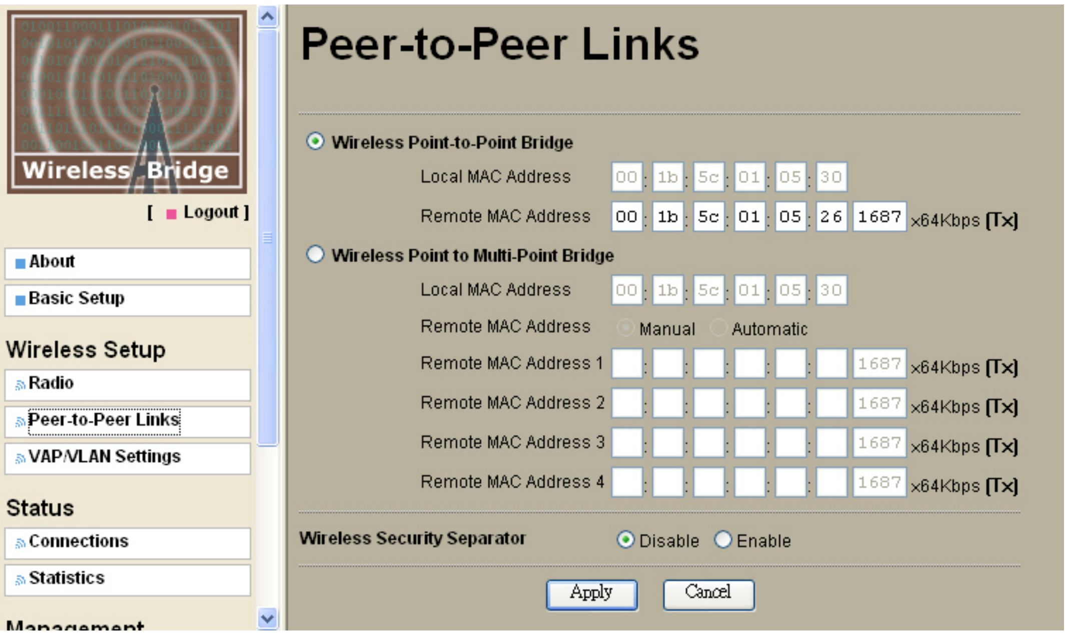
Beacon Interval: This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the outdoor radio to keep the network synchronized. A beacon includes the wireless LAN service area, the outdoor radio address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

Space In Meter: This is used for extending ACK time-out destination. The setting range is 0-10000 m. The longer is the distance, the lower the throughput.

Note: please set the value in this field according to the true distance, the value you set will affect the performance of the throughput. Our default value is 1000m.

Time Slice: set the time slice of the VQOS / TDM.

Wireless Setup / Peer-to-Peer Links



Peer-to-Peer Links

● Wireless Point-to-Point Bridge

Local MAC Address 00 : 1b : 5c : 01 : 05 : 30

Remote MAC Address 00 : 1b : 5c : 01 : 05 : 26 1687 x64Kbps [Tx]

○ Wireless Point to Multi-Point Bridge

Local MAC Address 00 : 1b : 5c : 01 : 05 : 30

Remote MAC Address ○ Manual ○ Automatic

Remote MAC Address 1 : : : : : 1687 x64Kbps [Tx]

Remote MAC Address 2 : : : : : 1687 x64Kbps [Tx]

Remote MAC Address 3 : : : : : 1687 x64Kbps [Tx]

Remote MAC Address 4 : : : : : 1687 x64Kbps [Tx]

Wireless Security Separator ● Disable ○ Enable

Configure a Wireless Point-to-Point Bridge

To activate the Point-to-Point Bridge mode please do the following:

1. Configure both radio1 on LAN Segment A and radio2 on LAN Segment B in Point-to-Point Bridge mode.
2. Enter the MAC address of radio2 into the “Remote MAC Address” field of radio1.
3. Enter the MAC address of radio1 into the “Remote MAC Address” field of radio2.

After you complete the settings, please click on “Apply” for changes to take effect.

Configure a Wireless Point to Multi-Point Bridge

There are two options under this setting:

I. Point to Multi-point Bridge:

Assume radio1 is the base station, radio2 and radio3 are clients.

To activate the Multi-Point to Multi-Point Bridge mode please do the following:

1. Configure radio1, radio2, and radio3 in Point-to Multi-Point Bridge mode.
2. Verify that radio1 on LAN Segment A with the Remote MAC Address of **radio2** and **radio3**.
3. Verify that radio2 on LAN Segment B with the Remote MAC Address of **radio1**.
4. Verify that radio3 on LAN Segment C with the Remote MAC Address of **radio1**.

II. Multi-point to multi-point Bridge:

To activate the Multi-Point to Multi-Point Bridge mode please do the following:

1. Configure radio1, radio2, and radio3 in Point-to Multi-Point Bridge mode.

2. Verify that radio1 on LAN Segment A with the Remote MAC Address of radio2 and radio3.
3. Verify that radio2 on LAN Segment B with the Remote MAC Address of radio1 and radio3.
4. Verify that radio3 on LAN Segment C with the Remote MAC Address of radio1 and radio2.

After you complete the settings, please click on "Apply" for changes to take effect.

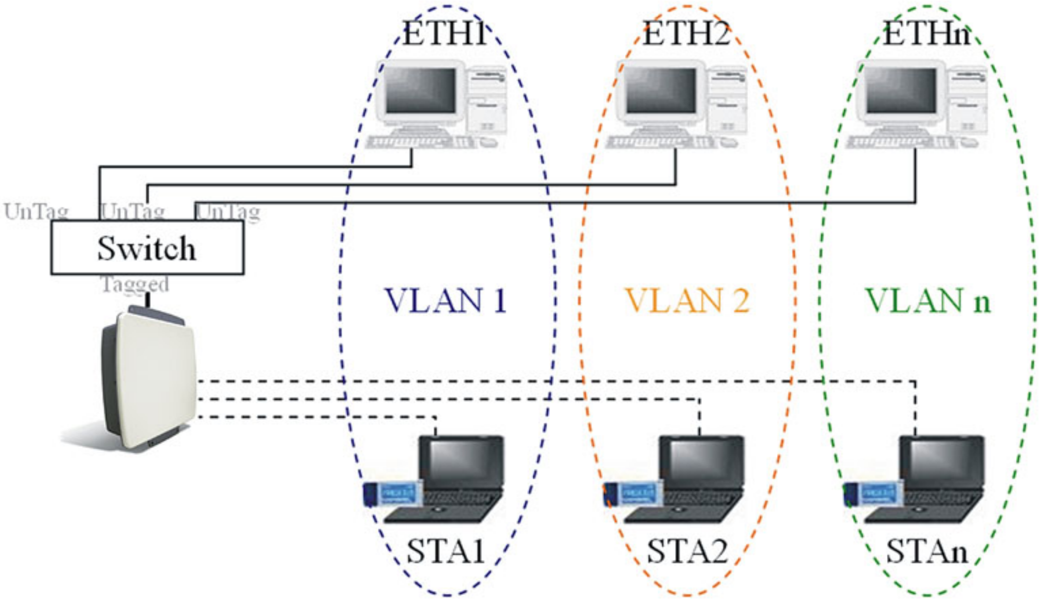
Note: Under Point-to Multi-Point Bridge mode, you can extend this multi-point bridge by adding additional Wireless Bridges for each additional LAN Segment.

Throughput control: you can set the throughput to n*64Kbps in each point.

VAP / VLAN Settings

As the number of data-based systems increase, it becomes more and more difficult to provide the network infrastructure (due to the sheer number of Ethernet connections that need to be provided) from the perspective of cost, space, and wire management. Luckily, the advent technology called VLAN (Virtual Local Area Network) can achieve her mission. Now it is possible for these multi devices in function without the need for multiple physical network APs.

See the diagram below.



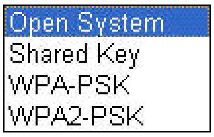
Under this mode, this radio can behave as 8 virtual Wireless LAN infrastructures. You can specify unique SSID for these different infrastructures. For example, VLAN1 contains ETH1 and STA1, VLAN2 contains ETH2 and STA2, and so on. However, they all share the same AP and undertake different tasks. Some VLANs can be used for guest Internet access, others for enterprise users, and administrators can be put on a high security VLAN with enhanced firewall permissions. All this can be achieved using a single infrastructure to emulate up to 8 infrastructures. The AP does this by assigning each of the 8 VLANs it's own SSID, so you will think you are looking at up to 8different wireless networks.

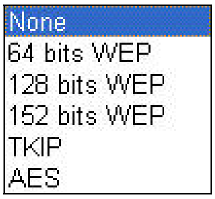
Enable this function to let associated clients be able to separate from each other when security is required. The default setting is Disable.

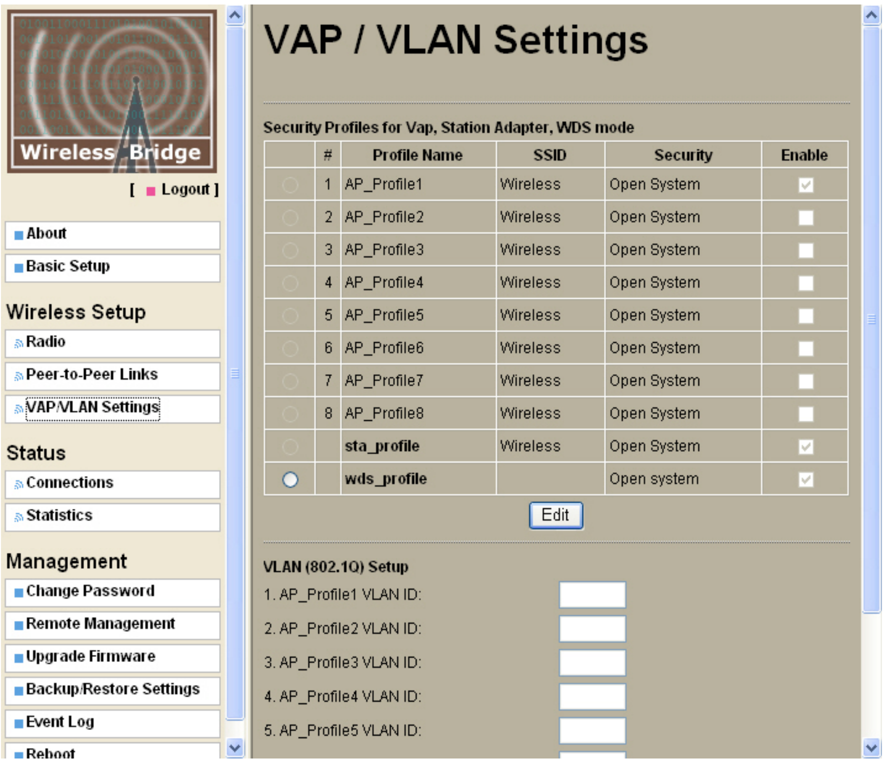
Note: If you complete the settings, please click on "Apply" for changes to take effect.

Wireless Setup / Encryption Settings

To prevent unauthorized radios from accessing data transmitted over the link, the Encryption Settings window offers WEP features, making your data transmission over air more secure and allows you to specify Encryption Key(s) if you enable encryption for the Wireless Bridge. There are three degrees of encryption could be selected: **64 bits WEP, 128 bits WEP and 152 bits WEP**. Also you can select WPA-PSK and WPA2-PSK for the advance security.







VAP / VLAN Settings

Security Profiles for Vap, Station Adapter, WDS mode

	#	Profile Name	SSID	Security	Enable
○	1	AP_Profile1	Wireless	Open System	☑
○	2	AP_Profile2	Wireless	Open System	□
○	3	AP_Profile3	Wireless	Open System	□
○	4	AP_Profile4	Wireless	Open System	□
○	5	AP_Profile5	Wireless	Open System	□
○	6	AP_Profile6	Wireless	Open System	□
○	7	AP_Profile7	Wireless	Open System	□
○	8	AP_Profile8	Wireless	Open System	□
○		sta_profile	Wireless	Open System	☑
○		wds_profile		Open system	☑

VLAN (802.1Q) Setup

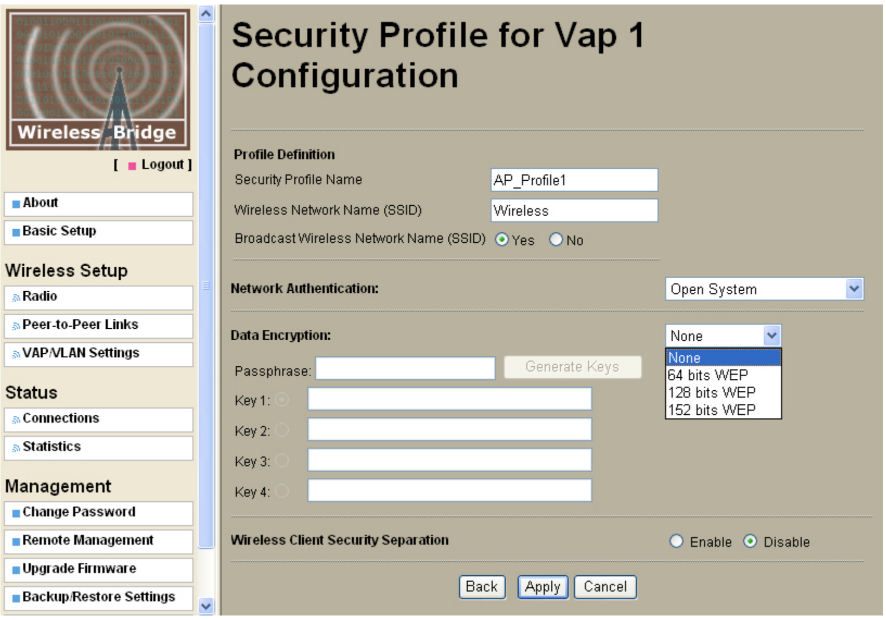
1. AP_Profile1 VLAN ID:

2. AP_Profile2 VLAN ID:

3. AP_Profile3 VLAN ID:

4. AP_Profile4 VLAN ID:

5. AP_Profile5 VLAN ID:



Security Profile for Vap 1 Configuration

Profile Definition

Security Profile Name: AP_Profile1

Wireless Network Name (SSID): Wireless

Broadcast Wireless Network Name (SSID) ● Yes ○ No

Network Authentication: Open System

Data Encryption: None (None / 64 bits WEP / 128 bits WEP / 152 bits WEP)

Passphrase:

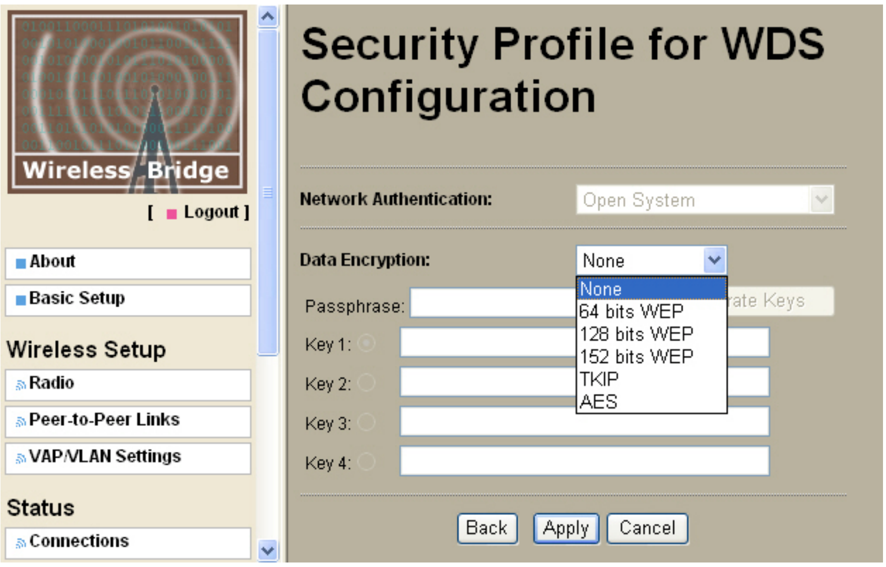
Key 1: ○

Key 2: ○

Key 3: ○

Key 4: ○

Wireless Client Security Separation ○ Enable ● Disable



Security Profile for WDS Configuration

Network Authentication: Open System

Data Encryption: None (None / 64 bits WEP / 128 bits WEP / 152 bits WEP / TKIP / AES)

Passphrase:

Key 1: ○

Key 2: ○

Key 3: ○

Key 4: ○

The following elaborate WEP/WPA security options.

Field	Description
Network Authentication	You have two authentication options. • Open System: No authentication is imposed to the radio. However, if the 802.1x option is configured, authentication of connections can be performed by a RADIUS server. • Shared: this is for shared key authentication. Data is encrypted.

Encryption Strength	You can select the following data encryption options: Disabled 64- 128- or 152-bit WEP With Open System Authentication and 64- 128- or 152-bit WEP Data Encryption with Shared Key authentication
Security Encryption (WEP) Keys	WEP enabled, you can manually enter the four data encryption keys or enable Passphrase to generate the keys automatically. These values must be matched between all Clients and access points at your LAN (key 1 must be the same for all, key 2 must be the same for all, etc.) Two ways to create WEP encryption keys: • Passphrase. Passphrase functions as automatically case-sensitive characters. However, not all wireless adapters support passphrase key generation. • Manual. These values are not case sensitive. 64-bit WEP: enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F). 128-bit WEP: enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F). 152-bit WEP: enter 32 hexadecimal digits (any combination of 0-9, a-f, or A-F).
WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)	WPA Pre-Shared-Key uses a pre-shared key to perform the authentication and generate the initial data encryption keys. Then, it dynamically varies the encryption key. It uses Temporal Key Integrity Protocol (TKIP) for encryption keys. However not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA.
WPA 2-PSK	Identical to WPA-PSK with the exception of the way to encryption keys. WPA2-PSK uses Advanced Encryption Standard (AES) for encryption keys.
WPA-PSK& WPA 2-PSK	You may have the option of WPA-PSK associated with TKIP. Alternatively, you can select WPA2-PSK associated with AES.

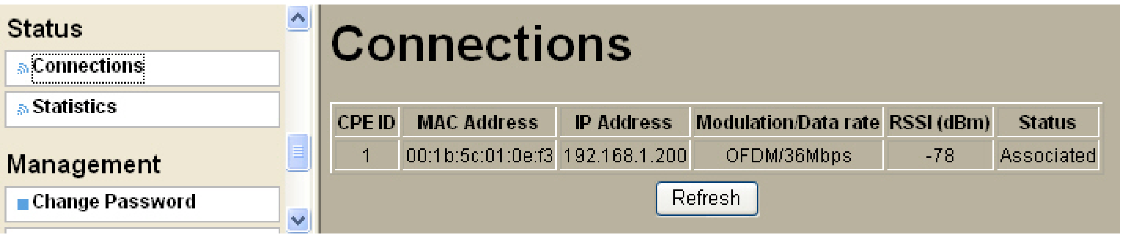
Note: WPA-PSK (TKIP) & WPA2-PSK (AES) only works at Base station and CPE mode.

3-3 Status

Status / Connections

The connections page provides below information in different settings.

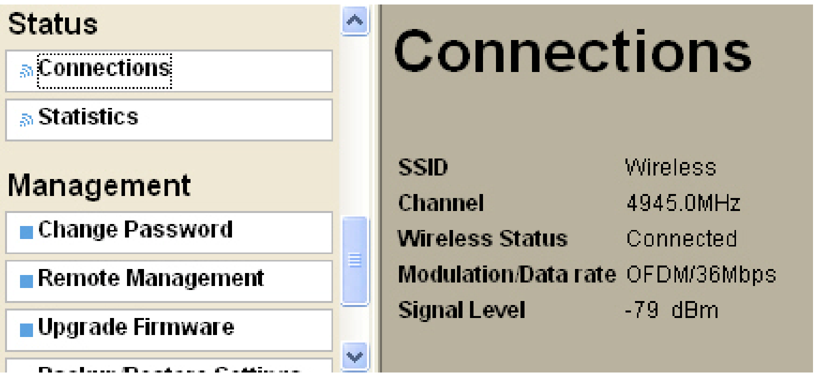
Mode	information
Base Station Mode	CPE ID, MAC Address, IP Address and Status
CPE Mode	SSID, Channel, Wireless Status and Signal level



Connections

CPE ID	MAC Address	IP Address	Modulation/Data rate	RSSI (dBm)	Status
1	00:1b:5c:01:0e:f3	192.168.1.200	OFDM/36Mbps	-78	Associated

Connections Page in Base Station mode



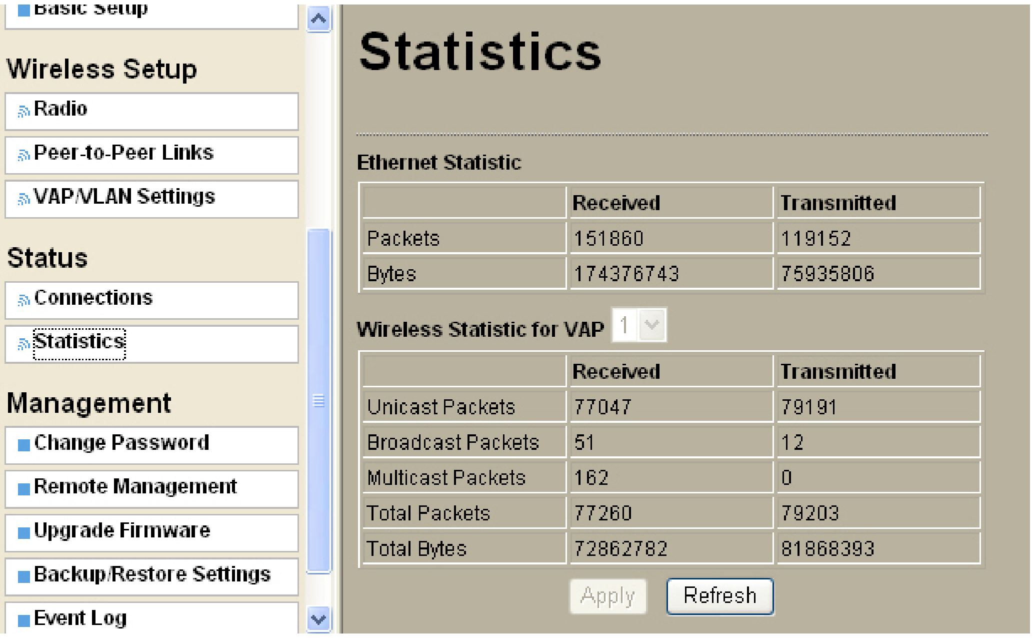
Connections

SSID	Wireless
Channel	4945.0MHz
Wireless Status	Connected
Modulation/Data rate	OFDM/36Mbps
Signal Level	-79 dBm

Connections Page in CPE mode

Status / Statistics

The Statistics screen provides various Ethernet and Wireless TX/RX packet statistics on the Wireless Bridge. Click the **Refresh** button to update the statistics on this screen.



Statistics

Ethernet Statistic

	Received	Transmitted
Packets	151860	119152
Bytes	174376743	75935806

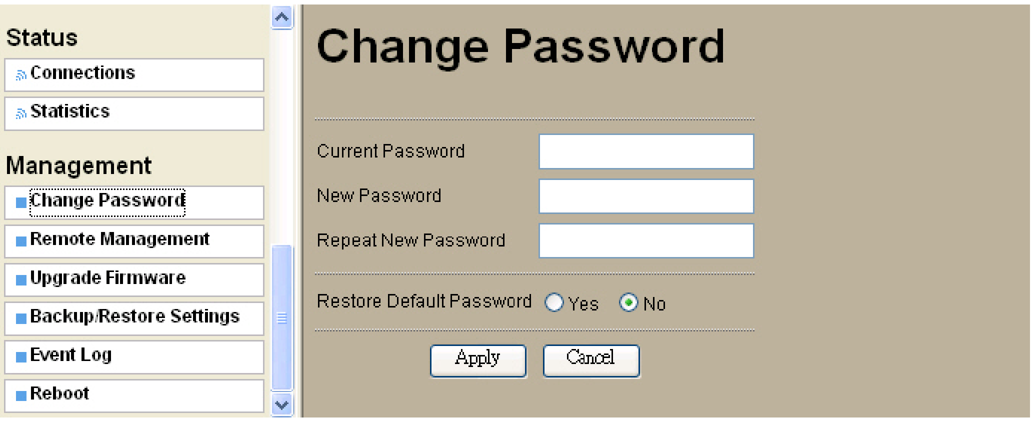
Wireless Statistic for VAP 1

	Received	Transmitted
Unicast Packets	77047	79191
Broadcast Packets	51	12
Multicast Packets	162	0
Total Packets	77260	79203
Total Bytes	72862782	81868393

3-4 Management

Management / Change Password

Here allow you to change the Wireless Bridge’s password.



Change Password

Current Password
New Password
Repeat New Password

Restore Default Password ○ Yes ● No

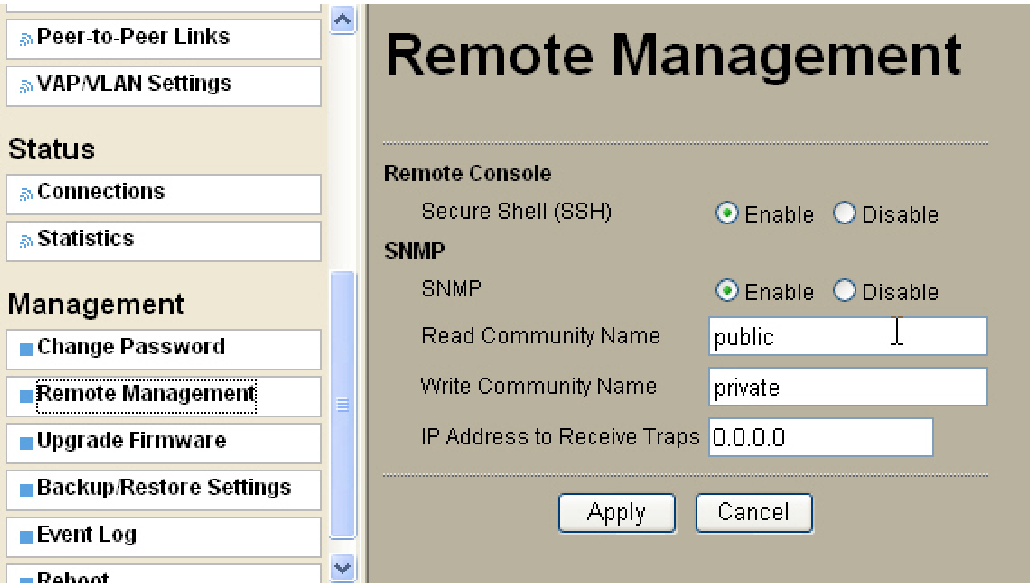
To change the password of the Wireless Bridge, do the following:

1. To change the current password, choose the “Change Password” option from the “Management” section in the Wireless Bridge’s left page. Key in the default password “password” in the “Current Password” filed.

2. Changing password for the Wireless Bridge is as easy as typing the password into the New Password field. Then, type it again into the Retype New Field to confirm. Click the “Apply” button to save the setting.

Note: After you change password, please take note of your new password. Otherwise, you will not able to access the Wireless Bridge setup.

Management / Remote Management



Remote Management

Remote Console

Secure Shell (SSH) ● Enable ○ Disable

SNMP

SNMP ● Enable ○ Disable

Read Community Name: public

Write Community Name: private

IP Address to Receive Traps: 0.0.0.0

Remote Console

Secure Shell (SSH): If enable Secure Shell, the Wireless Bridge will only allow remote access via Secure Telnet.

SNMP

Enable SNMP to allow the SNMP network management software to manage the Wireless Bridge via SNMPv2 protocol.

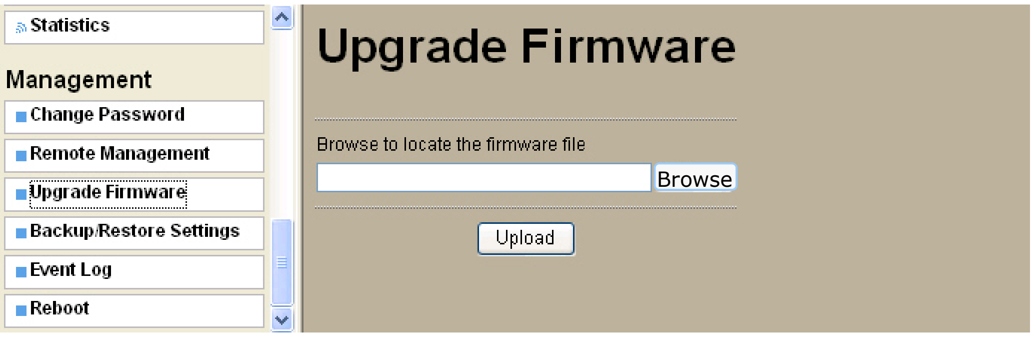
Read Community Name: Allow the SNMP manager to read the MIB objects of the Wireless Bridge. The default setting is “public”.

Write Community Name: Allow the SNMP manager to write the MIB objects of the Wireless Bridge. The default setting is “private”.

IP Address to Receive Traps: The IP address of the SNMP manager to receive traps sent from the Wireless Bridge.

Click “Apply” if you make any changes.

Management / Upgrade Firmware



Upgrade Firmware

Browse to locate the firmware file

The Upgrade Firmware menu will display the Upgrade Firmware window so that you could update the latest firmware on the Wireless Bridge.

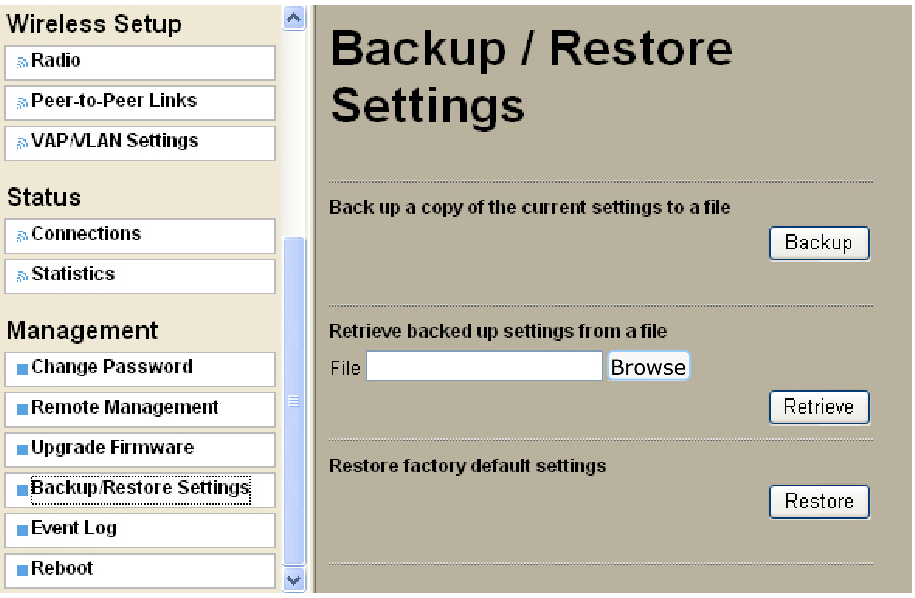
Please make sure that you have downloaded the latest and correct firmware from the website before upgrading the firmware of the Wireless Bridge.

To upgrade the latest firmware, complete the following:

- Using browser to access the main page of the Wireless Bridge.
  1. Select "Upgrade Firmware" from the **Management** section.
  2. Input the exact file path and name or select the file by clicking **Browse** button, then press **Upload** button to upgrade the firmware.
  3. Please wait for few seconds.
- If download fail, please repeat the step 1~3 to download again.

Note! Do not power off the unit when it is being upgraded.

Management / Backup / Restore Settings



Backup / Restore Settings

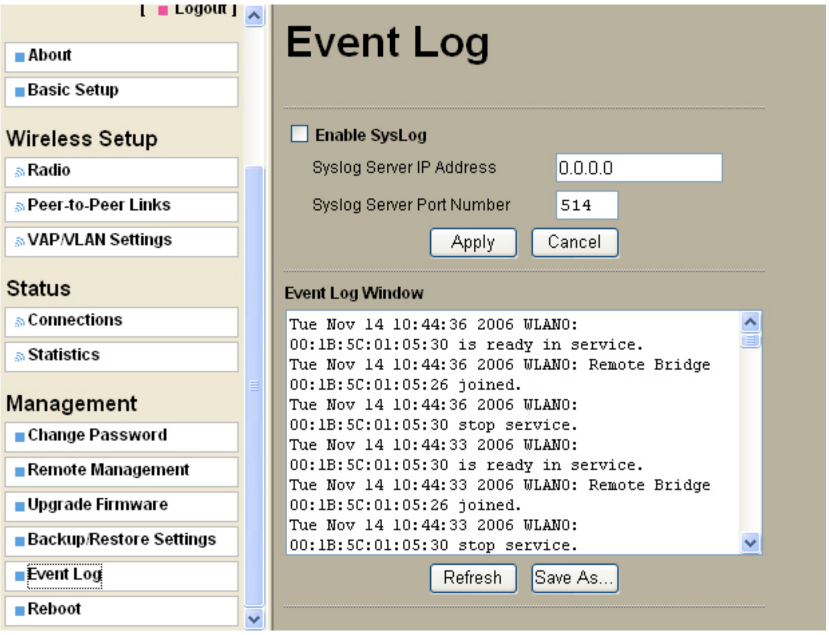
Back up a copy of the current settings to a file

Retrieve backed up settings from a file

Restore factory default settings

The current system settings can be saved into a file as a backup by clicking "**Backup**". The saved file can be loaded back on the radio by clicking "**Browse**". When you have selected the settings file, click "**Retrieve**" to begin the process. Furthermore, you may click "**Restore**" to factory default settings.

Management / Event Log



Event Log

☐ Enable SysLog

Syslog Server IP Address: 0.0.0.0

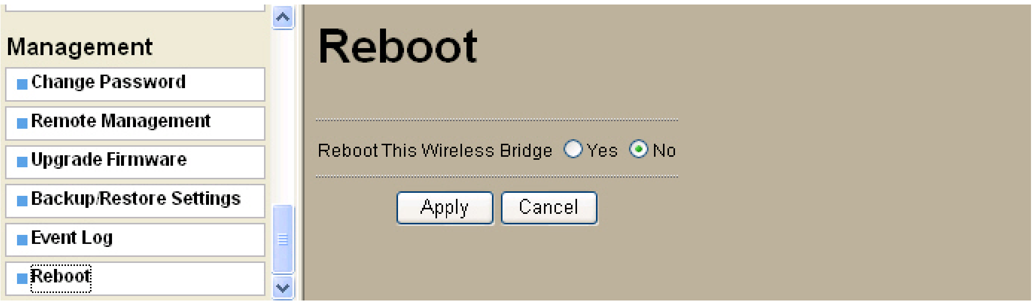
Syslog Server Port Number: 514

Event Log Window

```
Tue Nov 14 10:44:36 2006 WLAN0:
00:1B:5C:01:05:30 is ready in service.
Tue Nov 14 10:44:36 2006 WLAN0: Remote Bridge
00:1B:5C:01:05:26 joined.
Tue Nov 14 10:44:36 2006 WLAN0:
00:1B:5C:01:05:30 stop service.
Tue Nov 14 10:44:33 2006 WLAN0:
00:1B:5C:01:05:30 is ready in service.
Tue Nov 14 10:44:33 2006 WLAN0: Remote Bridge
00:1B:5C:01:05:26 joined.
Tue Nov 14 10:44:33 2006 WLAN0:
00:1B:5C:01:05:30 stop service.
```

Enable SysLog if you have a Syslog Server on your network environment. If enable, you need to input the Syslog Server IP Address (default is 0.0.0.0) and the port number your Syslog Server is configured to use. The default port number is 514. The Event Log Window lists Wireless Bridge events. Click on “Refresh” to update the network events or “Save As…” to save the event into a file on your computer. Click “Apply” if you made any changes.

Management / Reboot



Reboot

Reboot This Wireless Bridge ○ Yes ● No

The Reboot AP screen enables you to reboot your Wireless Bridge. If any changes are made and you want them to take effect, you need to reboot the Wireless Bridge. Select the “**Yes**” check box and click “**Apply**”. It will take you about 50 seconds to go through reboot. The Web-browser will not be accessible until the Wireless Bridge has finished its reboot process.

Hardware reset

If your Web User Interface stops responding, ping the IP address of the radio to check whether “reply” is obtained, or unplug and then plug back in the power supply of the Wireless AP Access Point. This will reboot the Wireless AP Access Point. If you are still unable to communicate with the Web User Interface, screw off the screw next to the grounding stud. Then use a stick to press in and hold the RESET button for five to ten seconds. This will reset the Wireless AP Access Point to the factory default settings. If you applied any personal configuration settings, you will need to make the changes again. Below is the tool to revolve the screws and press the reset button for your reference:

Tool to screw off the screw of reset button.

⚠ CAUTION	2 Button head socket cap screws are attached with the mounting kits for spares, 3 times the most to reuse each screw for ensure the water-proof function.

Appendix A: Trouble shooting

This Appendix helps you to isolate and solve the problems with the 4.9GHz outdoor subscriber. Before you start troubleshooting, it is important that you have checked the details in the product user manual and QIG.

In some cases, rebooting the unit clears the problem. If the radio still can't work well, please try to contact your local vendor or supplier.

General Descriptions

To successfully use the radios, engineers must be able to troubleshoot the system effectively. This section will show you how an 4.9GHz outdoor subscriber could be analyzed in the case of "no link," usually, we thinks that the link is down because there is no traffic being passed. The four main reasons that a link may not work are list as below:

- Configuration
- Path issues (such as distance, obstacles, RF reflection…)
- Personal reasons (careless mounting or the incorrectly connection.)
- Hardware (includes the radio, cable and connectors…etc. In few cases, the radio will conflict with the laptop or PC)
- Environment (anything that is outside the equipment and not part of the path itself)

After verified the correct configuration, double-checked the path terms, ensure no personal reasons and the hardware works well in the office, but the user still report that the link does not work. Most likely, the problem reported is caused by the environment or by improper tests to verify the connection. Assumes that the test method, cabling, antennas, and antenna alignment have been checked, (Always ensure this before checking the environment.) then you can do the follow to check the environment.

General Check

Two general checks are recommended before taking any action:

- Check whether the software version at both sides is the most current
- Check for any reported alarm messages in the Event Log

Analyzing the Spectrum

The best way to discover if there is a source of interference is to use the spectrum analyzer. By turning the antenna 360 degrees, you can find out which direction is the interference coming from. it will also show the frequencies and the level of signal is detected.

Avoiding Interference

When a source of interference is identified and when the level and frequencies are known, the next step is to avoid the interference. Some of the following actions can be tried:

- Change the RF channel to the one away from the interference source

- Change the polarization of the antenna; try to change to a polarization different from the interferer.
- A small beam antenna may helps. (Such as some grid or dish antenna, align the antenna in to the particular direction will reduce the affects from the interference source) This solution cannot help when the source of interference is right behind the remote site.

Before checking for interference, ensure all the hardware works well and configurations are correct. The path analysis, cabling and antennas should be checked as well.

Connection Issues

This section describes several common troubles the customer might have while setting the radios.

Radio Does Not Boot

When the Radio does not Boot, do the following steps to check your whole system:

1. Ensure that the power supply is properly working and correctly connected.
2. Ensure that all cables are workable and connected correctly.
3. Check the power source.

Cannot use the Web Interface

If the radio boot, but can’t enter it via the Web site.

1. Open a command prompt window and enter **ping <ip address unit>** (for example: `ping 192.168.1.1`). If there is no response from the radio, make sure that you the IP address is correct. If there is response, the Ethernet connection is working properly, do the next step.
2. Make sure that you are using one of the following Web browsers:
   - Microsoft Internet Explorer version 5.0 or later
   - Netscape version 5.0 or later.
3. Ensure that you are not using a proxy server for the connection with your Web browser.

Double-check the physical network connections (includes the cables and the connectors).

Use a well-known unit to ensure the network connection is properly functioning.

Configuration Issues

The following problems relate to setup and configuration problems.

Some basic configurations might make the link fail, below are the major ones:

- RF Channel
- SSID
- IP address
- Rule of MAC address filter
- Rule of security settings (such as WEP or WPA)

- Rule of authentication (such as settings of radius server and 802.1x)
- Configurations of WDS page

If the links of the two radios works within close distance of each other, then there are two possible reasons why wireless connectivity is not possible while the 4.9GHz outdoor subscribers are at their desired locations:

- RF path, for example, a bad antenna alignment, the tower is not tall enough when the radios are installed in a long distance or the connector do not attachment well…etc (these are the most common problems in installations)
- Interference problem caused by a high signal level from another unit. The interference can be checked by changing the frequency and then see if another channel works better. Or you can change the polarization of the antenna as a way of avoiding the interfering signal. To know in advance how much interference is present in a given environment, a Spectrum Analyzer can be attached to a (temporary) antenna for measuring the signal levels on all available Channels.

If the link still not works after resetting the configurations, checking the connectors and cables, double-check the path and environment issues, then the problem is possible a hardware problem. Acquiring a third radio and then testing it amongst the existing units will help to find out the broken unit.

Please contact your local vendor for advance technical support.