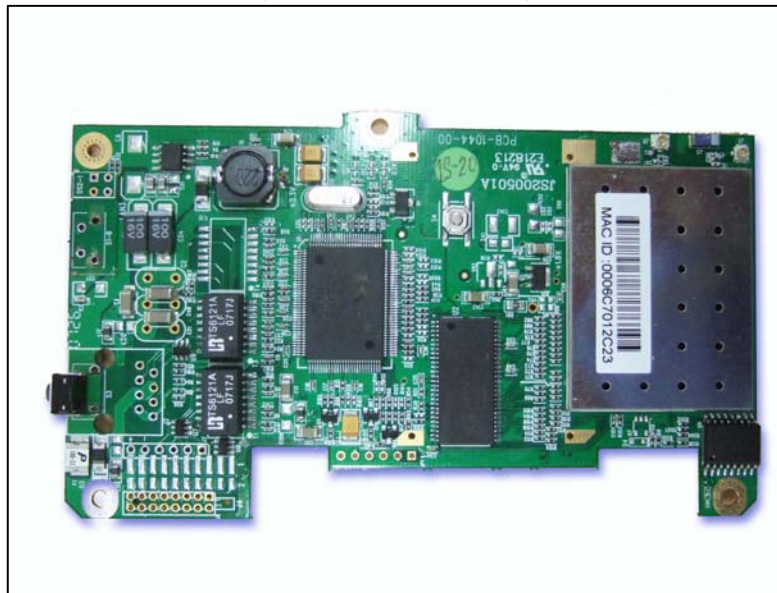# User Manual

Wireless LAN 802.11 b/g
AP & Ethernet Bridge

(EB1-TOO2-TLDO1)

Version 1.0
Last Updated: Dec 6th 2007

Federal Communication Commission Interference Statement

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 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.

This device complies with 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.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

The manufacturer declares that APRT-2518G/APRT-2518GS is limited to channel 1~channel 11 by specified firmware controlled in USA.

IMPORTANT NOTE:

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
To maintain compliance with FCC RF exposure compliance requirements, please avoid direct contact to the transmitting antenna during transmitting.

This equipment intended for use on particular type of equipment

Information to User

The user's manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

CONTENT PAGE

1 INTRODUCTION

The Product

The product is based on the IEEE **802.11g** standard, which is the latest **54Mbps** Wireless LAN (WLAN) standard. This standard is five times faster than the widely deployed **WiFi** (802.11b) products that are found in homes, airport and public wireless hotspots. Because 802.11g uses the same **2.4GHz** frequency band, the product is fully interoperable with existing WiFi cards and devices. Having two wireless protocols in one product ensure that your investments are protected, while enabling you to enjoy the fastest Wireless LAN speed.

The product is a combination of 3 devices:
    a.   Wireless Access Point (AP) compliant to 802.11b/g standards.
    b.   Wireless Ethernet Client (Bridge)
    c.   Client, CPE

The product is an all-in-one device that allows multiple PCs to share a common broadband (ADSL/Cable) modem. It can serve up to 4 Ethernet-PCs and many WLAN-notebooks. The built-in NAT and DHCP Servers ensure almost plug-and-play convenience for your home network. Advanced features such as Firewall, DMZ and WPA Encryption make this a product equally suitable for your office needs.

Product Features

- Fully compatibility with **IEEE 802.11g** WLAN standard
- Utilize OFDM (**O**rthogonal **F**requency **D**ivision **M**ultiplexing)
- Wireless data rate of up to **54Mbps,** support **"Turbo"** mode up to **108Mbps**
- Operates in the **2.4GHz** license-free frequency band
- Connects multiple computers to a broadband modem to share Internet connection
- Full backward compatibility with **802.11b** standard (WiFi 11Mbps)
- **WEP** (Wired Equivalent Privacy) authorizes users based on a simple WLAN encryption standard to protect wireless data from sniffers.
- **WPA** (WiFi Protected Access) authorizes users and identifies users based on an improved WLAN encryption standard where the secret key changes dynamically at regular intervals
  - **TKIP** (**T**emporal **K**ey **I**ntegrity **P**rotocol), when used in conjunction with a corporate RADIUS server, ensure higher security for enterprise networks.
  - **Pre Shared Key**, suitable for home user, without a RADIUS server. A new key is generated each time the PC connects to the network, vastly improving the safety of information exchange within the network
- User-friendly web-based interface for managing and configuring the wireless AP.

2   STANDARD PACKAGE
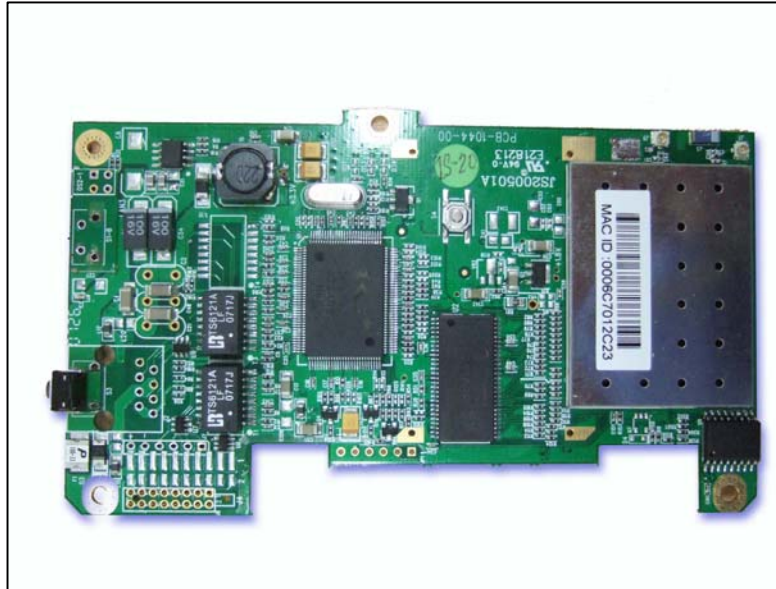
Contents of Package

- 2.4GHz Wireless AP & Ethernet Bridge *(EB1-T002-TLD01)*
- Software Interface User Manual

Note: Using a power adaptor with a power rating other than the one included in the package will cause serious damage to the AP and void the warranty for this product.

System Requirements for Configuration

- Computers with Windows, Macintosh or Linux-based operating systems and with an Ethernet adaptor
- Internet Explorer version 5.5 and above or Netscape Navigator that supports Java.

3   BASIC IP NETWORKING

Internet Protocol (IP)

IP stands for Internet Protocol. In an IP network, every device has a **unique** IP Address (For example: 192.168.1.35) to identify itself. There are two ways of assigning an IP address to a PC or Router: Static and Automatic (DHCP). Static IP addresses are keyed-in manually, while Dynamic IP's are distributed by a DHCP Server.

Ports

Every packet of traffic is identified by its Source and Destination Addresses, which would ensure that the packet arrives at the correct destination. A Port Number is also embedded in each packet; to identify which software application that generated and uses that packet. Therefore, if the Router blocks a certain port number, it denies the particular software from using the connection.

Static IP Address

Static IP addressing ensures that the device will always have the same IP address. Static addressing is commonly used for your servers.

Dynamic IP Address

A dynamic IP address is one that is automatically assigned to a PC. These IP addresses are "dynamic" because they are only temporarily leased to the PC when it connects to the network. This is the most convenient and common way of managing IP addresses in a network. The Server that manages this pool of IP addresses is called the DHCP Server. The product has a DHCP Server built-in to simplify the network management.

DHCP (Dynamic Host Configuration Protocol)

The PC obtaining an IP address from the Server is called the DHCP Client. If there is already a DHCP Server running on your network, you must disable one of the two DHCP servers. Running more than one DHCP server together will cause network problems!

What is a Router?

A router is a network device that connects two networks together, to let them communicate. All the PCs in your home or office would be considered to be in one network: the Local Area Network (**LAN**). The Internet (including the ADSL modem) is considered to be another network: the Wide Area Network (**WAN**). The Router serves 2 purposes:

- Connect all the PCs in the LAN together, allowing them to communicate with one another. (File sharing, Printer sharing etc.)
- Connect all the PCs in the LAN to the Internet, allowing them to simultaneously surf the web and access e-mails.

The Router is connected to 2 networks at the same time. Therefore, it has two IP addresses: one for the LAN, and one for the WAN. The Router's LAN IP address can be configured, but it is best to use the default settings. The WAN port is a DHCP client by default.

4   WIRELESS LAN BASICS

A Wireless LAN (WLAN) is a computer network that transmits and receives data with radio signals instead of using cables. WLAN have become common in homes, offices, airports and public Hotspots. WLAN can support the same applications and software that run on a wired network (LAN). Besides supporting the same software and functions, WLAN brings greater convenience and eliminates the need to lay Ethernet cables in a home or office.

The wireless AP is based on the finalized **802.11g** standard. The IEEE 802.11g standard is an improvement on the 802.11b (WiFi) standard. It increases the data rate up to 54 Mbps within the 2.4GHz band. As the 802.11b standard is also using the 2.4GHz frequency band, the product is fully backward compatible with the older 802.11b devices. WiFi cards can be used to connect to the wireless AP at 11Mbps.

The **AP** is also known as the Wireless Bridge. The PC using the Card bus is known as the **Client**. WLAN networking involves a few additional parameters to be configured:

SSID

The SSID is the "network name" for the WLAN network. The SSID is any name, and can be any set of characters or numbers, and must be configured on both the AP and Client. The Client sniffs the radio frequencies for an AP with the same SSID with itself. The client locks onto the AP and they are "**associated**".
To enable plug-and-play convenience, most client cards can sniff the frequencies to extract the available SSID to let the user choose from. Alternatively, setting the client's SSID to "ANY" can allow it to connect to most AP's regardless of the AP's SSID setting.

Encryption

WLAN traffic can be captured by anybody to be read! The solution is to use encryption to make the traffic appear as random characters to the eavesdropper. Both the AP and client must use the same encryption standard and key to enable them to decode the "rubbish". If the encryption settings are mismatched, the client and AP cannot associate. WEP (Wired Equivalent Privacy) is the most common WLAN encryption standard.

MAC Address Control

Every client card has a unique MAC Address. This MAC Address can be input into the wireless AP such that the wireless AP only allows this pool of MAC Addresses to use the WLAN.

Channel

There are a total of 11 channels in the 2.4GHz band. Depending on regulation, not all the frequencies may be available in every country. Frequency is configured on the wireless AP only. The client searches for the wireless AP and locks onto that AP's channel.

Signal Strength

Radio signals drop in power over a distance. Even if all the settings are correct, low signal strength makes association impossible. The usable distance between the AP and client can range from a few meters indoor to 200m outdoors maximum. When setting up the wireless AP, make sure that you:

- Keep the distance from the wireless AP to the clients as short as possible.
- Make sure that the WLAN signals do not have to pass through too many concrete walls and metal structures to reach the client.
- Make sure that wireless AP is located far away from one another to avoid interference.

To access the *Configuration* menu of the Wireless AP connect the device as shown in the previous section.

- Open the web browser.
- Type the AP default IP address (**10.0.0.1**) into the browser's Address field.

■
■   Type in **admin** for the password.
■   Click on *Log In*.

Note: If you have changed the default user name and password of the Router, make sure you enter the correct user name and password.

Once the login is successful, you'll see a configuration menu and a pop up window for wizard setup. The wizard is a quick guide to run you through the configuration process so as to setup your system in the shortest time. After the initial setup, you may wish to turn off the setup wizard by removing the tick on *Run This Wizard at Start*. Click on *Next* to proceed with the setup wizard.

Note: If you have pop-ups blocker installed on your computer, it may prevent the Wizard window from functioning properly.

Detailed configuration for the wireless AP can be found at the configuration menu. The Configuration menu consists of a navigation menu and a configuration panel. The configuration panel is a place to set the entire detailed configuration.

These buttons will appear at most configuration pages.

- **Help:** Clicking help will bring up helpful information on the functions.
- **Save:** Click to save the configuration. Do a reboot when you have configured all the parameters.
- **Reset:** Click to reset all the parameters on the page.

5 CONFIGURATION WIZARD

Once you have logged in, the Wizard screen will appear.

Click Next

Set up your new password
The default User Name is admin and the password is admin.

Click Next

Choose your Time Zone
Enter the SNTP Server. If
you do not know of any
SNTP Server, you can use
the default.

Choose your time zone from
the drop down list.

Click Next

Wireless AP & Ethernet Bridge (11b/g)

Log Out

| System Summary | Setup Wizard | Basic | Wireless | System Tools |

Setup Wizard > Step 2: Set Time Zone

The system gets the current time from SNTP server. Server Address can be a
name or an IP address. For the time zone, select the local time zone.

SNTP Server Address: pool.ntp.org

Time Zone: GMT +8 Beijing,Hong Kong,Singapore,Taipei

? Help ← Previous → Next

Wireless Setup
Enter the SSID you preferred
for your network.
You can manually select the
channel you wish to use or
allow the wireless AP to select a
clean channel to use by
selecting *SmartSelect*.

Click Next

Wireless AP & Ethernet Bridge (11b/g)

Log Out

| System Summary | Setup Wizard | Basic | Wireless | System Tools |

Setup Wizard > Step 3.1: Set the basic of Wireless

Enter the SSID and Channel to be used by the Wireless Access Point.

SSID: 11g-0

Channel: 2437MHz (Channel 6)

2412MHz (Channel 1)
2417MHz (Channel 2)
2422MHz (Channel 3)
2427MHz (Channel 4)
2432MHz (Channel 5)
2437MHz (Channel 6)
2442MHz (Channel 7)
2447MHz (Channel 8)
2452MHz (Channel 9)
2457MHz (Channel 10)
2462MHz (Channel 11)
SmartSelect

? Help ← Previous → Next

Wireless Security
Enter the type of security mode you wish to use. Take note that if you are using 802.11b card, it does not support WPA-PSK or WPA.

Click Next

End of Setup
Click on *Reboot* to save the setting and reboot the wireless AP. If you wish to discard all the setting, click on *Discard*.

Click Next

Click Discard to cancel all settings

Click Reboot to finish the setup Wizard

6 CONFIGURATION MENU

System Summary > Configuration

This page presents a convenient overview of the overall status of the wireless AP. The most common configuration parameters are shown here, for a quick look.

System Summary > Associations

This page allows you to view the MAC address of all the wireless laptop and PC connected to the Wireless AP. ID AP is the MAC address of the AP itself. Any wireless computers or laptop associated with the access point will have an ID of STA.

System Summary > Statistics

This page allows you to view the packets and bytes receive and transmit by the wireless AP.

System Summary > Site Scan

Using the site scan, you can scan for the presence of other wireless AP near you. The ESSID, BSSID, wireless mode, channel, signal strength, security mode and network mode of the surrounding AP will be display in the table. You can use this function to select a clean channel for your AP. Take note that there would be no any result if the wireless function of the AP is disabled.

Basic > SNTP Setting

Simple Network Time Protocol (SNTP) allows the wireless AP to set its internal clock based on periodic updates from the specified timeserver (SNTP or NTP). The time is useful in the IP filter section, where you can configure to block certain IP address daily at a certain time.

Basic > LAN Setting

This page is for the configuration of the wireless Access Point internal (LAN) IP Address.

System Name: This is to assign a name to the wireless AP so that you can identify the device.

LAN IP address: This is where you assign a local IP address to your access point LAN port. The factory default value is 10.0.0.1 if you give your computer a static IP address, the gateway of your computer must be set to this IP for you to access the Internet.

Subnet Mask: This is where you assign the corresponding subnet mask. The default subnet mask is 255.0.0.0

Basic > MAC CLONE

The default WAN MAC address is set to the WAN's physical interface MAC address on the wireless Access Point. You can use the MAC Clone function to replace the default MAC address to that of the Ethernet Card installed by your ISP. It is not recommended that you change the default MAC address unless required by your ISP.

Enable MAC Clone: Tick to enable MAC Clone function.

MAC Address: Enter the MAC address you wish to clone or use the default MAC by clicking on the *Use Default MAC* button.

Your PC MAC Address: This field reflects the MAC address of your computer.

Basic > VLAN Setting

The VLAN provides broadcast filtering, security, address summarization, and traffic flow management. VLAN tagging is to control traffic flow patterns and react to port relocations.

Note: LAN3 is not supported for *EB1-T002-TLD01* as per hardware design.

This page lets you configure the wireless Access Point, VLAN tagging configuration and additional function of the wireless AP.

The new features of this firmware are described as follows:

1. VLAN Tagging function in Access Point mode
2. VLAN Tagging function in Ethernet Bridge mode
3. Management VLAN support for both Access Point and Ethernet Bridge mode
4. Viper features enable for EB1-T002-TLD01

VLAN mode: Can be set as enabled or disabled.

VLAN Tagging: Can be configured both in AP & Bridge mode.

Once the AP or Bridge is set to **Enabled mode**, use LAN1 as your uplink port to connect to your PC (for configuration use). You may also set LAN2 port to have the same VLAN ID as the management port to enable the PC connected to LAN2 to get access to webpage or management console.

Basic > Vlan Setting

The applications set vlan configurations.

VLAN Mode: Enable ▼

Vlan Setting Table

Port	Vlan ID
Vap0	1
Vap1	2
Vap2	3
Vap3	4
LAN1	5
LAN2	8
LAN3	7
Management	8

must have the same VLAN ID

Help Save Reset

Note: Any change in configurations will take effect after reboot!

VLAN Settings Table: are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLAN tagging addresses issues such as scalability, security, and network management.

Wireless > Basic Setting

This page lets you configure the wireless settings of the Access Point. There are 2 sections: Radio and Security.

Wireless AP & Ethernet Bridge (11b/g)

Log Out

System Summary   Setup Wizard   Basic   Wireless   System Tools

Wireless Setting > Basic Setting

☑ **Enable Wireless**
☑ **Disable Wireless if VDSL Down**

Operation mode: ⊙ Access Point ○ Ethernet Bridge
Configured BSS: ⊙ BSS0 ○ BSS1 ○ BSS2 ○ BSS3
Enabled BSS: ☑ BSS0 ☑ BSS1 ☑ BSS2 ☑ BSS3
SSID: 11g-0
    SSID suppressed: ○ Yes ⊙ No
Channel: 2437MHz (Channel 6) ▼
Wireless Mode: 2.4GHz 54Mbps (802.11g) ▼
Enable WDS: ☐
Wireless Isolation: ☐

Wireless AP & Ethernet Bridge (11b/g)

Log Out

System Summary   Setup Wizard   Basic   Wireless   System Tools

Wireless Setting > Basic Setting

☑ **Enable Wireless**
☑ **Disable Wireless if VDSL Down**

Operation mode: ○ Access Point ⊙ Ethernet Bridge
SSID: 11g-0
    SSID suppressed: ○ Yes ⊙ No
Channel: 2437MHz (Channel 6) ▼
Wireless Mode: 2.4GHz 54Mbps (802.11g) ▼
Remote AP MAC Address   00:00:00:00:00:00
    00:00:00:00:00:00
    00:00:00:00:00:00

Enable Wireless: Tick to enable wireless function. With this function, laptop with card bus or in-built wireless function can access the AP wirelessly.

SSID: Service Set Identifier. It is a sequence of characters that uniquely names a Wireless LAN. This name allows PCs to connect to the correct Wireless Access Point when multiple Access Points (or Wireless Routers) operate in the same location.

Channel: The radio channel number. You can select channel 1 to 11 or use SmartSelect, where the Access Point will select the cleanest channel to use upon booting up. The number of channels varies according to countries.

SSID Suppressed: When SSID is suppressed, the wireless AP will not broadcast the SSID. Unwelcome PCs will not be able to scan for the SSID of this AP, and they can only associate if they know exactly what the SSID is.

Wireless Mode: You can choose to operate the wireless Access Point **802.11g** or **802.11b** mode. The data rate for 802.11g is 54Mbps while the data rate for 802.11b is 11Mbps. 802.11g is compatible with 802.11b.Other model such as the APRT-2518gs, you will be able to select Dynamic Turbo or Static Turbo Mode. Turbo mode operates in 108Mbps.

Security Mode: This section allows you to configure wireless encryption to prevent unwelcome parties from reading your traffic. You must **Enable** the Security Mode before choosing the type of wireless security

Open-System/Shared Key
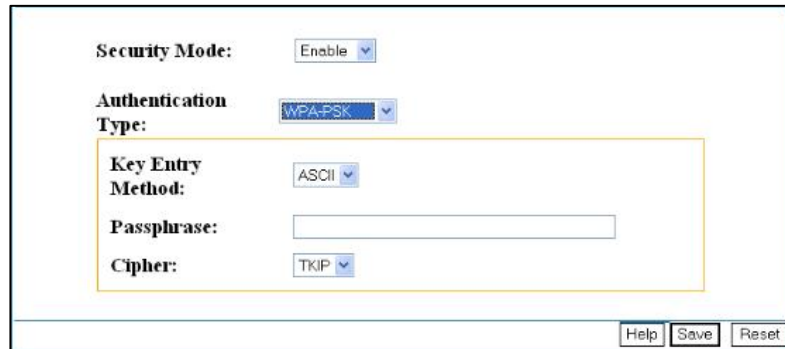
System: When chosen, the Key is not used for authentication. It is only used for encryption. Open-System uses Static Keys for encryption. Static (Shared) Keys are never changed, and a hacker can crack the key after a period of time.

Shared-Key: When chosen, the encryption Key is also used for authentication between the Access Point and Client. Note that this system is also using Static Keys.

Key Entry Method: Choose **HEX** if you want to enter the Keys in hexadecimal format. Otherwise, enter in ASCII format. ASCII is also called Alphanumeric in some systems. Use the same key format for the Access Point and Client!

Key 1-4: The Key is to be entered in the boxes. The **SAME Key** must be entered in both the Access Point and Client. Take note that there is a different Key length for a different number of encryption bits. 152 bits is the most secure, but make sure that your Client card supports it. The last point to take note is that if you use Key 4 on the AP, you must also use Key 4 on the Client, for example. The same logic applies for Keys 1-3.

WPA-PSK

WPA-PSK is also known as WPA-Preset-Key. This implementation is more secure than WEP as the encryption is automatically changed periodically. To configure this feature, just key in an 8-63 ASCII character or 64 HEX character pass-phrase for both the Router and Cards.

Cipher: You can choose to use TKIP or AES for the cipher type.

WPA
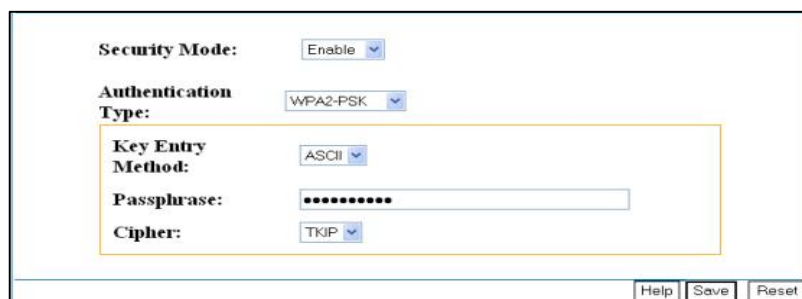
WPA (**W**iFi **P**rotected **A**ccess) is a standard where the Wireless Card has to authenticate to a RADIUS Server, through the Access Point. The Server can also manage the encryption keys such that they are changed dynamically. You need to have a RADIUS Server to be able to use this feature.

RADIUS Server: Enter the IP Address and the port of the RADIUS Server.

Shared Secret: Enter the Shared Secret of the RADIUS Server.

Confirm Source: Enter the Shared Secret again to confirm.

Wireless > Advance Setting

This page allows you to configure the advance wireless setting of the Access Point.

Date Rate (Mbps): You can set the wireless data rate from the available list or choose the best to allow the access point to choose the most appropriate data rate. When Best is used, the access point will determine the optimal data rate according to the environment.

Transmit Power: To adjust the transmit power of the antenna. Sometimes, it is useful to decrease the coverage range of each access point, so that more AP's can be located together without interfering one another.

Preamble: Choose Short Preamble or Long Preamble. Most manufacturers implement long preambles. Even if there is a mismatch between the access point and the card, they can still connect well and the mismatch may not be noticeable to most users. Do not change this setting without seeking advice.

Slot Time: Choose short or long slot time. The slot time is the amount of time a device waits after a collision before retransmitting.

Wireless > MAC Address Control

This page allows you to specify which *wireless* computer can get access to the internet and which *wireless* computer cannot access the internet. The specified MAC address and the policy for the computer are reflected in the table.

Enable Wireless MAC Control: Tick to enable Wireless MAC Control.

Default Policy: This policy determines whether computers, whose MAC addresses are not in the table, are able to access the Internet. If you choose **Deny All**, all computer associated to the access point will not be able to access the internet other than those specified in the table.

MAC Address: Enter the MAC address of the computer. The format for the MAC address is aa:bb:cc:dd:ee:ff.

Policy: Choose to deny or allow the computer to access the computer. Click on the *Add* button to add the policy.

IP Address pool: When 'System Define' is selected, router will assign IP address automatically from the pre-defined pool. If 'User Define' is selected, you would have to define the range of the pool manually.

IP Address pool (For User Defined only), Start Address: This is the start address of the DHCP pool. The router will assign this to the first computer connected to the router.

IP Address pool (For User Defined only), End Address: This is the end address that the router will assign to the computers connected to the router.

Lease Time: The amount of time a network computer will be allowed to connect with the DHCP Server. By default, the lease time is 2880 minutes.

System Tools > System Log

This page allows you to configure the wireless AP to dump its status to a System Log Server.

Enable Remote System Log: Enable this feature to allow the wireless to constantly update its status on a System log Server.

System Log Server IP: Enter the IP Address of the System Log Server if you had enabled Remote Logging.

System Log Server Port: Enter the port number the System Log Server is using.

Enable Local System Log: Enable this feature if you do not have a System log Server. The events would then be logged locally on the Router.

Log Management when log is full (Stop Logging): When this option is chosen, the Router will stop logging.

Log Management when log is full (Auto Delete): The maximum number of local log entry is 200. When all the 200 entries are used up, the Router will overwrite previous entries with new logs.

Remember to click **Apply** and **Reboot** for the settings to take effect.

System Tools > System Admin

This page allows you to change the Administrator's Username and Password. The default username and password is admin / admin. After every **Factory Reset**, the Router reverts to this combination.
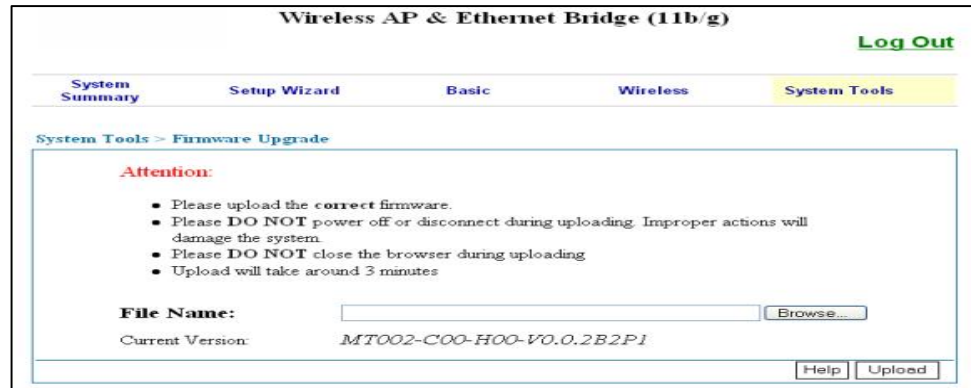

System Tools > Backup/Restore Settings

Use this page to preserve any good setting. You can save the configuration file into your computer and upload it back to the wireless AP when the setting of your AP when necessary. In addition, you can do a factory reset and restore the Access Point back to factory default setting. The factory default setting is shown in the *Factory Reset* section.

System Tools > Firmware Update

This page allows you to update the firmware (software) in the wireless AP. New firmware is issued to improve the performance and provide additional features to the product.

1. The new firmware is a file name "apimg1".
2. Save the file in your PC.
3. **Browse** and select the firmware file.

You will see the following page when firmware upgrading is successful.

Upload Succeeds.

The file has been uploaded.

Back

⚠	Do not close the browser or shutdown the Router during firmware upgrading. Failure to do so will cause serious damage to Router.

6   FACTORY RESET

When you have wrongly configured the wireless Access Point and wish to start all over again, you can perform a Factory Reset to restore the AP to its original state. Simply use a paper clip or any pointed object to press in the switch button for 10 seconds and release.
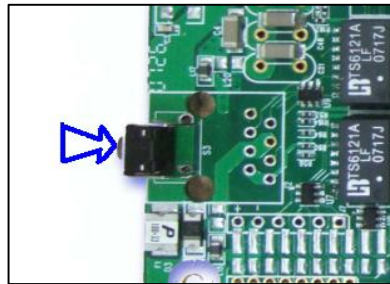
The wireless Access Point would be reset to its original Factory Default configuration:

Access Point Feature	Factory Default
User Name	admin
Password	admin
WAN IP	-
WAN subnet mask	-
LAN IP	10.0.0.1
LAN subnet mask	255.255.255.0
SysLog	Local System logging on
SSID	11g
Channel	SmartSelect
MAC Address Control	Off
Wireless Security	Off
DMZ	Off
Virtual Server	Off
IP Filter	Off.

7 TECHNICAL SUPPORT

For technical support, please contact the following local distributor or reseller.

8 DISCLAIMER

- Manufacturer assumes no responsibility for any damage or loss resulting from the use of this manual.
- Manufacturer assumes no responsibility for any loss or claims by third parties that may arise through the use of this product.
- Manufacturer assumes no responsibility for any damage or loss caused by incorrect use of Wireless Access Point, 802.11g & Ethernet Bridge.
- The contents of this manual are subject to change without prior notice due to engineering improvement.
- No part of this manual may be reproduced in any form without the express written consent of the Manufacturer.
- Sample displays shown in this Manual may differ somewhat from the displays actually produced by the product.
- User Manual may differ for different firmware version.
- All brands and product names are trademarks or registered trademarks of their respective holders.