User Manual

AP - 2001G

Brand	Model Number	Description
RFNet	AP - 2001G	Wireless LAN 802.11b/g AP & Ethernet Bridge
Teraoka	AP - 2001G	Wireless LAN 802.11b/g AP & Ethernet Bridge

Revision: 1.1

Last updated: 3 Mar 08

FCC Compliance

NOTE: 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.

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

Important Note:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth 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.

This device is intended only for OEM integrators under the following conditions:

1) The antenna must be installed such that 20cm is maintained between the antenna and users, and
2) The transmitter module may not be co-located with any other transmitter or antenna.

As long as 2 conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end product for any additional compliance requirements required with this module installed (for example, digital device emissions, PC peripheral requirements, etc.)

IMPORTANT NOTE: In the event that these conditions cannot be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID cannot be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the product (Including the transmitter) and obtaining a separate FCC authorization.

End Product Labeling

This transmitter module is authorized only for use in device where the antenna may be installed such that 20cm may be maintained between the antenna and users (for example: Notebook, Access Point, Router and similar product). The final end product must be labeled in a visible area with the following: “Contains **TX FCC ID: PXPAP2001G**’’.

Manual Information That Must be Included

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the user’s manual of the end product which integrates this module.
The user’s manual for OEM integrators must include the following information in a prominent location “IMPORTANT NOTE: To comply with FCC RF exposure compliance requirements. The antenna must not be co-located or operating in conjunction with any other antenna or transmitter and antenna must be installed such that 20cm is maintained between the antenna and users

Canada-Industry Canada (IC)

Operation is subject to the following two conditions:

1) This device may not cause interference and
2) This device must accept any interference, including interference that may cause undesired operation of the device.

This device has been designed to operate with an antenna having a maximum gain of 0.52 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

Contents

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.

This product could operate as either one of the following modes:

a. Access Point mode, or
b. Wireless Ethernet Bridge mode.

Product Features

- Fully compatibility with **IEEE 802.11g** WLAN standard
- Wireless data rate of up to **54Mbps**
- **2.4GHz** license-free frequency band
- Adjustable Radio Transmit Power
- Two LAN ports
- Full backward compatibility with **802.11b** standard (WiFi 11Mbps)
- Management support for administration control with ID & password, Web and Telnet.
- **802.1x** Authentication (For AP mode only). Used with a RADIUS server to check and verify the identity of WLAN users.
- **WEP** (Wired Equivalent Privacy). A simple WLAN encryption standard to protect wireless data from sniffers.
- **WPA** (WiFi Protected Access), for AP mode only. An improved WLAN encryption standard where the secret key renew automatically at regular intervals.
  - **TKIP** (Temporal Key Integrity Protocol). A new encryption key will be generated by corporate RADIUS server when a authorized wireless adaptor/user associate with the Access Point. This encryption key renew automatically at regular intervals. This is normally used in high security enterprise networks.
  - **Pre Shared Key (WPA-PSK).** A new key is generated each time a wireless adaptor connects to the Access Point. This normally used for home user without a RADIUS server.
- Intuitive Web-based configuration
- **Access Control List** provides added security for AP mode.

Basic IP Networking

IP = Internet Protocol

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 IPs 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 AP-2001g 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!

Wireless LAN Basics

A Wireless LAN (WLAN) is a computer network that transmits and receives data with radio signals instead of using cables. WLANs 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 AP-2001g is based on the finalised **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 AP-2001g at 11Mbps.

The AP-2001g can even support 108Mbps wireless data rate at Turbo mode. This is only applicable for user using recommended Turbo-capable Cardbus (with Atheros chipset).

The AP-2001g is also known as the Wireless Access Point (**AP**). The PC using the Cardbus 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 SSIDs to let the user choose from.

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 AP (Router), such that the AP only allows this pool of MAC Addresses to use the WLAN.

Channel

There are a total of 13 channels in the 2.4GHz band. Depending on regulation, not all the frequencies may be available in every country. Frequency is configured on the AP only. The client searches for the 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, a 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 AP, make sure that you:

- Keep the distance from the 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 APs are located far away from one another to avoid interference.

Interference

Interference happens when 2 APs with the same channels are placed near to one another. The speed of the network drops and the signal strength fluctuates wildly.

Roaming

Association happens when the SSID, Encryption and MAC Address Control settings are correct between the AP and client. If 2 APs with these same settings are located in the same area, the client would choose to associate to the one which gives it a better signal strength. The client would roam over to the 2nd AP when he moves nearer to it. The client switches AP and frequency as he does so.

GETTING STARTED

Connecting AP-2001g

This manual is for both AP-2001g and EB1-T002-TRK. Connect RJ45 and the power adapter as shown in Figure 1.

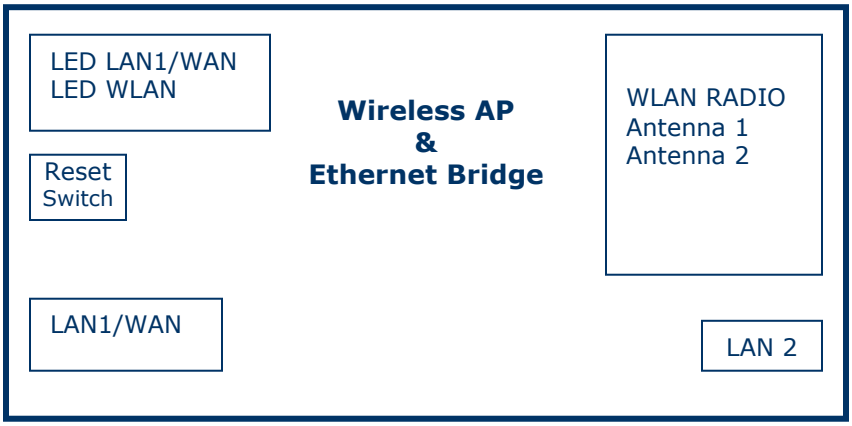


Figure 1

AP-2001g CONFIGURATION

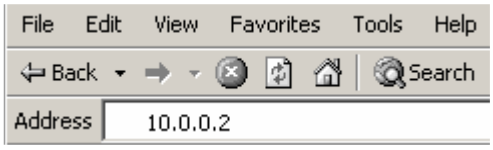
Web Configuration

AP-2001g can be configured using a web server.

1. Connect the network as shown previously.

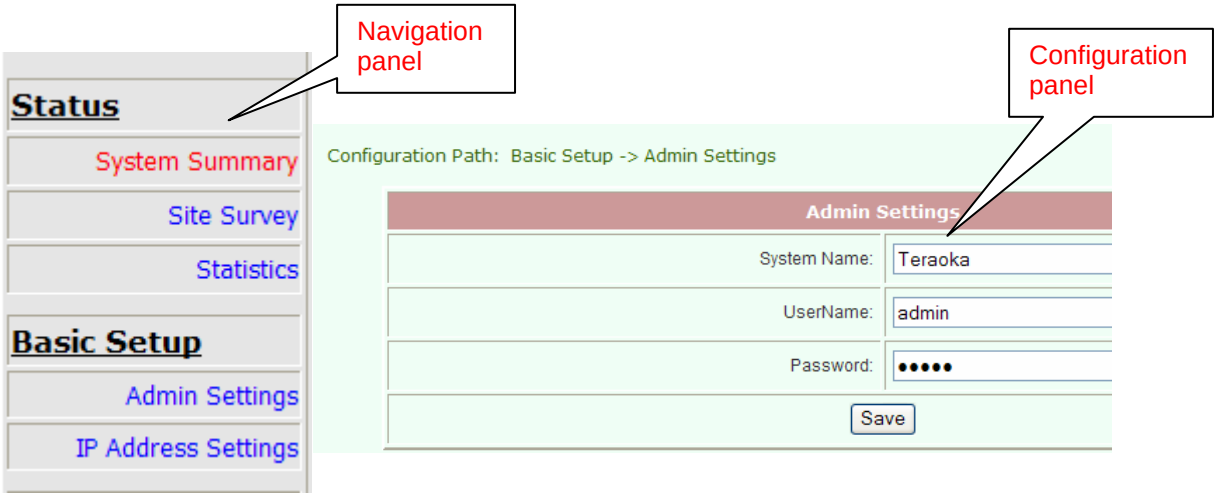
- If you are accessing the web server via Ethernet cable, check that the upper LED lights up on AP-2001g.
- If your PC is **wireless**, check the PC's card utility to make sure that the signal strength is good and that the bottom LED lights up on AP-2001g.

2. Open a Web browser (Internet Explorer, Netscape etc.).
3. Type AP-2001g LAN IP (**10.0.0.2**) address into the browser's Address field. The default LAN IP address of AP-2001g is 10.0.0.2.



4. Enter username and password. The default username is admin and the default password is admin.

In every AP-2001g Web Configuration page, the left panel is the navigation menu containing the main sections. The right-side frame is where the detailed configuration is done.



Remember that after every configuration change, it is necessary to:

- Click **Save** on the page.
- **Reboot** AP2001g.

The changes take effect only **AFTER Reboot**.

Status

System Summary

This page presents a convenient overview of the overall status of the AP-2001g. The most common configuration parameters are shown here, for a quick look.

System Summary

Basic Information	
System Name:	Teraoka
Operation Mode:	Client
WDS:	Disable
Wireless Access Control :	Disable
SSID:	Teraoka
Channel:	Current Channel 11: 2462MHz
Wireless Mode:	802.11g
State:	Disconnected

Advanced Information			
Data Rate:	Best	Short Slot Time:	Enable
Transmit Power:	Full	Short Preamble:	Enable
Antenna Diversity:	Best	Protection Mode:	Auto
Fragment Length:	2346	Protection Type:	cts only
RTS/CTS Threshold:	2346	Protection Rate:	11Mbps

Security Information	
Security Mode:	NONE
RADIUS Server:	:1812
Key Entry Method:	
Authentication Type:	
Key ID:	1
Cipher Type:	

Site Survey

This page shows all the AP around AP-2001g. It also shows details such as the SSID, channel, MAC Address, radio mode and etc. of the surrounding AP.

Index	ESSID	BSSID	Radio Mode	Channel	Signal Strength (RSSI)	Link Quality	Security Mode	Network Mode
1	105_AP	00:06:C7:14:07:BC	802.11g	6	30	100%	NONE	Infrastructure
2	wpa-eap	00:09:CA:02:6C:7A	802.11g	11	46	100%	WPA	Infrastructure
3	iconnect_mc	00:0A:06:FF:80:CA	802.11g	11	4	30%	NONE	Infrastructure
4	iconnect	00:06:C7:01:00:C8	802.11g	5	39	100%	NONE	Infrastructure

Statistics

This page shows the Statistics of AP-2001g such as the signal strength of the radio, the data rate, the error rate and etc.

Statistics

-	Signal Strength (RSSI)	Data Rate (Mbps)
Receive	13	1
Transmit	30	1 | 1

Encryption	Advertised Cipher	Unicast Cipher	Multicast Cipher
no	None	None	None

Authentication	Deauthentication	Association	Disassociation	Reassociation
0	0	0	0	0

-	MSDU	Data	Multicast	Management	Control
Receive	0	0	0	9546	0
Transmit	5004	0	5004	12784	0

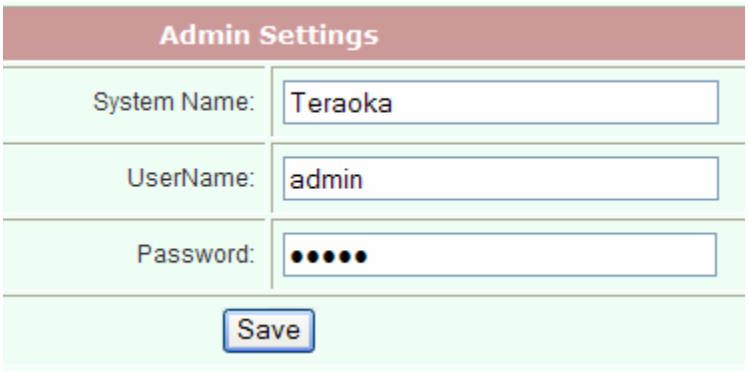
Receive	Discarded Frames	Duplicate Frames	CRC Errors	Decrypt Errors	DMA Errors
-	0	0	78842	0	0

Transmit	Discarded Frames	Excessive Retries	DMA Errors
-	7778	0	0

Basic Setup

Admin Setting

This page allows you to change the System Name, Username and Password for AP-2001g. The default system name is Teraoka and the default username and password is admin / admin. After every factory reset, the Username and Password reverts to this combination.



The username and password are case sensitive.

User Setting

This page allows you to change the User name and Password of the new user.
The default User name is user and the password is user

IP Address Setting

This page allows you to change the IP address, Subnet Mask and Gateway of AP-2001g. The default IP address is 10.0.0.2.

Wireless Setup

Basic Setting

This page allows you to change the basic settings of the wireless configuration.

Operation Mode: AP-2001g can be used as an Access Point or as a Wireless Client. The default setting is Client
WDS: Wireless Distribution System. Enable WDS allows more than one user to connect to AP-2001g. Disable WDS allows only one user to connect to AP-2001g. The default setting is WDS disable.
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 operate in the same location. The default SSID is Teroaka.
Wireless Mode: To choose to operate the AP or Client in 802.11b or 802.11g. Both operate in the frequency of 2.4GHz but 802.11g has a faster data rate of 54Mbps as compared to the 11Mbps of 802.11b.

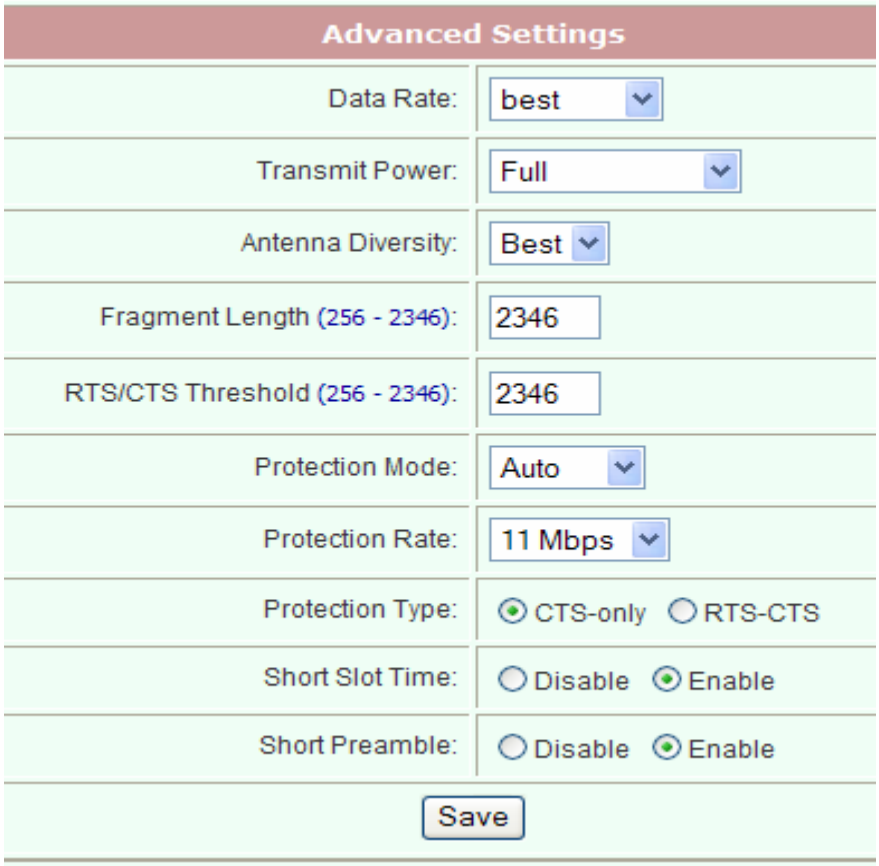
Country: List of different countries which you can choose and set for the AP-2001g device.
Radio Channel: There are 11 different frequency channels. You can choose to set the frequency channel to use or use SmartSelect for automatic channel selection.

Remember that after every configuration change, it is necessary to:

- Click **Save** on the page.
- **Reboot** AP-2001g.

The changes take effect only **AFTER Reboot**.

Advance Setting

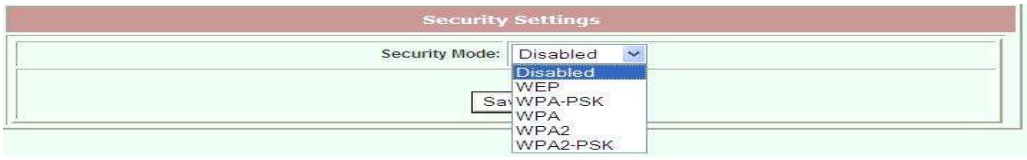


Data Rate: You can fix the data rate to different values as 11Mbps or 24Mbps. However it is recommended to set the setting to “Best” for AP-2001g to determine the best data rate to be use.

Transmit Power: Sometimes, it is useful to decrease the coverage range of each AP-2001g, so that more AP-2001g can be located together without interference to one another. The default transmission power is 100% (full).
Antenna Diversity: Allows you to choose which antenna to use. Always choose Best for best performance. Do not change this setting without seeking advice.
Fragment Length: Specifies the fragment length. Enter a value between 256 and 2346.
RTS/CTS Threshold: Enter a value between 256 and 2346
Protection Mode: Select None, Always or Auto
Protection Rate: Select 1Mbps, 2Mbps, 5.5Mbps or 11Mbps
Protection Type: Select either CTS only or RTS-CTS
Short Slot Time: Enable or disable short time slot usage
Short Preamble: Enable to use Short Preamble in the Wireless LAN packet headers. Most manufacturers implement long preambles. Even if there is a mismatch between AP-2001g and the client, they can still connect well and the mismatch may not be noticeable to most users. Do not change this setting without seeking advice.

Security Setting

This page allows you to choose the wireless security setting. WPA is only available if AP-2001g operates as an Access Point. If AP-2001g is in Client mode, WPA is not available.

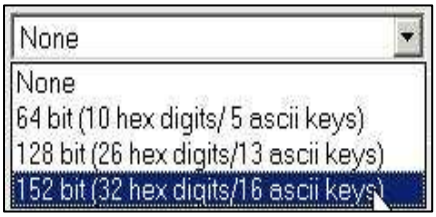


Disabled: To disable wireless security.
WEP: To enable WEP security.
WPA_PSK: To enable WPA PSK Security.
WPA: To enable WPA Security.
WPA2: To enable WPA2 Security
WPA2-PSK: To enable WPA2-PSK Security

WEP Security

Open System: The key is used for encryption only. No authentication is required. To configure, enter the encryption Key in the “Encryption Key” field.
Pre-shared Key: When chosen, the encryption Key is also used for authentication. To configure, enter the encryption Key in the “Encryption Key” field.

Key Entry Method: Choose Hexadecimal if you want to enter the Keys in hexadecimal format. Otherwise, choose Ascii Text to enter the Key in ASCII format. ASCII is also called Alphanumeric in some systems.
Key Length: Choose the number of bit for the encryption key.



WPA-PSK Security

Key Entry Method: Choose Hexadecimal if you want to enter the Keys in hexadecimal format. Otherwise, choose Ascii Text to enter the Key in ASCII format. ASCII is also called Alphanumeric in some systems.
Key: Enter the Encryption key. The Encryption key has to be between 8 - 64 characters.
Cipher Type: Choose TKIP or AES

Hexadecimal Characters:
0,1,2,3,4,5,6,7,8,9 and a,b,c,d,e,f

ASCII Characters:
0,1,2,……8,9 and
a,b,c,d,…….x,y,z

WPA Security

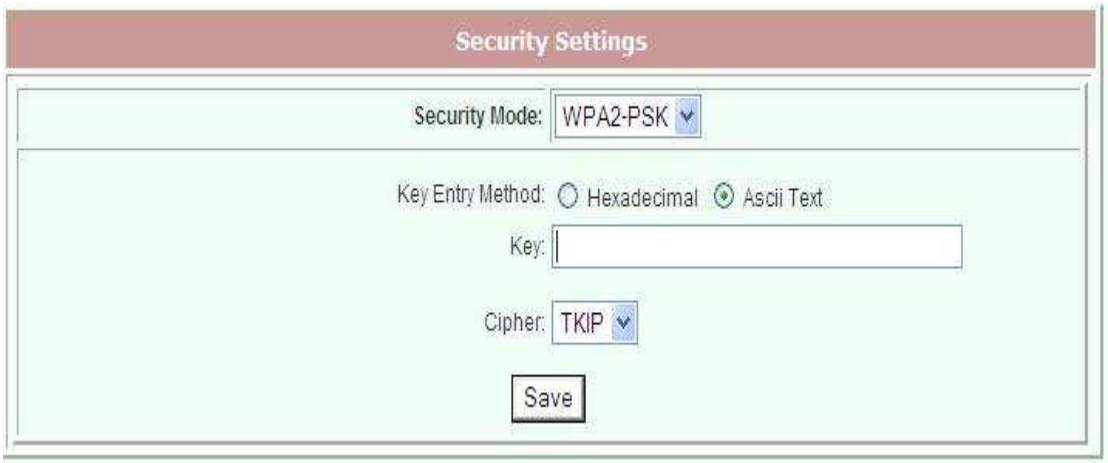
This security setting is only available when AP-2001g is operating as an Access Point.

RADIUS Server: Enter the IP Address or the Name of the RADIUS Server (for 802.1x authentication purposes). This is used only when you have a RADIUS Server and want to use it for authenticating the Wireless Clients.
RADIUS Secret: Enter the Shared Secret of the RADIUS Server. (Only if 802.1x protocol is used)
Confirm Shared Secret: Enter the Shared Secret again.
RADIUS Port: Enter the port number of the RADIUS Server.

WPA2 Security

Common feature for both Access Point and Wireless Ethernet Bridge mode

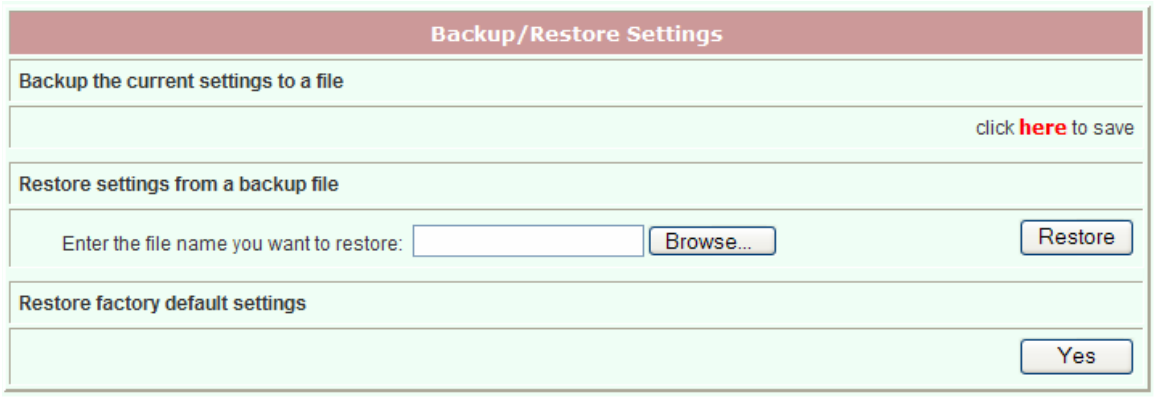
WPA2-PSK Security



Key Entry Method: Choose Hexadecimal if you want to enter the Keys in hexadecimal format. Otherwise, choose ASCII Text to enter the Key in ASCII format. ASCII is also called Alphanumeric in some systems.
Key: Enter the Encryption key. The Encryption key has to be between 8 - 64 characters.
Cipher Type: Choose TKIP or AES

System Setup

Backup/Restore Settings



Backup the current settings to a file: To save the current configuration of AP-2001g.
Restore settings from a backup file: To restore the previous configuration that was previously saved.
Restore factory default settings: To restore AP-2001g back to factory default.

Firmware Upload

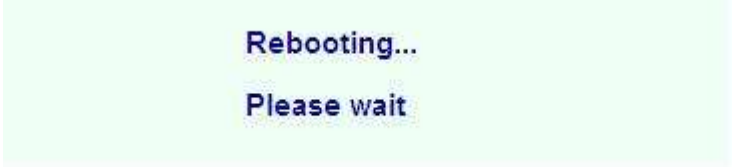
This page allows you to update the firmware (software) in AP-2001g. New firmware is issued to improve the performance and add features to the product.

Browse to the new firmware file name apimg1 and click upload. Do not change the filename of the new firmware as doing so will cause the upgrading process to fail.

Do not change the filename of the new firmware. New firmware with filename other than “apimg1” will cause the process to fail.

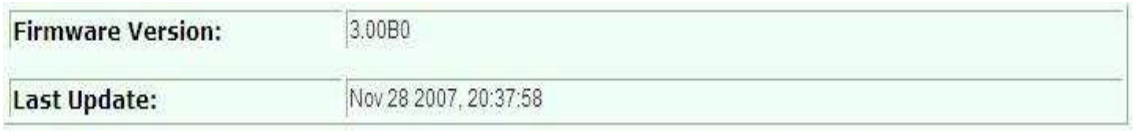
Reboot

This page allows you to check when you do the device rebooting until such time the system is up.



About

This page shows the firmware version and the date at which the firmware was updated.



Factory Default Setting

To set the wireless bridge back to factory default setting, press the reset button for 5sec and release.

The factory default setting is as follows:

No	Item	Factory Default
1	User ID (for configuration)	admin
2	Password (for configuration)	admin
3	Default Static IP address	10.0.0.2
4	Default Subnet Mask	255.0.0.0
5	Default Gateway Address	0.0.0.0
6	WLAN Client Mode	Client
7	WDS	Disable
8	ESSID	Teraoka
9	WEP/WPA	Off
10	Radio Power	100%
11	FTP Port	1301
12	Country Default	NA
13	Additional Files in Flash	Version
14	Firmware Version	Version 3.00B0