802.11g Wireless LAN Travel Kit

WAP-4050

User's Manual

Copyright

Copyright© 2004 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes..

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

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 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:

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

FCC Caution:

To assure continued compliance.(example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

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.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm(8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8,2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

Revision

User's Manual for PLANET 802.11g Wireless LAN Travel Kit

Model: WAP-4050

Rev: 1.0 (September, 2004)

Part No. EM-WAP4050v1

TABLE OF CONTENTS

Chapter 1 Introduction

Thank you for purchasing WAP-4050.

As small as a box of poker cards, the WAP-4050 is not only a wireless access point but also a wireless NAT router and Ethernet adapter. With these three most commonly used operating mode, WAP-4050 provides greater flexibility for a mobile user in various environments.

This manual guides you on how to install and properly use the WAP-4050 in order to take full advantage of its features.

1.1 Package Contents

Make sure that you have the following items:

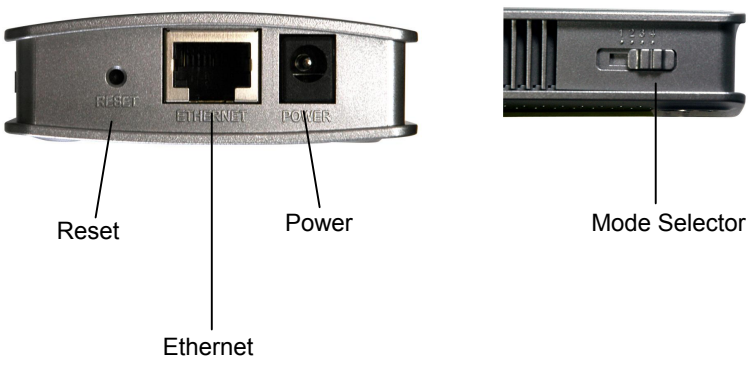
- 802.11g WLAN Pocket AP
- Power Adapter
- Quick Installation Guide
- User's manual CD
- RJ-45 cable
- Travel bag

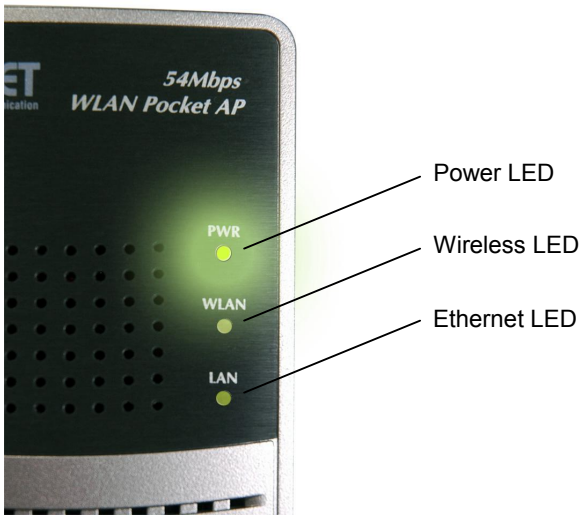
Note:	If any of the above items are missing, contact your supplier as soon as possible.

1.2 Features

- Wireless standard IEEE 802.11b/g compliant
- Pocket size wireless access point
- 3 operating modes selectable: AP, NAT Router, and AP Client
- Up to 54Mbps data rate
- Support WPA-PSK and 64/128-bit WEP encryption
- Support MAC Access Control in AP and AP/Router modes
- Support DDNS, DMZ, DHCP server, and virtual server in AP/Router mode
- Provide basic firewall features in AP/Router mode
- Support VPN pass through in AP/Router mode
- Driver free, plug 'n play

1.3 Physical Features





LED Indication	
Ethernet LED	• On - Ethernet connection established. • Off - No Ethernet connection. • Flashing - Data being transferred.
Wireless LED	• On - Wireless interface available. • Off - Wireless interface unavailable. • Flashing - Data being transferred.
Power LED	• On - Power is available. • Off - No power.
Physical Interface Description	
Mode Selector	This switch has 4 positions: 1 - AP Mode 2 - AP/Router Mode 3 - Config Mode 4 - Client Mode
Reset Button	This button has 2 functions: • **Restart** (reboot) - press & release. • **Set all settings to factory defaults** - press & hold (for 8 seconds), then release. Note: This should not be done while connected or using the WAP-4050.
Ethernet Port	Connect the 10/100BaseT Ethernet cable here. • In **AP mode** or **AP/Router mode**, this is connected to the LAN or WAN.

	• In **Config mode**, this should be directly connected to your PC. • In **Client mode**, this is connected to the Ethernet port of a network device.
Power	Connect the supplied power adapter here.

1.4 Specification

Standard	IEEE 802.11b, IEEE 802.11g	
Signal Type	DSSS (Direct Sequence Spread Spectrum)	
Modulation	BPSK / QPSK / CCK / OFDM	
Port	10/100Base-TX (RJ-45) * 1	
Antenna	Internal antenna	
Output Power	13dBm	
Sensitivity	802.11b	11 Mbps (CCK): -72dBm 5.5 Mbps (QPSK): - 76dBm 1, 2 Mbps (BPSK): - 80dBm (typically @PER < 8% packet size 1024 and @25ºC + 5ºC)
	802.11g	54 Mbps: -70dBm 48 Mbps: - 70dBm 36 Mbps: -72dBm 24 Mbps: -72dBm 18 Mbps: -74dBm 12 Mbps: -76dBm 9 Mbps: -79dBm 6 Mbps: -80dBm (typically @PER < 8% packet size 1024 and @25ºC + 5ºC)
Operating Mode	AP, AP/Router, AP Client	
Security	64/128-bit WEP encryption WPA-PSK Password Protect MAC Filtering SSID Broadcast Disable function	
Frequency Band	2.4 GHz ~2.484GHz	
Data Rate	802.11g	Up to 54Mbps (6/ 9/ 12/ 18/ 24/ 36/ 48/ 54)
	802.11b	Up to 11Mbps (1/ 2/ 5.5/ 11)

1.5 Wireless Performance

The following information will help you utilizing the wireless performance, and operating coverage of WAP-4050.

1. Site selection

To avoid interferences, please locate WAP-4050 and wireless clients away from transformers, microwave ovens, heavy-duty motors, refrigerators, fluorescent lights, and other industrial equipments. Keep the number of walls, or ceilings between AP and clients as few as possible; otherwise the signal strength may be seriously reduced.

2. Environmental factors

The wireless network is easily affected by many environmental factors. Every environment is unique with different obstacles, construction materials, weather, etc. It is hard to determine the exact operating range of WAP-4050 in a specific location without testing.

3. WLAN type

If WAP-4050 is installed in an 802.11b and 802.11g mixed WLAN, its performance will reduced significantly. Because every 802.11g OFDM packet needs to be preceded by an RTS-CTS or CTS packet exchange that can be recognized by legacy 802.11b devices. This additional overhead lowers the speed. If there are no 802.11b devices connected, or if connections to all 802.11b devices are denied so that WAP-4050 can operate in 11g-only mode, then its data rate should actually 54Mbps.

1.6 Network Setup

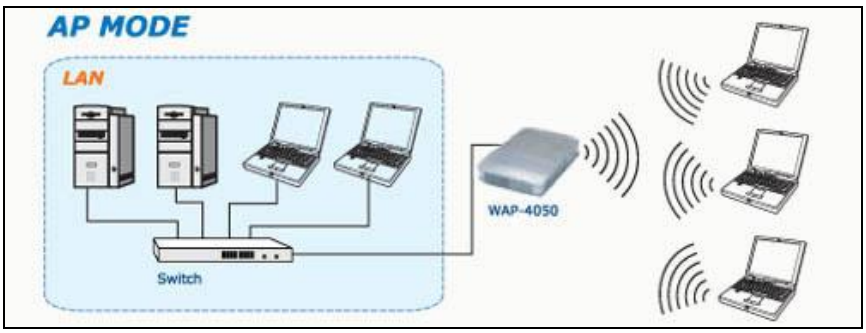
The WAP-4050 can be configured as an AP, AP/Router, or AP client. It is recommended to determine your network settings before installing WAP-4050.

Note: While you can change modes at any time, please pay attention to the following points:

- Whenever the mode is changed, the WAP-4050 will restart. You need to wait for the restart to be completed, which will take a few seconds. When the restart is completed, the Wireless LED will be ON.
- After changing modes, any Wireless connections will be lost. On your PC, you need to select the SSID (Wireless LAN) for the new mode in order to re-establish a Wireless connection to the WAP-4050.

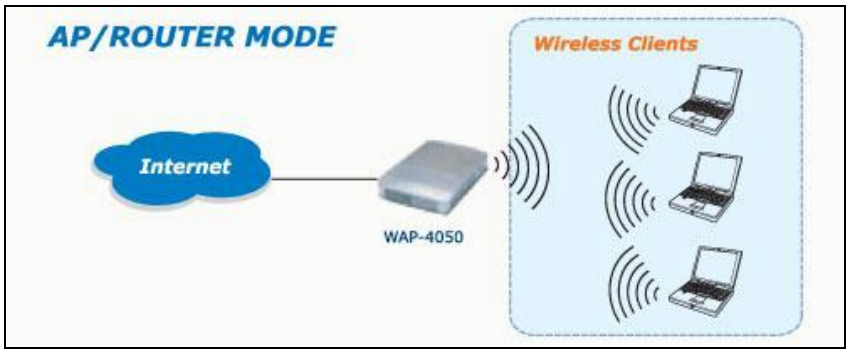
1.6.1 AP Mode

In AP mode, the WAP-4050 allows wireless clients to connect to LAN or WLAN.



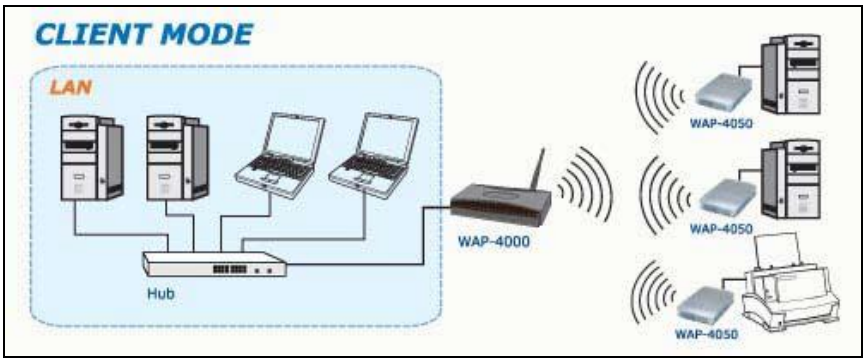
1.6.2 AP/Router Mode

In AP/Router mode, the WAP-4050 allows wireless clients to share a single Internet connection.



1.6.3 Client Mode

In Client mode, the WAP-4050 converts an Ethernet-ready device into a wireless device.



Chapter 2 Initial Configuration

2.1 System Requirements

Before installing WAP-4050, make sure that your system meets the following requirements:

- Network cable. Use a standard 10/100BaseT network (UTP) cable with RJ45 connectors.
- The administrative PC must be installed TCP/IP protocol, and configured as a DHCP client.
- To use the Wireless interface, your PC must be compliant with the IEEE802.11b or IEEE802.11g specifications.

2.2 Procedures

1. Switch the mode selector to position 3 to enter Config mode.

2. Power up and wait for the Wireless LED to turn on. This indicates the WAP-4050 is ready.

Note: ONLY use the power adapter supplied with the WAP-4050. Otherwise, the product may be damaged.

If you want to reset your WAP-4050 to default settings, press the Reset button for 8 seconds.

3. Establish a wired or wireless connection to the WAP-4050. It is strongly suggested to use wired connection to configuration.

- Wired – directly connect a standard LAN cable from administrative PC to WAP-4050. Please note there should be no hub or switch in between.
- Wireless – use the wireless adapter to connect the WLAN with SSID: default. Please also check the MAC address of target AP to ensure you are associating to the correct AP.

4. Activate the web browser.

5. Enter "**config.ap**" in the "Location" or "Address" field. Or you can access the WAP-4050 by its default IP address in Config mode, i.e. http://192.168.0.1.

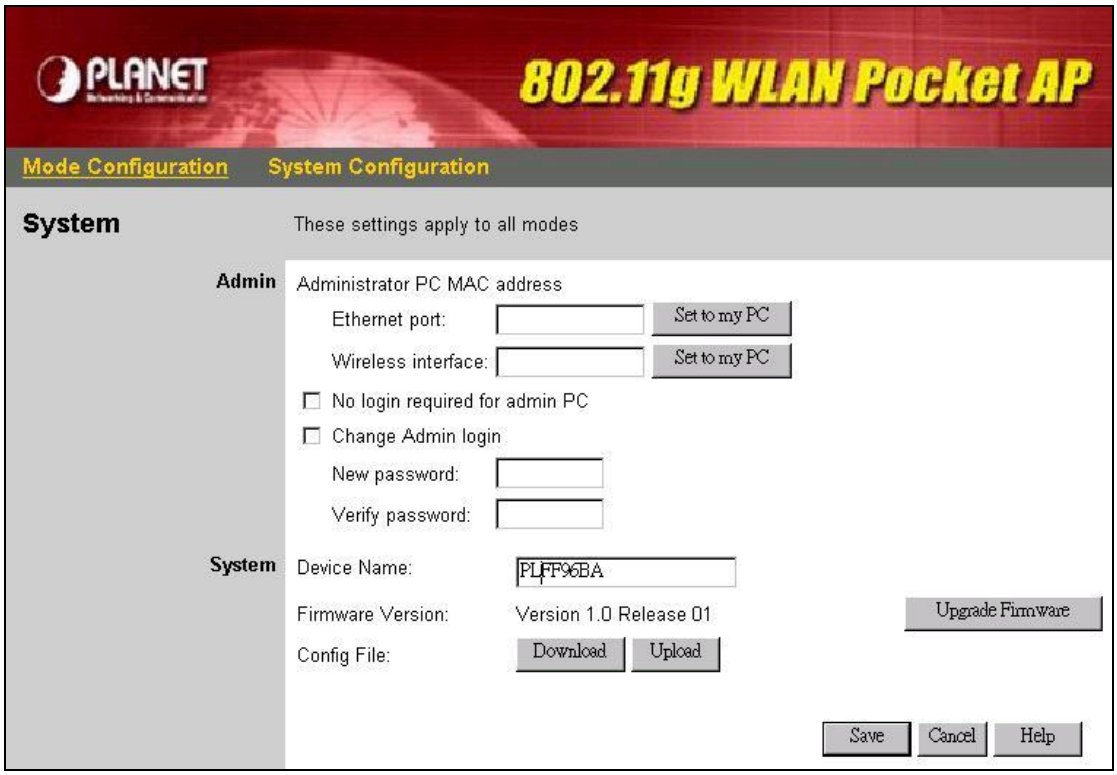
Note: Either being activated by wired or wireless interface. If the administrative PC has active wired and wireless interfaces at the same time, it may not be able to access WAP-4050 successfully.

6. By default, there is no username and password needed for the first time access. It is strongly suggested to set admin login password for securing the management access.

7. After successfully access the WAP-4050, you will see the **Mode Configuration** screen. As for the detailed settings of each mode, please refer to following chapters.

2.3 System Configuration

The settings of System Configuration screen will apply to all modes.



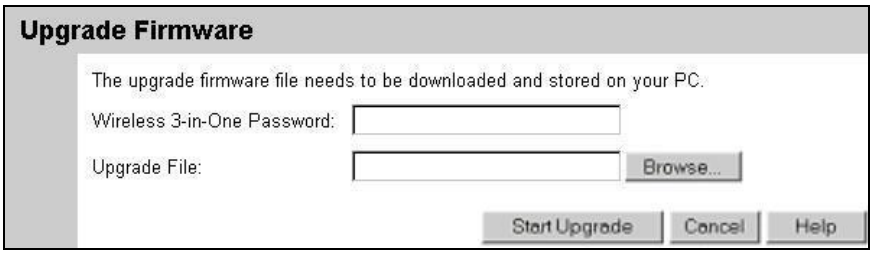
Admin	
Administrator PC MAC Address	This is used to identify your PC. If you normally use the same PC, you should provide this information. The MAC address is also called the "Physical Address". This address can be determined by checking the Properties for the desired network interface, but the provided **Set to my PC** buttons make this unnecessary. • **Ethernet Port** - the MAC address of the 10/100BaseT Ethernet Port on administrative PC. • **Wireless Interface** - the MAC address of the wireless interface on administrative PC. • **Set to my PC** - only 1 of these buttons will work. If you have connected via Wireless, click the button will insert your PC's wireless MAC address into the field provided. If you connected via the wired Ethernet interface, click the button will insert your PC's Ethernet MAC address into the field provided.

No login required for admin PC	If you check this, and provide the MAC address of administrative PC (see above), you will not be prompted for the password when using the specified PC. You **should** set a password for the admin login, using the password fields below. This option is provided to allow you to set a password, but avoid the inconvenience of being prompted for the password whenever you wish to change the settings.
Change Admin login	Check this box to change the current password, and then enter the required password in the fields below. If this checkbox is enabled, and the password fields left blank, then the password is cleared (set to no password).
New Password	Enter the new password here. Note that if the password is set, you will be prompted for the user name and password when you connect. You must use **admin** as the user name.
Verify Password	Re-enter the new password in this field, to ensure it is correct.
System	
Device Name	The name of the WAP-4050. You can change this if you wish.
Firmware version	This displays the current version of the firmware. Click the *Upgrade Firmware* button if you wish to install a new version of the firmware. • You need to download the new firmware file first. • Clicking the button will display the ***Upgrade Firmware*** screen. See the following section for further details.
Config File	This feature allows you to download (save) the current settings as a file on your PC, upload (restore) a previously-saved config file. Click the desired button: • Download will prompt you for the location, on your PC, for the configuration file. • Upload will display the ***Config File*** screen. See below for details.

2.3.1 Upgrade Firmware

To perform the firmware upgrade, please download the new firmware file to administrative PC first.

After clicking **Upgrade Firmware** button from **System** page, you will see the following screen.



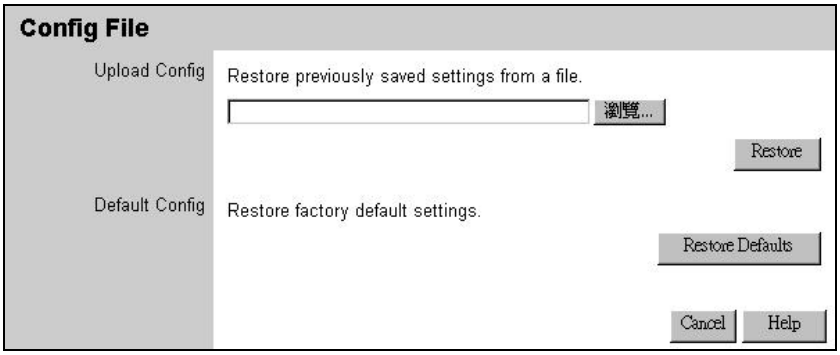
1. Enter the password of the WAP-4050.

2. Use **Browse** button to specify the firmware file.

3. Click **Start Upgrade** button to perform the task.

Note: WAP-4050 is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the WAP-4050 will be lost.

2.3.2 Config File



Restore Config	The feature allows you to restore a pre-saved configuration file back to the WAP-4050. Click **Browse** to select the configuration file, then click **Restore** to upload the configuration file. **WARNING:** Uploading a configuration file will destroy (overwrite) ALL of the existing settings.
Default Config	Clicking the **Restore Defaults** button will reset the WAP-4050 to its factory default settings. **WARNING:** This will delete ALL of the existing settings.

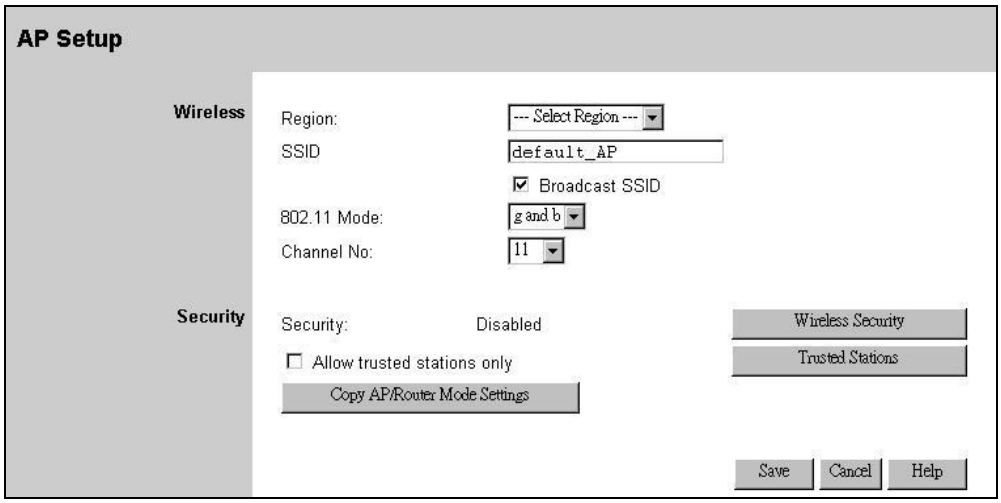
Chapter 3 Configuring the Wireless Access Point

3.1 AP Mode

WAP-4050 is not allowed to be configured in AP mode. Configuration for AP mode must be performed while in Config Mode.

Please follow the procedures described in section 2.2 to access the Mode Configuration screen and click on the Configure button in AP Mode.

3.1.1 AP Setup

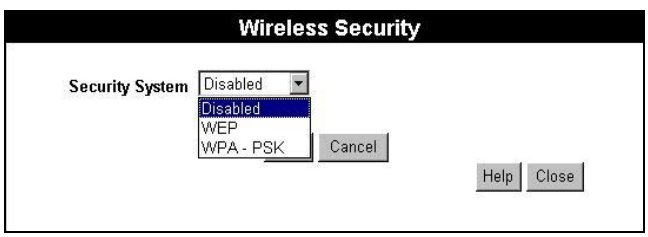


Wireless	
Region	Select your region from the drop-down list. This field displays the region of operation for which the wireless interface is intended. It may not be legal to operate the device in a region other than the region shown here. If your country or region is not listed, please check with your local government agency for more information on which channels you are allowed to use, and select a region that allows those channels. (The channel list changes according to the selected region.)
SSID	This field allows you to set the SSID of WAP-4050 in AP mode. The SSID is an identification string that differentiates from other WLANs. AP Mode and AP/Router mode must use different SSIDs. Using the same SSID for both modes would confuse Wireless clients. The default value is **default_AP**.
Broadcast SSID	Enable or disable a Service Set Identifier broadcast. When enabled, the SSID of the WAP-4050 is sent to wireless enabled devices on the area, thus may cause unauthorized user to connect your wireless networks.

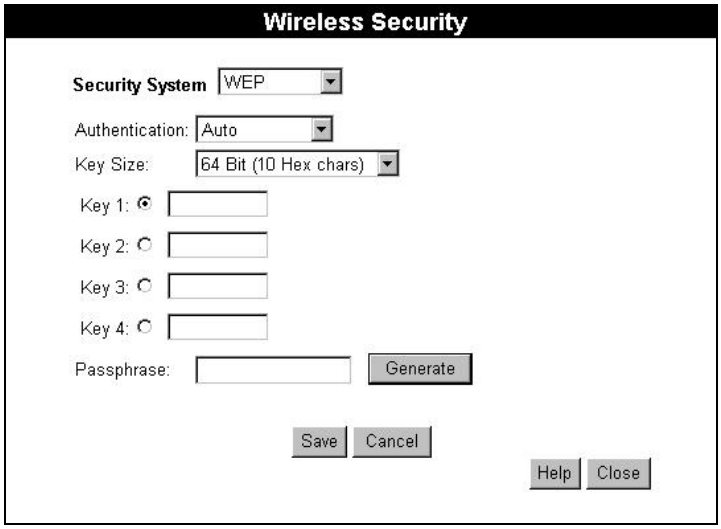
802.11 Mode	Select the desired mode: • **g & b** - Both 802.11.g and 802.11b Wireless stations will be able to use the WAP-4050. • **g only** - Only 802.11g Wireless stations can use the WAP-4050, and obtain better performance than in g & b mix mode..
Channel No.	This selection determines which operating frequency will be used. The channel list changes according to the selected region. Select the desired channel. Adjacent Access Points should use different channels to avoid interference.
Security	The current security settings for wireless connections are displayed. The default value is Off, meaning no security.
Wireless Security	Click this button to access the **Wireless Security** sub-screen, and modify the security settings as required.
Allow trusted stations only	This feature can be used to prevent unknown Wireless stations from using the WAP-4050. To use this feature: • Select the checkbox. • Click the **Trusted Stations** button to open a sub-window containing the **Trusted Wireless Stations** screen, where you can enter details of the Trusted Wireless Stations. See the following section for further details. **Warning:** Ensure your own PC is in the Trusted Stations list before you enable this feature.
Copy AP/Router Mode Settings	Clicking this button will copy the Wireless settings, including the Trusted Station list, from the AP/Router mode to AP mode. • This is only useful if you already completed the configurations of AP/Router mode. • The SSID will not be copied. Each mode must use a different SSID. Using the same SSID for different modes would confuse wireless clients.

3.1.2 Wireless Security

The default setting of this option is **Disabled**. You can select desired security system from the drop-down list.

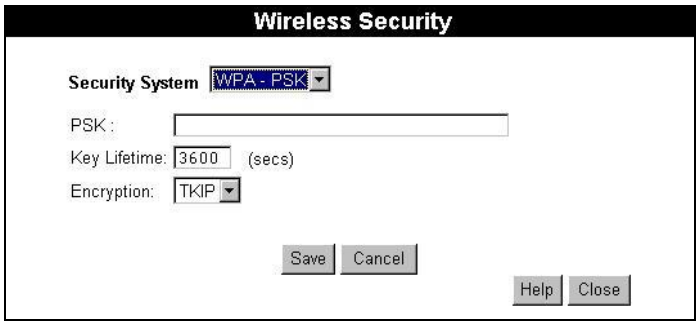


WEP Wireless Security



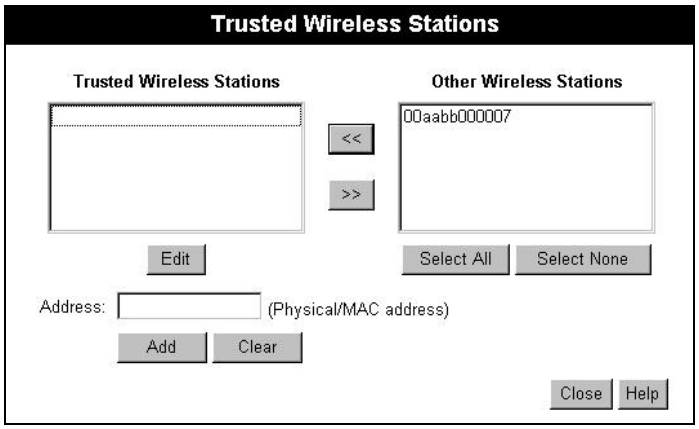
Authentication	Normally, this should be left at the default value of "Auto". Before changing to "Open System" or "Shared Key", please ensure that your Wireless Stations use the same setting.
Key Size	Select the desired option. Wireless Stations must use the same setting. • **64 Bit (10 Hex chars)** - For 64 Bit Encryption, the key size is Hex 10 chars. • **128 Bit (26 Hex chars)** - For 128 Bit Encryption, the key size is 26 Hex chars. Note: Hex chars are 0~9 and A~F.
Default Key	Select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only. You must enter a **Key Value** for the **Default Key**. Other stations must have the same key.
Passphrase	If desired, you can generate a key from a phrase, instead of entering the key value directly. Enter the desired phrase, and click the "Generate Keys" button.

WPA-PSK Wireless Security



PSK	Enter the PSK (Pre-shared Key), sometimes called the network key. Wireless clients must use the same key.
Key Lifetime	Specify a time period for WAP-4050 to renew the encryption value.
Encryption	Select the desired encryption algorithm. Currently, WAP-4050 supports TKIP only. Wireless stations must use the same setting.

3.1.3 Trusted Stations



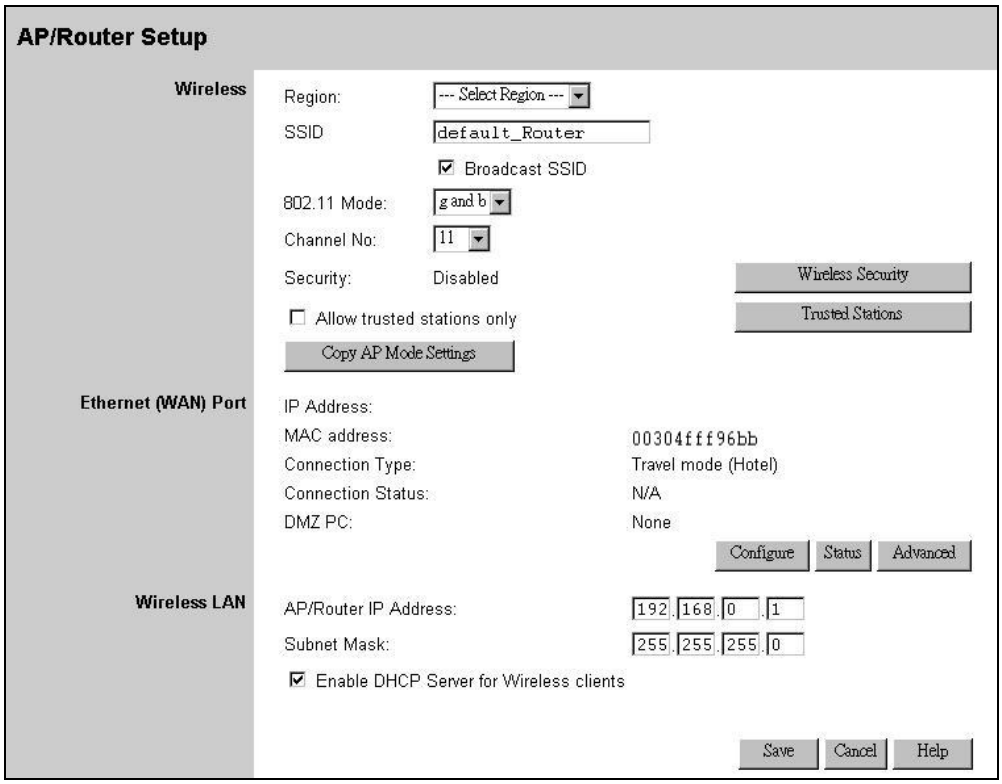
Trusted Wireless Stations	This field lists all Wireless Stations which you have designated as “Trusted”.
Other Wireless Stations	This field lists all Wireless Stations detected by theWAP-4050, which you have not designated as "Trusted".
Address	Use this field to manually add or edit a Trusted Station.
Buttons	
<<	Add a Trusted Wireless Station to the list (move from the **Other Stations** list). • Select an entry (or entries) in the **Other Stations** list. • Click the **<<** button.
>>	Delete a Trusted Wireless Station from the list (move to the **Other Stations** list). • Select an entry (or entries) in the **Trusted Stations** list. • Click the **>>** button.

Select All	Select all of the Stations listed in the **Other Stations** list.
Select None	Select none of the Stations listed in the **Other Stations** list.
Edit	To change an existing entry in the **Trusted Stations** list, select it and click this button. 1. Select the Station in the **Trusted Station** list. 2. Click the **Edit** button. The address will be copied to the **Address** field, and the **Add** button will change to **Update**. 3. Edit the address (MAC or physical address) as required. 4. Click **Update** to save your changes.
Add	To add a Trusted Station which is not in the **Other Wireless Stations** list, enter the required data and click this button.
Clear	Clear the **Address** field.

3.2 AP/Router Mode

To configure AP/Router mode, you can connect while in Config mode or in AP/Router mode. Please follow the procedures described in section 2.2 to access the Mode Configuration screen and click on the Configure button in AP/Router Mode.

3.2.1 AP/Router Setup



Wireless	
Region	Select your region from the drop-down list. This field displays the region of operation for which the wireless interface is intended. It may not be legal to operate the router in a region other than the region shown here. If your country or region is not listed, please check with your local government agency for more information on which channels you are allowed to use, and select a region that allows those channels. (The channel list changes according to the selected region.)
SSID	This field allows you to set the SSID of WAP-4050 in AP mode. The SSID is an identification string that differentiates from other WLANs. AP Mode and AP/Router mode must use different SSIDs. Using the same SSID for both modes would confuse Wireless clients. The default value is **default_Router**.
Broadcast SSID	Enable or disable a Service Set Identifier broadcast. When enabled, the SSID of the WAP-4050 is sent to wireless enabled devices on the area, thus may cause unauthorized user to connect your wireless networks.
802.11 Mode	Select the desired mode: • **g & b** - Both 802.11.g and 802.11b Wireless stations will be able to use the WAP-4050. • **g only** - Only 802.11g Wireless stations can use the WAP-4050, and obtain better performance than in g & b mix mode..
Channel No.	This selection determines which operating frequency will be used. The channel list changes according to the selected region. Select the desired channel. Adjacent Access Points should use different channels to avoid interference.
Security	The current security settings for wireless connections are displayed. The default value is Off, meaning no security.
Wireless Security	Click this button to access the **Wireless Security** sub-screen, and modify the security settings as required.

Allow trusted stations only	This feature can be used to prevent unknown Wireless stations from using the WAP-4050. To use this feature: • Select the checkbox. • Click the **Trusted Stations** button to open a sub-window containing the **Trusted Wireless Stations** screen, where you can enter details of the Trusted Wireless Stations. See the following section for further details. **Warning:** Ensure your own PC is in the Trusted Stations list before you enable this feature.
Copy AP Mode Settings	Clicking this button will copy the Wireless settings, including the Trusted Station list, from the AP mode to AP/Router mode. • This is only useful if you already completed the configurations of AP mode. • The SSID will not be copied. Each mode must use a different SSID. Using the same SSID for different modes would confuse wireless clients.
Ethernet (WAN) Port	
IP address	The current IP address for the Ethernet port. This will be blank if: • The WAP-4050 is not in AP/Router mode. • The WAP-4050 is in AP/Router mode, but there is no active connection on the Ethernet (WAN) port. **Note**: In AP/Router mode, the WAP-4050 has 2 IP addresses, one for the Wireless interface, and another for the Ethernet (WAN) port.
MAC Address	The MAC address, also called the Physical address, is a low-level identifier for Ethernet connections. This field displays the MAC address for the Ethernet (WAN) port.
Connection Type	The login method is the type of connection used on the Ethernet (WAN) port. • The default value is **Travel Mode (Hotel)**. This mode requires no additional information to be input. • To change the Login method, click the **Configure** button.
Connection Status	This indicates the current status of the connection on the Ethernet (WAN) port. This can only show **Connected** if the WAP-4050 is in AP/Router mode.

DMZ PC	The DMZ PC will receive all incoming traffic for which the correct destination PC is unknown. • This field shows the current DMZ PC. • The default value is "None", meaning the DMZ feature is disabled.
Wireless LAN	
AP/Router IP Address	The IP address of the WAP-4050 on the Wireless LAN. • The default value is 192.168.0.1 • If you wish to change any settings while in AP/Router mode, you must connect to the WAP-4050 using this IP address. • Normally, it is not necessary to change this IP address. • You MUST change this address if the LAN/WAN on the Ethernet (WAN) port is using the same IP address range (192.168.0.1 ~ 192.168.0.254). The recommended value to change to is 192.168.1.1 **Note**: In AP/Router mode, the WAP-4050 has 2 IP addresses, one for the Wireless interface, and another for the Ethernet (WAN) port.
Subnet Mask	The subnet mask for the IP address above. The default value is 255.255.255.0, which is the standard value for small networks.
Enable DHCP Server for Wireless clients	The DHCP Server will provide an IP address and related information to Wireless clients when they connect to the WAP-4050. • The default value is **Enabled.** It is strongly recommended that this feature be enabled.

3.2.2 Wireless Security

It is the same as the configurations in AP mode, please refer to section 3.1.2.

3.2.3 Trusted Stations

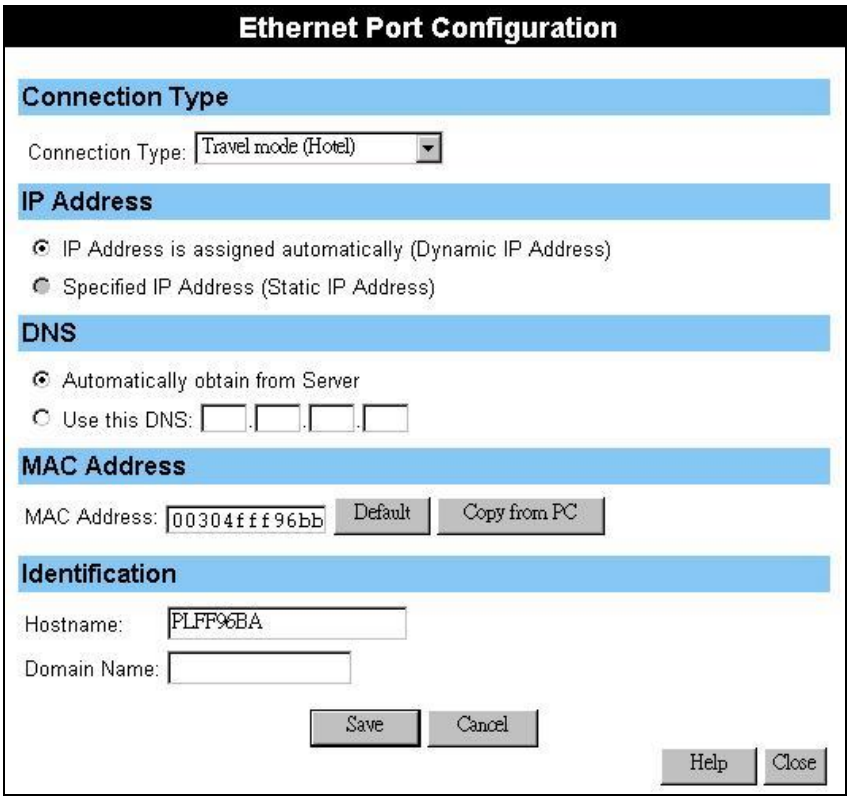
It is the same as the configurations in AP mode, please refer to section 3.1.3.

3.2.4 Ethernet (WAN) Port Configuration

This screen can be accessed by clicking the **Configure** button in **AP/Router Setup** page.

Travel Mode (Hotel)

The **Ethernet Port Configuration** is set to **Travel mo**de (Hotel) by default.



Connection Type	
Connection Type	The default setting is **Travel Mode (Hotel)** See the following section for details of the other options, and the settings associated with each option.
IP Address	
IP Address is assigned automatically	Also called Dynamic IP Address. This is the default, and the most common IP assignment method. Only change this if advised to do so by the person or organization providing the LAN/WAN port connection.
Specified IP Address	This option is not available in **Travel mode**.
DNS	
Automatically obtain from Server	The DNS (Domain Name Server) address is normally obtained automatically from the DHCP Server.
Use this DNS	If this option is selected, you must enter the IP address of the DNS (Domain Name Server) you wish to use.

MAC Address	
MAC Address	Also called *Network Adapter Address* or *Physical Address*. This is a low-level network identifier, as seen from the WAN port. Normally there is no need to change this, but if necessary, you can use the **Copy from PC** button to copy your PC's address into this field. This is only necessary if the MAC address of your PC has been recorded. You can also use the **Default** button to insert the default value, or enter a value directly. **Note:** To avoid problems regarding the MAC address, you should NOT swap the LAN/WAN connection from your PC to the WAP-4050, or from the WAP-4050 to your PC.
Identification	
Hostname	Normally, this field has no effect. If the LAN/WAN administrator asks you to use a particular Hostname, enter it here.
Domain Name	Normally, this field has no effect. If the LAN/WAN administrator asks you to use a particular Domain name, enter it here

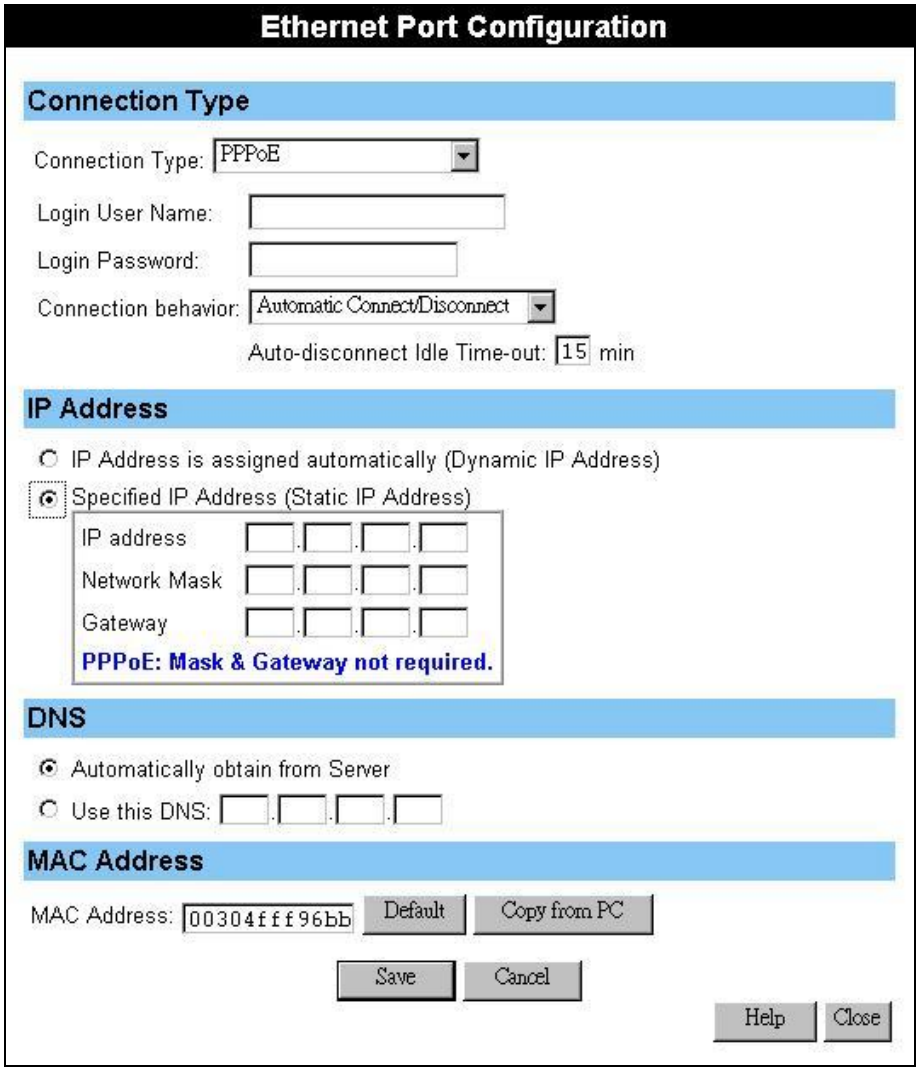
Other Connection Methods

Apart from **Travel Mode (Hotel)**, the other connection possibilities are:

- **PPPoE** - this is the most common login method for DSL modems. Normally, your ISP will provide some software to connect and login. If using the WAP-4050, this software is not required, and should not be used.
- **PPTP** - this is mainly used in Europe. You need to know the PPTP Server address as well as your name and password.
- **L2TP** - this is not widely used. You need to know the L2TP Server address as well as your name and password.
- **No Login (Static IP address)** - Use this if you have a static (fixed) IP address, and do not need to login to a server to gain access to the LAN or WAN.

To determine which method to use, you should consult with the network administrator about related information.

The following picture and table shows all available settings.


Ethernet Port Configuration
Connection Type
Connection Type: PPPoE
Login User Name:
Login Password:
Connection behavior: Automatic Connect/Disconnect
Auto-disconnect Idle Time-out: 15 min
IP Address
IP Address is assigned automatically (Dynamic IP Address)
Specified IP Address (Static IP Address)
IP address
Network Mask
Gateway
PPPoE: Mask & Gateway not required.
DNS
Automatically obtain from Server
Use this DNS:
MAC Address
MAC Address: 00304fff96bb
Default
Copy from PC
Save
Cancel
Help
Close

Connection Type	
Connection Type	The available options are: • **Travel Mode (Hotel)** - This is the default. No data needs to be input. This setting will work in many situations, not just hotels. • **PPPoE** - this is the most common login method for DSL modems. Normally, your ISP will have provided some software to connect and login. If using the WAP-4050, this software is not required, and should not be used. • **PPTP** - this is mainly used in Europe. You need to know the PPTP Server address as well as your name and password. • **L2TP** - this is not widely used. You need to know the PPTP Server address as well as your name and password. • **No Login (Static IP address) -** Use this if you have a static (fixed) IP address, and do not need to login to a server to gain access to the LAN or WAN.
Login User Name	The User Name (or account name) provided by your ISP.
Login Password	Enter the password for the login name above.
Server Address	For PPTP or L2TP, enter the Server address. For other connection methods, this address should be ignored.
Connection Behavior	Select the desired option: • **Automatic Connect/Disconnect** A connection is automatically made when required, and disconnected when idle for the time period specified by the **Auto-disconnect Idle Time-out**. • **Manual Connect/Disconnect** You must manually establish and terminate the connection. • **Keep alive (maintain connection)** The connection will never be disconnected by this device. If disconnected by the Server, the connection will be re-established immediately. (However, this does not ensure that the Ethernet (WAN) Port IP address will remain unchanged.)
Auto-disconnect Idle Time-out	This field has no effect unless using the Automatic Connect/Disconnect setting. If using this setting, enter the desired idle time-out period (in minutes). After the connection has been idle for this time period, the connection will be terminated.

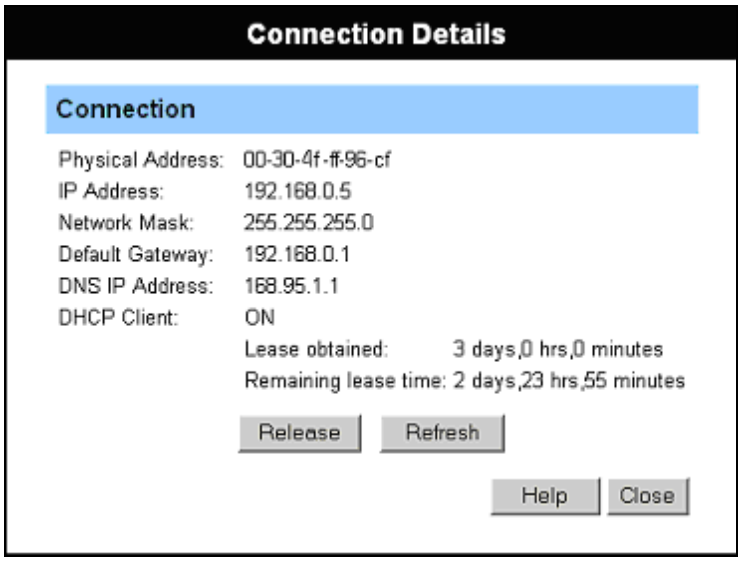
IP Address	
IP Address is assigned automatically	Also called Dynamic IP Address. This is the default, and the most common IP assignment method. Only change this if advised to do so by the person or organization providing the LAN/WAN port connection.
Specified IP Address	Also called a Static IP Address. If this option is selected, the following data must be entered. • **IP Address** - The IP address on the LAN or WAN. • **Network Mask** - The subnet mask associated with the IP address above. • **Gateway** - The IP address of the router or gateway on the LAN or WAN you are connecting to. **Note**: If using PPPoE, the Network Mask and Gateway are not required; just enter the IP address.
DNS	
Automatically obtain from Serve	The DNS (Domain Name Server) address is normally obtained automatically from the DHCP Server. Note that if using a fixed IP address, this option cannot be used.
Use this DNS	If this option is selected, you must enter the IP address of the DNS (Domain Name Server) you wish to use. If using a Static IP address, you must select this option.
MAC Address	
MAC Address	Also called *Network Adapter Address* or *Physical Address*. This is a low-level network identifier, as seen from the WAN port. Normally there is no need to change this, but if necessary, you can use the **Copy from PC** button to copy your PC's address into this field. This is only necessary if the MAC address of your PC has been recorded. You can also use the **Default** button to insert the default value, or enter a value directly. **Note:** To avoid problems regarding the MAC address, you should NOT swap the LAN/WAN connection from your PC to the WAP-4050, or from the WAP-4050 to your PC.

3.2.5 Ethernet (WAN) Port Status

This screen is accessible only when you log in the WAP-4050 in active AP/Router mode (Mode Selector is in position 2). You can have the connection status by clicking the **Status** button, and the information displayed is depending on the current connection method.

Fixed/Dynamic IP Address

If your access method is **Travel Mode** or **No Login**, a screen like the following example will be displayed when the **Status** button is clicked.



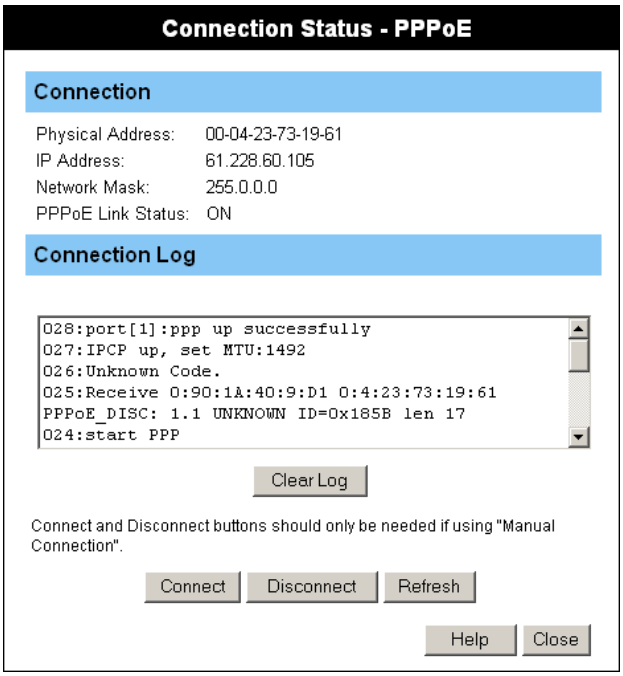
Internet	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen from the Ethernet (WAN) Port interface. If using DHCP, and there is no current connection, this will be blank or 0.0.0.0.
Network Mask	The Network Mask associated with the IP Address above.
Default Gateway	The IP Address of the remote Gateway or Router associated with the IP Address above.
DNS IP Address	The IP Address of the Domain Name Server which is currently used.
DHCP Client	This indicates whether or not this device is functioning as a DHCP client. • If acting as a DHCP client, the IP address above has been allocated by the DHCP Server on the LAN or WAN. • If not a DHCP client, the IP address (if shown) is fixed or static. • If using DHCP, the Lease Obtained and Remaining lease time fields indicates when the IP Address allocated by the DHCP Server was obtained and when it will expire. The lease is automatically renewed on expiry.

Buttons	
Release (Renew)	This button is only useful if the IP address shown above is allocated automatically on connection (Dynamic IP address). If you have a Fixed (Static) IP address, this button has no effect. • If the ISP's DHCP Server has NOT allocated an IP Address for the WAP-4050, this button will say "Renew". Clicking the "Renew" button will attempt to re-establish the connection and obtain an IP Address from the ISP's DHCP Server. • If an IP Address has been allocated to the WAP-4050 (by the ISP's DHCP Server), this button will say "Release". Clicking the "Release" button will break the connection and release the IP Address.
Refresh	Update the data shown on screen.

PPPoE

If your access method is **Travel Mode** or **No Login**, a screen like the following example will be displayed when the **Status** button is clicked.

If using PPPoE (PPP over Ethernet), a screen like the following example will be displayed when the Status button is clicked.



Connection	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen from the Ethernet (WAN)

	Port interface. If using DHCP, and there is no current connection, this will be blank or 0.0.0.0.
Network Mask	The Network Mask associated with the IP Address above.
PPPoE Link Status	This indicates whether or not the connection is currently established. • If the connection does not exist, the **Connect** button can be used to establish a connection. • If the connection currently exists, the **Disconnect** button can be used to break the connection.
Connection Log	
Connection Log	• The Connection Log shows status messages relating to the existing connection. • The most common messages are listed in the table below. • The **Clear Log** button will restart the Log, while the **Refresh** button will update the messages shown on screen.
Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

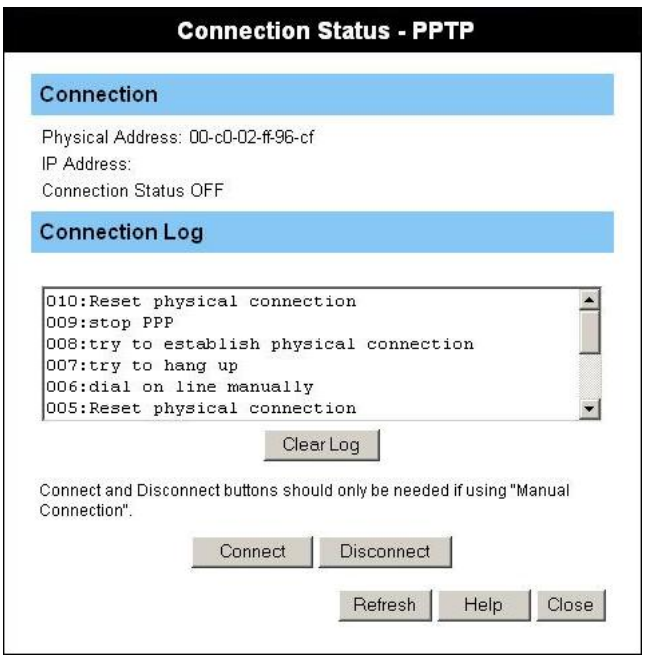
CONNECTION LOG MESSAGES

Message	Description
Connect on Demand	Connection attempt has been triggered by the "Connect automatically, as required" setting.
Manual connection	Connection attempt started by the "Connect" button.
Reset physical connection	Preparing line for connection attempt.
Connecting to remote server	Attempting to connect to the ISP's server.
Remote Server located	ISP's Server has responded to connection attempt.
Start PPP	Attempting to login to ISP's Server and establish a PPP connection.
PPP up successfully	Able to login to ISP's Server and establish a PPP connection.

Idle time-out reached	The connection has been idle for the time period specified in the "Idle Time-out" field. The connection will now be terminated.
Disconnecting	The current connection is being terminated, due to either the "Idle Time-out" above, or "Disconnect" button being clicked.
Error: Remote Server not found	ISP's Server did not respond. This could be a Server problem, or a problem with the link to the Server.
Error: PPP Connection failed	Unable to establish a PPP connection with the ISP's Server. This could be a login problem (name or password) or a Server problem.
Error: Connection to Server lost	The existing connection has been lost. This could be caused by a power failure, a link failure, or Server failure.
Error: Invalid or unknown packet type	The data received from the ISP's Server could not be processed. This could be caused by data corruption (from a bad link), or the Server using a protocol which is not supported by this device.

PPTP

If using **PPTP** (Peer-to-Peer Tunneling Protocol), a screen like the following example will be displayed when the **Status** button is clicked.

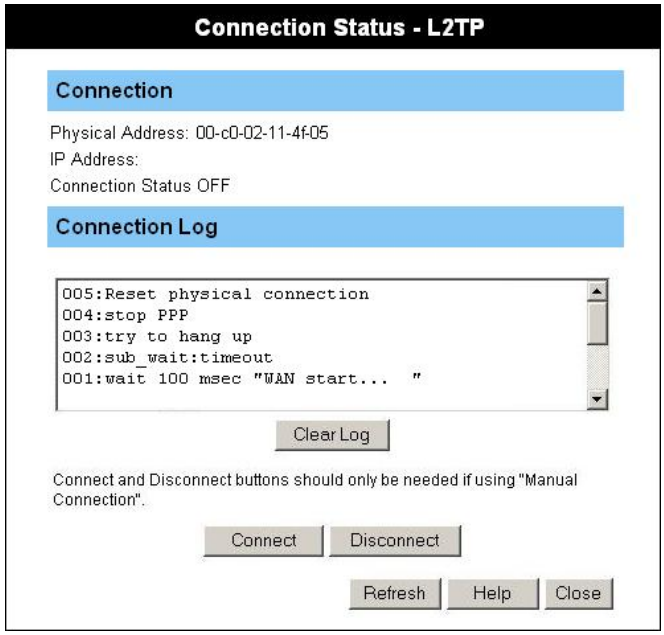


Connection	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)

IP Address	The IP Address of this device, as seen from the Ethernet (WAN) Port interface. If using DHCP, and there is no current connection, this will be blank or 0.0.0.0.
PPTP Status	This indicates whether or not the connection is currently established. • If the connection does not exist, the **Connect** button can be used to establish a connection. • If the connection currently exists, the **Disconnect** button can be used to break the connection.
Connection Log	
Connection Log	• The Connection Log shows status messages relating to the existing connection. • The **Clear Log** button will restart the Log, while the **Refresh** button will update the messages shown on screen.
Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

L2TP

If using **L2TP**, a screen like the following example will be displayed when the **Status** button is clicked.



Connection	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen from the Ethernet (WAN) Port interface. If using DHCP, and there is no current connection, this will be blank or 0.0.0.0.
Connection Status	This indicates whether or not the connection is currently established. • If the connection does not exist, the **Connect** button can be used to establish a connection. • If the connection currently exists, the **Disconnect** button can be used to break the connection.
Connection Log	
Connection Log	• The Connection Log shows status messages relating to the existing connection. • The **Clear Log** button will restart the Log, while the **Refresh** button will update the messages shown on screen.
Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read

	new messages.
Refresh	Update the data on screen.

3.3 AP/Router Mode - Advanced

The following advanced features are provided in AP/Router mode.

- Advanced Internet
  - Communication Applications
  - DMZ
- Port Forwarding
- Dynamic DNS
- Network Diagnostics
- Option
- PC Database
- Security

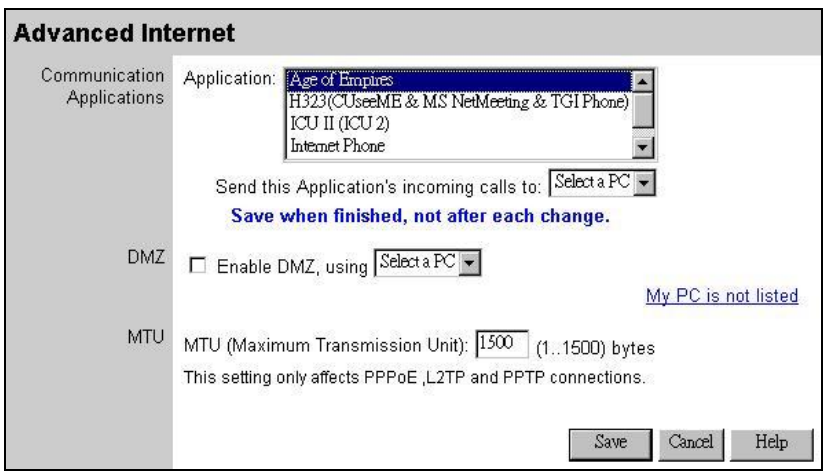
These features are accessed via the **Advanced** button on the **AP/Router Setup** screen.

3.3.1 Advanced Internet

This screen allows configuration of all advanced features relating to Internet access.

- Communication Applications
- DMZ
- MTU (Maximum Transmission Unit)

An example screen is shown below.



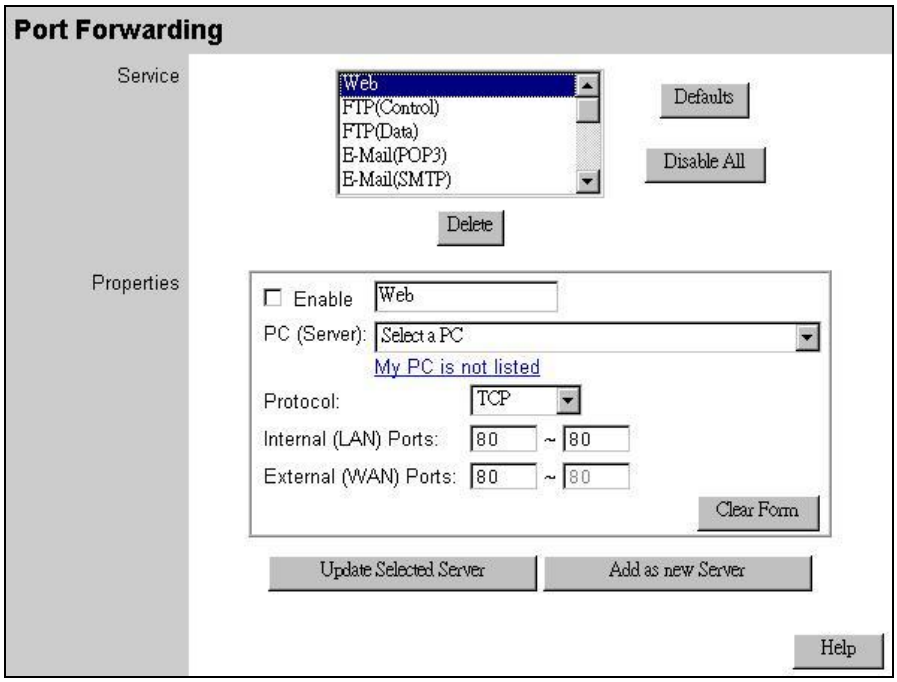
Communication Applications	
Application	This box lists applications which may generate incoming connections, where the destination PC (on your local LAN) is unknown. For each application, you can select the PC to which incoming connections may be sent.

Send this Application's incoming calls to	This field lists the PCs on your wireless LAN. • For each application listed above, you can choose a destination PC. • If necessary, you can add PCs manually, using the **PC Database** menu option. • There is no need to aave after each change; you can set the destination PC for each application, and then click **Save**.
DMZ	
Enable DMZ…	Use this to enable the DMZ feature as required. • The DMZ PC will receive all "Unknown" connections and data. This feature is normally used with applications which do not usually work when behind a Firewall. • The DMZ PC is effectively outside the Firewall, making it more vulnerable to attacks. For this reason, you should only enable the DMZ feature when required. • If Enabled, you must select the PC to be used as the DMZ PC.
DMZ PC	If the DMZ feature is enabled, you must select a PC. If the PC uses a fixed IP address, and is not in the list, you can add it using the "PC Database" menu option.
MTU	
MTU size	MTU (Maximum Transmission Unit) determines the size of network packets. This value should only be changed if advised to do so by technical person. • Enter a value between 1 and 1500. • This device will still auto-negotiate with the remote server, to set the MTU size. The smaller of the 2 values (auto-negotiated, or entered here) will be used. • For direct connections (not PPPoE or PPTP), the MTU used is always 1500.

3.3.2 Port Forwarding

This feature, sometimes called Virtual Servers, allows you to make Servers on your LAN accessible to Internet users.

An example screen is shown below.



Service	
Service	This field lists a number of pre-defined Services, plus any Services defined by yourself. Details of the selected Service are shown in the **Properties** area.
Properties	
Enable	Enable/Disable Port Forwarding for this Service, as required.
PC (Server)	Select the PC to be used as the Server for this Service. The PC must be running the appropriate Server software.
Protocol	Select the protocol (TCP, UDP or TCP/UDP) used by the Service.
Internal Ports	Enter the range of port numbers which the Server software is configured to use.
External Ports	Traffic from the Internet using this range of port numbers will be sent to the selected Server. These ports are normally the same as the Internal Port Numbers. If they are different, this device will perform a "mapping" or "translation" function, allowing the server to use a different port range to the clients. Using this feature allows the server to distinguish traffic from the WAN or from the LAN by using the port number, rather than having to check IP addresses.
Buttons	
Defaults	This will delete any Servers you have defined, and set the pre-defined Servers to use the default port numbers.
Disable All	This will cause the "Enable" setting of all entries to be set OFF.

Update Selected Server	Update the current entry, using the data shown in the **Properties** area on screen.
Add as new Server	Add a new entry to the list, using the data shown in the **Properties** area on screen. The entry selected in the list is ignored, and has no effect.
Delete	Delete the current Server entry. Note that the pre-defined Servers cannot be deleted. Only Servers you have defined yourself can be deleted.
Clear Form	Clear all data from the **Properties** area, ready for input of a new entry.

Defining your own Servers

If the type of Server you wish to use is not listed on the **Port Forwarding** screen, you can define and manage your own Servers:

Create a new Server:

1. Click **Clear Form**.
2. Enter the required data, as described above.
3. Click **Add**.
4. The new Server will now appear in the list.

Modify (Edit) a Server:

1. Select the desired Server from the list
2. Make any desired changes (for example, change the Enable/Disable setting).
3. Click **Update** to save changes to the selected Server.

Delete a Server:

1. Select the entry from the list.
2. Click **Delete**.

Note: You can only delete Servers you have defined. Pre-defined Server cannot be deleted.

Connecting to your Servers

Once configured, anyone on the WAN or Internet can connect to your Servers. They must use the WAN (Internet) IP Address of WAP-4050:

e.g.

http://203.70.212.52

ftp://203.70.212.52

It is more convenient if you are using a Fixed IP Address, rather than Dynamic. However, you can use the **Dynamic DNS** feature, described in the following section, to allow users to connect to your **Port Forwarding** using a URL, rather than an IP Address.

3.3.3 DDNS

This free service is very useful when combined with the **Port Forwarding** feature. It allows Internet users to connect to your servers using a URL, rather than an IP Address.

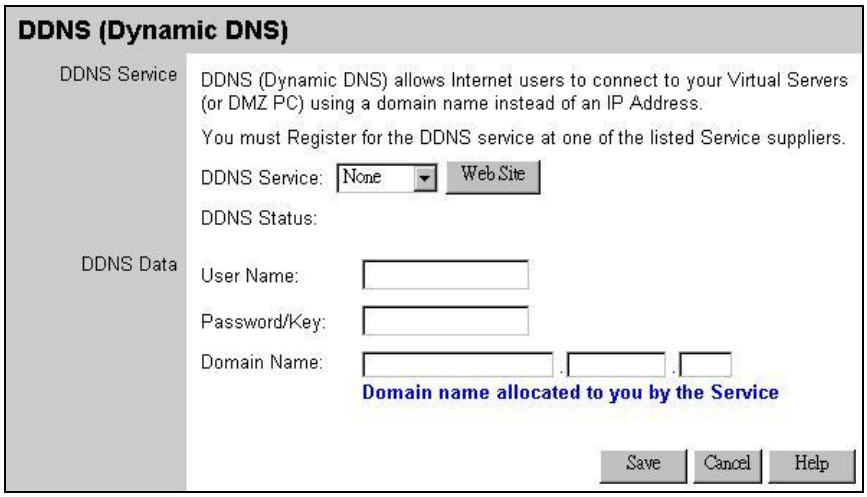
This also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change whenever you connect, which makes it difficult to connect to you.

The Service works as follows:

1. You must register for the service at one of the listed DDNS Service Providers.
2. After registration, follow the service provider's procedure to request a Domain Name and have it allocated to you.
3. Enter your DDNS data on the WAP-4050's DDNS screen.
4. The WAP-4050 will then automatically ensure that your current IP Address is recorded at the DDNS server.

   If the DDNS Service provides software to perform this "IP address update"; you should disable the "Update" function, or not use the software at all.
5. From the Internet, users will be able to connect to your servers (or DMZ PC) using your Domain Name.

An example screen is shown below.



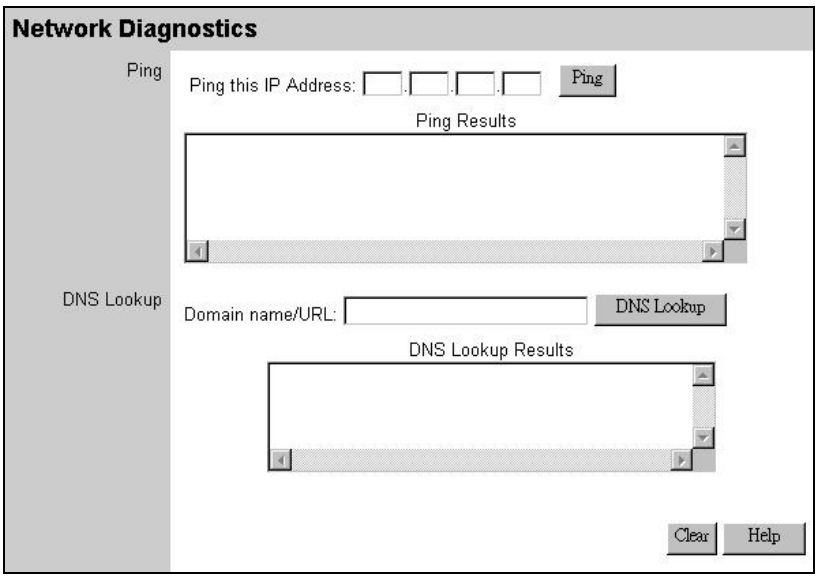
DDNS Service	
DDNS Service	Select the desired DDNS Service Provider from the list. You must register for the service at one of the listed Service Providers.
Web Site Button	Click this button to open another browser window and connect to the Web site of the selected DDNS service provider.
DDNS Status	• This message is returned by the DDNS Server • Normally, this message should be **Update successful.** • If the message is **No host** or some other error message, you need to connect to the DDNS Service provider and correct the problem.
DDNS Data	
User Name	Enter your Username for the DDNS Service.

Password/Key	Enter your current password for the DDNS Service.
Domain Name	Enter the domain name allocated to you by the DDNS Service. If you have more than one name, enter the name you wish to use.

3.3.4 Network Diag

This screen allows you to perform a "Ping" or a "DNS lookup". These activities can be useful in solving network problems. Please note this function is only available while in **AP/Router** mode (Mode Selector is in position 2).

An example **Network Diagnostics** screen is shown below.

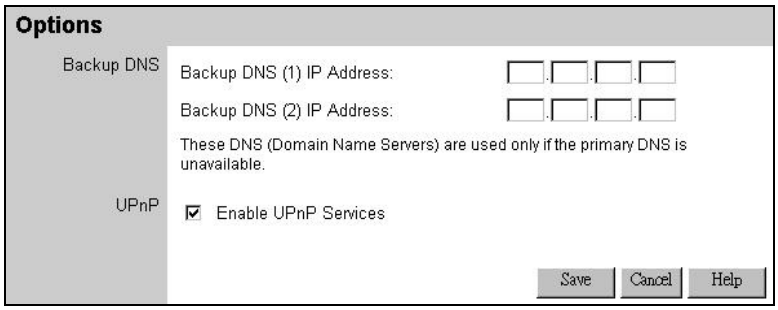


Ping	
Ping this IP Address	Enter the IP address you wish to ping. The IP address can be on your LAN, or on the Internet. Note that if the address is on the Internet, and no connection currently exists, you could get a **Timeout** error. In that case, wait a few seconds and try again.
Ping Button	After entering the IP address, click this button to start the "Ping" procedure. The results will be displayed in the **Ping Results** pane.
DNS Lookup	
Domain name/URL	Enter the Domain name or URL for which you want a DNS (Domain Name Server) lookup. Note that if the address in on the Internet, and no connection currently exists, you could get a **Timeout** error. In that case, wait a few seconds and try again.
DNS Lookup Button	After entering the Domain name/URL, click this button to start the "DNS Lookup" procedure. The results will be displayed in the **DNS Lookup Results** pane.

3.3.5 Options

This screen allows advanced users to enter or change a number of settings. For normal operation, there is no need to use this screen or change any settings.

An example **Options** screen is shown below.



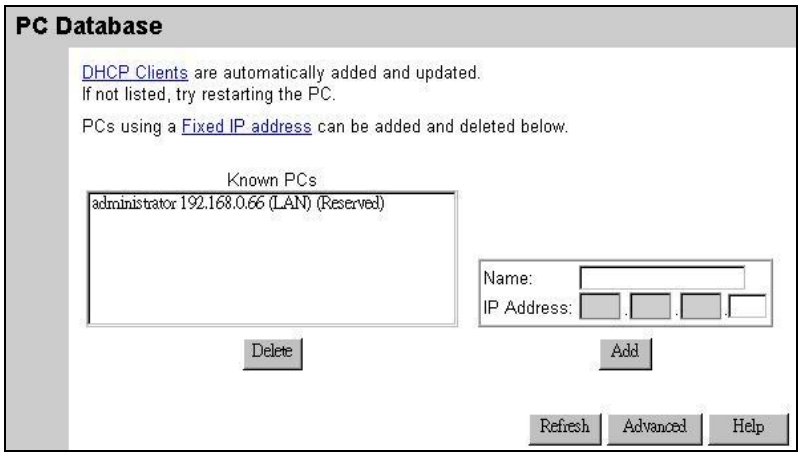
Backup DNS	
IP Address	Enter the IP Address of the DNS (Domain Name Servers) here. These DNS will be used only if the primary DNS is unavailable.
UPnP	
Enable UPnP Services	• UPnP (Universal Plug and Play) allows automatic discovery and configuration of equipment attached to your LAN. UPnP is by supported by Windows ME, XP, or later. • If Enabled, this device will be visible via UPnP. • If Disabled, this device will not be visible via UPnP.

3.3.6 PC Database

The PC Database is used whenever you need to select a PC (e.g. for the "DMZ" PC). PCs which are "DHCP Clients" are automatically added to the database, and updated as required. The WAP-4050 uses the "Hardware Address" to identify each PC, not the name or IP address. The "Hardware Address" can only change if you change the PC's network card or adapter.

This system means you do NOT need to use Fixed (static) IP addresses on your LAN. However, you can add PCs using Fixed (static) IP Addresses to the PC database if required.

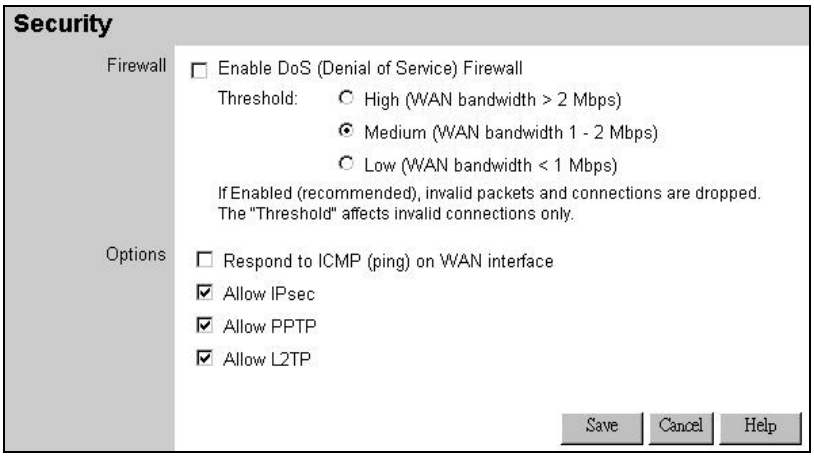
An example **PC Database** screen is shown below.



Known PCs	This field lists all current entries. Data displayed is **name (IP Address) type**. The **type** indicates whether the PC is connected to the LAN.
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's hostname.
IP Address	Enter the IP Address of the PC. The PC will be sent a "ping" to determine its hardware address. If the PC is not available (not connected, or not powered On) you will not be able to add it.
Buttons	
Add	This will add the new PC to the list. The PC will be sent a "ping" to determine its hardware address. If the PC is not available (not connected, or not powered On) you will not be able to add it.
Delete	Delete the selected PC from the list. This should be done in 2 situations: • The PC has been removed from your LAN. • The entry is incorrect.
Refresh	Update the data on screen.
Advanced	View the Advanced version of the PC database screen, which provides some additional options. See below for details.

3.3.7 Security

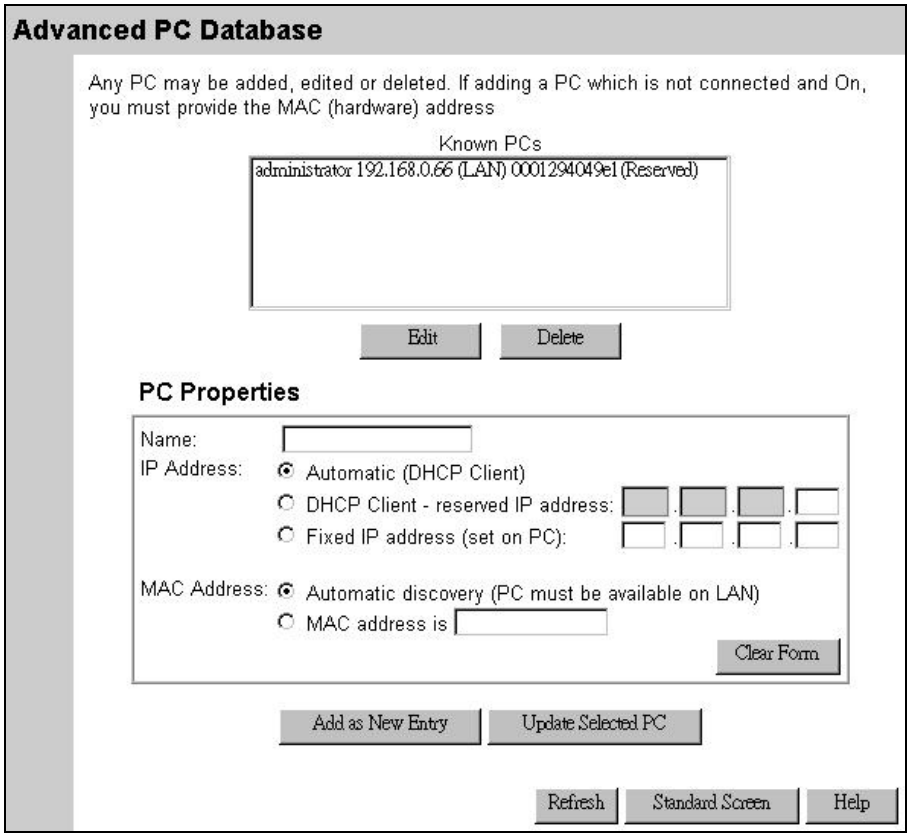
This screen allows you to set Firewall and other security-related options.



Firewall	
Enable DoS Firewall	If enabled, DoS (Denial of Service) attacks will be detected and blocked. The default is enabled. It is strongly recommended that this setting be left enabled. **Note:** • A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you cannot use it - the service is unavailable. • This device uses Stateful Inspection technology. This system can detect situations where individual TCP/IP packets are valid, but collectively they become a DoS attack.
Threshold	This setting affects the number of "half-open" connections allowed. • A "half-open" connection arises when a remote client contacts the Server with a connection request, but then does not reply to the Server's response. • While the optimum number of "half-open" connections allowed (the **Threshold**) depends on many factors, the most important factor is the available bandwidth of your Internet connection. • Select the setting to match the bandwidth of your Internet connection.

Options	
Respond to ICMP	The ICMP protocol is used by the "ping" and "traceroute" programs, and by network monitoring and diagnostic programs. • If checked, the WAP-4050 will respond to ICMP packets received via the WAN port. • If not checked, ICMP packets from the WAN port will be ignored. Disabling this option provides a slight increase in security.
Allow IPsec	The IPSec protocol is used to establish a secure connection, and is widely used by VPN (Virtual Private Networking) programs. • If checked, IPSec connections from the Wireless LAN are allowed. • If not checked, IPSec connections are blocked.
Allow PPTP	PPTP (Point to Point Tunneling Protocol) is widely used by VPN (Virtual Private Networking) programs. • If checked, PPTP connections from the Wireless LAN are allowed. • If not checked, PPTP connections are blocked.
Allow L2TP	L2TP is a protocol developed by Cisco for VPNs (Virtual Private Networks). • If checked, L2TP connections from the Wireless LAN are allowed. • If not checked, L2TP connections are blocked.

Advanced PC Database



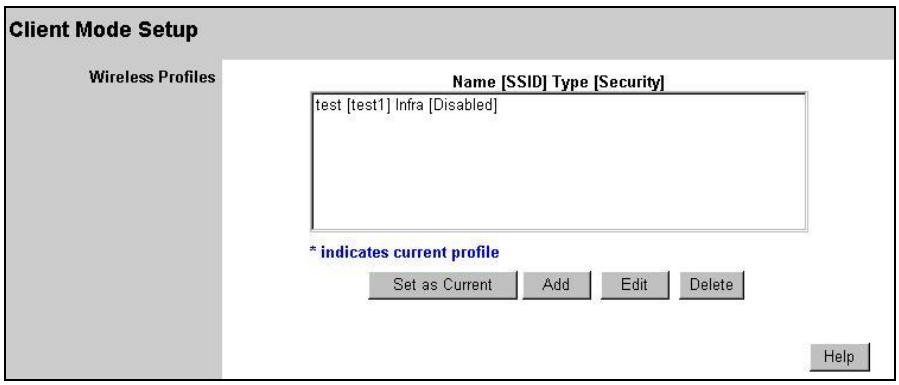
Known PCs	This field lists all current entries. Data displayed is **name (IP Address) type**. The **type** indicates whether the PC is connected to the LAN.
Edit	Use this to change the data for the selected PC in the list. The data for the selected PC will then be shown in the **Properties** area, where it may be edited. (Click **Update** to save any changes.)
Delete	Use this to Delete the selected PC from the list. This should be done in 2 situations: • The PC has been removed from your LAN. • The entry is incorrect.
PC Properties	
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's hostname.

IP Address	Select the appropriate option: • **Automatic** - The PC is set to be a DHCP client (Windows: "Obtain an IP address automatically"). The WAP-4050 will allocate an IP address to this PC when requested to do so. The IP address could change, but normally won't. • **DCHP Client - Reserved IP Address** - Select this if the PC is set to be a DCHP client, and you wish to guarantee that the WAP-4050 will always allocate the same IP Address to this PC. Enter the required IP address. Only the last field is required; the other fields must match the WAP-4050's IP address. • **Fixed IP Address** - Select this if the PC is using a Fixed (Static) IP address. Enter the IP address allocated to the PC. (The PC must be configured to use this IP address.)
MAC Address	Select the appropriate option • **Automatic discovery** - Select this to have the WAP-4050 contact the PC and find its MAC address. This is only possible if the PC is connected to the LAN and powered on. • **MAC address is** - Enter the MAC address on the PC. The MAC address is also called the "Hardware Address", "Physical Address", or "Network Adapter Address". The WAP-4050 uses this to provide a unique identifier for each PC. Because of this, the MAC address CANNOT be left blank.
Buttons	
Add as New Entry	Add a new PC to the list, using the data in the **Properties** box. If **Automatic discovery** (for MAC address) is selected, the PC will be sent a "ping" to determine its hardware address. This will fail unless the PC is connected to the LAN, and powered on.
Update Selected PC	Update (modify) the selected PC, using the data in the **Properties** box.
Clear Form	Clear the **Properties** box, ready for entering data for a new PC.
Refresh	Update the data on screen.
Standard Screen	Click this to view the standard **PC Database** screen.

3.4 Client Mode

You CANNOT connect to the WAP-4050 wirelessly while it is in **Client** mode. Configuration for **Client**

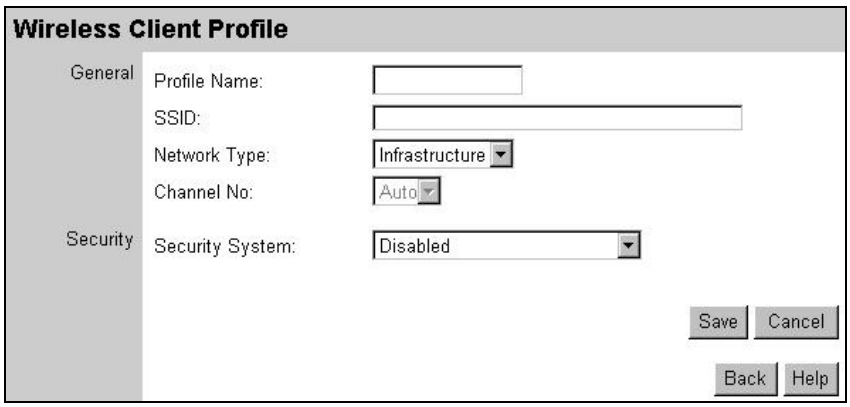
mode must be performed while in **Config** Mode. Please follow the procedures described in section 2.2 to access the **Mode Configuration** screen and click on the **Configure** button in **Client Mode**.



Wireless Profiles	All available profiles are listed. For each profile, the following data is displayed: • ***** If a * is displayed before the name of the profile, this indicates the profile is the current profile (it is enabled). • *Profile Name* The current profile name is displayed. • **[SSID]** The current SSID associated with this profile. • **Type** The network type - Auto, Ad Hoc, or Infrastructure. • **Security** The current security system (e.g. WEP) is displayed.
Buttons	• **Set as Current -** Make the selected profile the current profile. The selected profile will be enabled, and all other profiles will be disabled. • **Add -** Create a new Profile. • **Edit -** Change the settings for the selected profile. • **Delete -** Delete the selected profile.

Wireless Client Profile

This screen is displayed when the **Add** or **Edit** button on the **Client Mode Setup** screen is clicked.



General	
Profile Name	Enter a suitable name for this profile. Each profile must have a unique name.
SSID	Enter the SSID of the wireless network you wish to join. • In **Infrastructure** mode, this may be left blank; this device will then join any wireless network it can. This is only possible if the Access Point is broadcasting its SSID, and the security settings for this profile match the security settings on the Access Point. • If more than one Access Point is available with this profile, the one with the strongest signal will be used.
Network Type	Select the desired option: • **Ad Hoc** - only an Ad Hoc network will be used; Infrastructure networks will be ignored. • **Infrastructure** - only an Infrastructure network will be used; Ad hoc networks will be ignored.
Channel No.	This field determines which operating frequency will be used. • If the network type is **Infrastructure**, only the **Auto** channel selection is available, because this station must use the Channel used by the Wireless network it is joining. • For **Ad-hoc** mode, you can set the Channel to use. But to join an existing Wireless network, this station must adopt the Channel already in use, so this setting is only meaningful when creating a new Wireless network.

Security	
Security	Select the desired option, and then enter the settings for the selected method: • **Disabled** - No security is used. Data is not encrypted before transmission. • **WEP** The 802.11b standard. Data is encrypted before transmission. You have 2 options: • WEP 64 Bit - this uses 64-bit encryption. You must enter the WEP key (10 Hex characters). • WEP 128 Bit - this uses 128-bit encryption. You must enter the WEP key (26 Hex characters). • **WPA-PSK** Like WEP, data is encrypted before transmission. WPA-PSK is a later standard than WEP, and provides better security. If all your Wireless stations support WPA-PSK, you should use this rather than WEP. **Note:** WPA-PSK is only available in Infrastructure mode.
WEP	
WEP Key	• Enter the key value you wish to use. Other stations must have the same key value. • In **Infrastructure** mode, this key must match the **Default Key** value on the Access Point. • Keys must be entered in Hex. Hex characters are the digits (0 ~ 9) and the letters A ~ F.
Passphrase	Use this to generate a Hex key from an ASCII string. Enter a word or group of printable (ASCII) characters in the **Passphrase** box and click the **Generate** button to generate the WEP Key.
WEP Key Index	This is only useful in **Infrastructure** mode. It is possible for an Access Point to have more than one (1) key, but only one can be the **default key**. This index must be set to match the **default key** index on the Access Point. Normally, this is one (1).
WEP Authentication	This must match the authentication method used on the Access Point.

WPA - PSK	
PSK	Enter the PSK (Pre-shared Key), sometimes the network key, used on the Access Point.
WPA Encryption	This must match the Encryption method used on the Access Point.

Chapter 4 Troubleshooting

This chapter covers some common problems that may be encountered while using the WAP-4050 and some possible solutions to them.

Problem 1: **Can't connect to the WAP-4050 to configure it.**

Solution 1: Try using the wired Ethernet connection and the WAP-4050's IP address.

3. Connect a LAN cable from the WAP-4050 to the Ethernet port on your PC.
4. Set the WAP-4050 to "Config" mode.
5. Restart the WAP-4050.
6. Restart your PC. (Or, if you know how to do so, you could perform a **Release** and **Renew** of the IP address on the Ethernet port.)
7. Start your Web browser.
8. Enter the Address as: HTTP://192.168.0.1

Problem 2: **My PC can't locate the Wireless Access Point.**

Solution 2:

- Check the **Broadcast SSID** setting. Has it been disabled? If it has, the AP will not be listed in **Available Wireless Networks**, and you will have to configure your PC manually. If using manual configuration, ensure the mode is **Infrastructure** and not Ad-hoc.
- To see if radio interference is causing a problem, see if connection is possible when close to the WAP-4050.
  Remember that the connection range can be as little as 50 feet in poor environments.

Problem 3: **On my PC, I can locate the WAP-4050, but I can't establish a connection.**

Solution 3:

- The SSID on your PC and the Wireless Access Point must be the same. Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup".
- Both your PC and the WAP-4050 must have the same settings for Wireless security. The default setting for the WAP-4050 is disabled, so your wireless station should also have Wireless security disabled.
  If Wireless security is enabled on the WAP-4050, Wireless stations must use the same settings as the WAP-4050.
- If the WAP-4050 is set to **Allow Trusted Stations only**, then each of your Wireless stations must be in the **Trusted Wireless Stations** list, or access will be blocked.

Problem 4: **Wireless connection speed is very slow.**

Solution 4: The wireless system will connect at the highest possible speed, depending on the

distance and the environment. To obtain the highest possible connection speed, you can experiment with the following:

- WAP-4050 location.
  Try adjusting the location and orientation of the WAP-4050.
- Wireless Channel
  If interference is the problem, changing to another channel may show a marked improvement.
- Radio Interference
  Other devices may be causing interference. You can experiment by switching other devices Off, and see if this helps. Any "noisy" devices should be shielded or relocated.
- RF Shielding
  Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the WAP-4050.

Problem 5: **When I enter a URL or IP address I get a time out error.**

Solution 5: A number of things could be causing this. Try the following troubleshooting steps.

- Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address.
- If the PCs are configured correctly, but still not working, check the WAP-4050. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.)
- If the WAP-4050 is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.

Problem 6: **Some applications do not run properly when using the WAP-4050.**

Solution 6: The WAP-4050 processes the data passing through it, so it is not transparent.
Use the **Special Applications** feature to allow the use of Internet applications which do not function correctly.
If this does solve the problem you can use the **DMZ** function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.
- Only one (1) PC can use this feature.