3-in-1
IP802SM V2

802.11g Wireless Access Point

Broadband Router

802.11g Wireless Client

Quick Start Guide

Regulatory Approvals

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

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

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

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.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

Channel

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channel are available. If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference.
- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)
- If using "Ad-hoc" mode (no Access Point), all Wireless stations should be set to use the same Channel. However, most Wireless stations will still scan all Channels to see if there is an existing "Ad-hoc" group they can join.

CAUTION:

1) To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

2) This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Table of Contents

P/N: 9560P60001

Document Version: 1.4 (July, 2004)

Chapter 1
Introduction

This Chapter provides an overview of the Wireless 3-in-1 Companion's features and capabilities.

Congratulations on the purchase of your new Wireless 3-in-1 Companion. The Wireless 3-in-1 Companion can function in any of 3 modes:

- ***Wireless Access Point*** for 802.11b and 802.11g Wireless Stations.
- ***AP/Router*** providing Broadband LAN/WAN Access for all wireless stations.
- ***Client Mode*** converting your PC Ethernet port to a wireless interface.

There is also a **Config Mode** to make it easy to connect to the Wireless 3-in-1 Companion and change its configuration.

Features

The Wireless 3-in-1 Companion incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

General

- ***Compact Size.*** Both the Wireless 3-in-1 Companion and its power supply are small and light, making it easy to move from one location to another as required.
- ***Easy Setup.*** Use your WEB browser for configuration. In **Config Mode**, you don't even have to know the IP address of the Wireless 3-in-1 Companion.
- ***Configuration File Upload/Download.*** You can Save (download) the configuration data from the Wireless 3-in-1 Companion to your PC, and restore (upload) a previously-saved configuration file to the Wireless 3-in-1 Companion.
  If used in many different environments , this make it easy to change the configuration to match the current environment.

Wireless

- ***Standards Compliant.*** The Wireless 3-in-1 Companion complies with the IEEE802.11g (DSSS) specifications for Wireless LANs.
- ***Supports both 802.11b and 802.11g Wireless Stations.*** The 802.11g standard provides for backward compatibility with the 802.11b standard, so both 802.11b and 802.11g Wireless stations can be used simultaneously.
- ***Speeds to 54Mbps.*** All speeds up to the 802.11g maximum of 54Mbps are supported.
- ***WEP support.*** Support for WEP (Wired Equivalent Privacy) is included. Key sizes of 64 Bit and 128 Bit are supported.
- ***WPA-PSK support.*** The WPA-PSK standard for data encryption is supported. This standard provides better encryption ;than WEP.
- ***Wireless MAC Access Control.*** The Wireless Access Control feature can check the MAC address (hardware address) of Wireless stations to ensure that only trusted Wireless Stations can access your LAN.

- ***Simple Configuration.*** If the default settings are unsuitable, they can be changed quickly and easily.

Router Mode Features

- ***DHCP Server Support.*** **D**ynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The Wireless 3-in-1 Companion can act as a **DHCP Server** for PCs using the Access Point.
- ***Shared LAN/WAN Access.*** All users on the Wireless LAN can share the IP Address on the Wireless 3-in-1 Companion's Ethernet port, providing shared access to the LAN or WAN. This process is called NAT (Network Address Translation).
- ***Fixed or Dynamic IP Address.*** On the Ethernet (WAN) port connection, the Wireless 3-in-1 Companion supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.
- ***PPPoE, PPTP Support.*** On the Ethernet (WAN) port connection supports PPPoE (PPP over Ethernet) and PPTP (Peer-to-Peer Tunneling Protocol) login methods if required.
- ***Communication Applications.*** Support for Internet communication applications, such as interactive Games, Telephony, and Conferencing applications, which are often difficult to use when behind a Firewall, is included.
- ***Port Forwarding.*** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- ***DDNS Support.*** DDNS (Dynamic DNS) allows Internet users to connect to Port Forwarding on your LAN using a domain name, even if your IP address is not fixed.
- ***DMZ.*** One (1) PC on your local LAN can be configured to allow unrestricted 2-way communication with Servers or individual users on the Internet. This provides the ability to run programs which are incompatible with Firewalls.
- ***VPN Pass through Support.*** PCs with VPN (Virtual Private Networking) software using PPTP, L2TP and IPSec are transparently supported - no configuration is required.
- ***Network Diagnostics.*** You can use the Wireless 3-in-1 Companion to perform a *Ping* or *DNS lookup*.
- ***Stateful Inspection Firewall.*** All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources.
- ***Protection against DoS attacks.*** DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The Wireless 3-in-1 Companion incorporates protection against DoS attacks.

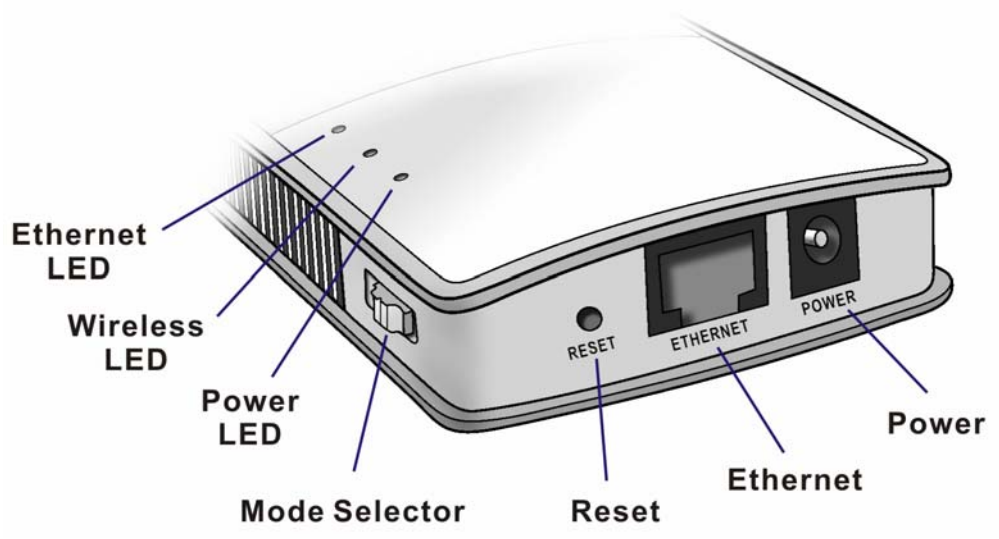
Package Contents

The following items should be included:

- The Wireless 3-in-1 Companion Unit
- Power Adapter
- Quick Start Guide
- CD-ROM containing the on-line manual.

If any of the above items are damaged or missing, please contact your dealer immediately.

Physical Features



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.
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 Wireless 3-in-1 Companion.
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 connected to your PC. • In **Client mode**, this is connected to your PC.
Power	Connect the supplied power adapter here.

Modes

Your Wireless 3-in-1 Companion has 4 modes:

- **Config Mode** – used for configuration only.
- **AP (Access Point) Mode**.
- **AP/Router Mode** – both AP and Router.
- **Client Mode** - the Wireless 3-in-1 Companion is connected to your PC's Ethernet port, and converts that port to a Wireless interface. You PC can then use the Wireless 3-in-1 Companion to join a Wireless network.

The mode is set ONLY by the mode selector switch on the side of the Wireless 3-in-1 Companion. (You will need to wait a few seconds after changing modes.)

It is important to understand these different modes, and the benefits and limitations of each.

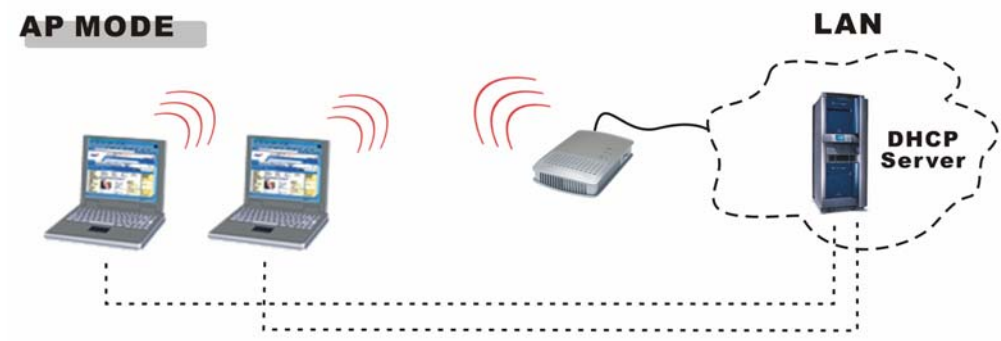
Config Mode

Use this mode to any perform any required configuration. In Config mode, the following settings are always used.

Password	The current password is used. The Default password is blank. If the password is set, you must use `admin` as the login name.
IP address	`192.168.0.1` (Mask: `255.255.255.0`)
DHCP Server	Enabled (for both Ethernet & Wireless)
SSID	`default`
Wireless Security	Disabled

You can connect to the Wireless 3-in-1 Companion using either the Wireless interface or the wired Ethernet connection. Using the Wired connection is recommended.
See the later section ***Initial Configuration*** for details.

Access Point Mode



The Wireless 3-in-1 Companion connects Wireless stations to each other, and to the LAN on the Ethernet port. Because the Wireless 3-in-1 Companion is “transparent” (does not have an IP address) you cannot configure it while in AP mode.

Q. When Should I use Access Point (AP) Mode?

Ans. Use this mode in any of these situations:

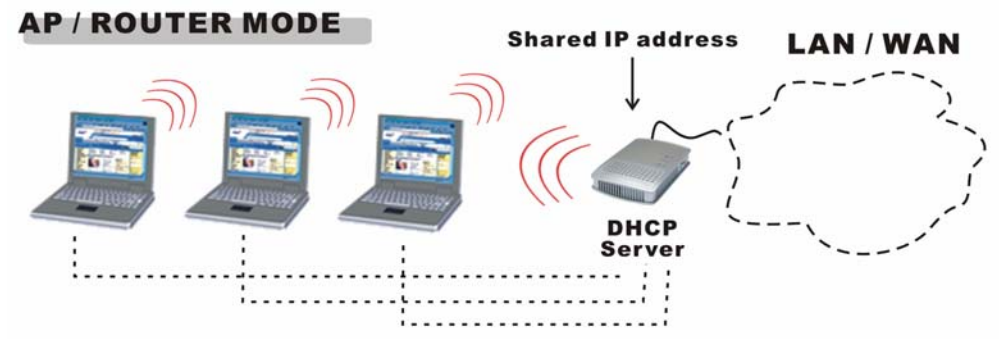
- You are the ONLY user (wireless client).
- There are multiple wireless clients, and you have explicit permission for all users to connect to the LAN or WAN to which the Ethernet port is connected.
- You want to create a private Wireless LAN (not using the Ethernet port), using Infrastructure mode instead of Ad-hoc mode. In this case, each PC must "self-assign" an IP address, since there is no DHCP Server available. If using Windows XP, this self-assignment will work correctly; all wireless stations will have compatible IP addresses.

Q. When Shouldn't I use Access Point (AP) Mode?

Ans. Do NOT use this mode in this situation:

- There are multiple users (wireless clients).
- You do NOT have permission for all of these users to connect to the LAN or WAN on the Ethernet port.
  In this situation, you should use AP/Router mode.

AP/Router Mode



In AP/Router Mode, the Wireless 3-in-1 Companion acts as an AP and a DHCP Server, allocating IP addresses for Wireless stations (clients). It also acts as a NAT Router, sharing the IP address on the Ethernet (LAN/WAN) port with all Wireless clients. (It has 2 IP addresses, one on the LAN/WAN port and another on the Wireless LAN.)

When Should I use AP/Router Mode?

Use this mode in any of these situations:

- The Ethernet port is connected to a Broadband modem rather than an Ethernet port.
- You have permission for ONLY ONE (1) user to connect to the LAN or WAN, but you need to connect multiple users. (In AP/Router mode, the IP address on the Ethernet port is shared by all Wireless clients.)

Q. When Shouldn't I use AP/Router Mode?

Ans. You can always use AP/Router mode to establish a wireless connection to the LAN or WAN.

However, this mode uses a technology called "NAPT" (Network Address Port Translation), and NAPT may cause problems with some complex multi-user communication applications. (There is no problem with common services such as HTTP, FTP, E-mail, etc.) If you have problems, you should try getting permission for all users to connect to the LAN/WAN, so you can use AP mode instead.

Note:

You can connect to the Wireless 3-in-1 Companion, and change its configuration, while it is **AP/Router Mode**.

The IP address used is the "Wireless LAN" IP address, which can be set on the AP/Router setup screen. The default value is 192.168.0.1 (the same as the Config Mode IP address), but you can change this if you wish.

You MUST change the Wireless LAN IP address if the LAN/WAN is using the address range 192.168.0.1 ~ 192.168.0.254.

Client Mode

In Client mode, the Wireless 3-in-1 Companion is connected to the Ethernet port of your PC (or other device), and will connect to a Wireless LAN. This has the effect of converting the Ethernet port to a Wireless interface.

Note that in client mode, the Wireless 3-in-1 Companion is transparent; it has no IP address.

Q. When Should I use Client Mode?

Ans. Use this mode in any of these situations:

- Your PC does not have a wireless interface.
- The wireless interface on your PC does not support the features you need.
- You wish to connect to two (2) Wireless networks simultaneously - one via your wireless interface, the other via the Ethernet port and the Wireless 3-in-1 Companion.

Chapter 2
Initial Configuration

This Chapter covers the initial configuration of the Wireless 3-in-1 Companion.

Requirements

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

Procedure

1. Use the mode selector switch on the side on the Wireless 3-in-1 Companion to select "Config" mode.
2. Power up and wait for the Wireless LED to turn on. This indicates the Wireless 3-in-1 Companion is ready.
3. Establish a Wired or Wireless connection to the Wireless 3-in-1 Companion (a Wired connection is recommended).
   - **Wired** - connect a standard LAN cable from your PC's 10/100BaseT Ethernet port to the Ethernet port on the Wireless 3-in-1 Companion.
   - **Wireless** - select the wireless network with the SSID `default`
4. Start your Web browser.
5. In the "Location" or "Address" bar, enter the following:

   `config.ap`

   - This will work only while in **Config** mode.
     In AP mode, you cannot connect.
     In Router mode, you must connect using the **Wireless LAN IP address**.
   - This may not work if using a wireless connection and your PC also has an active 10/100BaseT Ethernet connection.
6. By default, the admin password is blank, and you will NOT be prompted for a username and password.
   If the admin password has been set (on the ***System*** screen), you will be prompted for the username and password.
   - Enter `admin` for the user name.
   - Enter the current password.
7. You will then see the ***Mode Configuration*** screen.

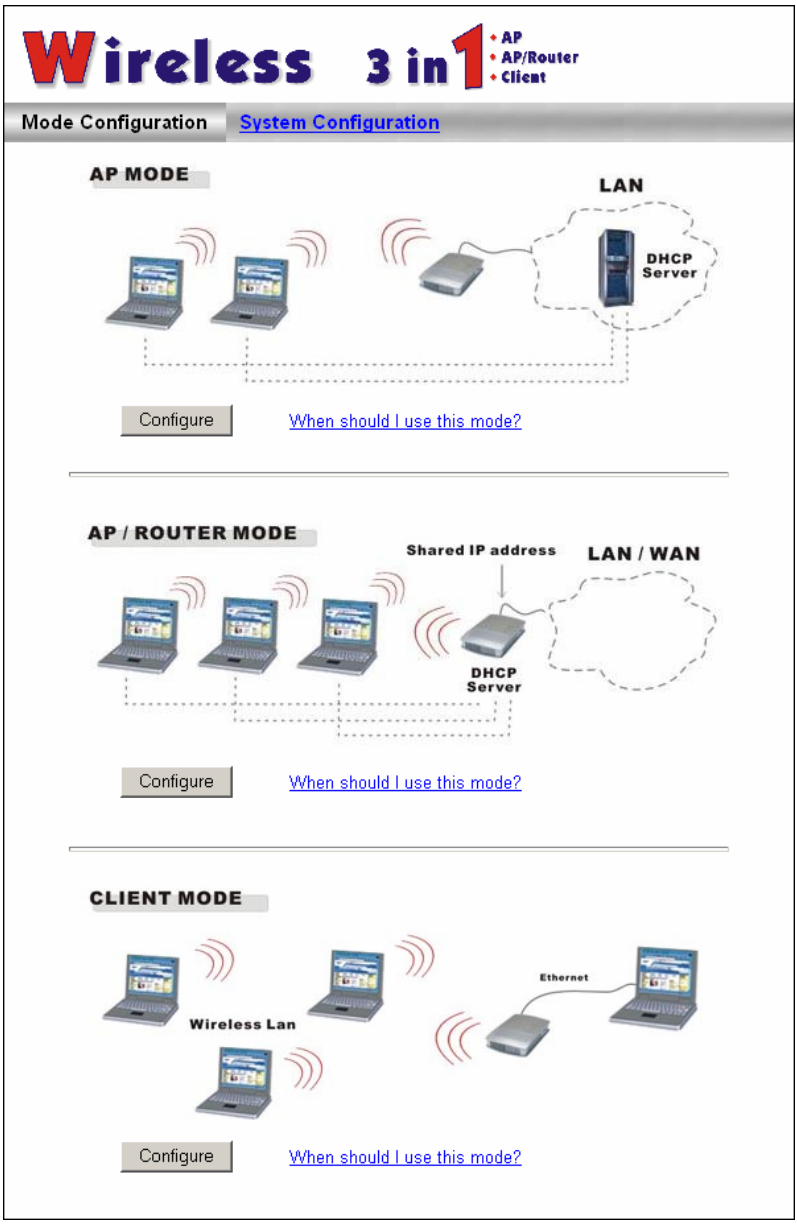


Figure 1 : Mode Configuration Screen

This screen provides access to the 3 main setup screens:

- **System** - settings which are independent of each mode.
- **AP Mode** - settings for AP (Access Point) mode.
- **AP/Router Mode** - settings for AP/Router mode.
- **Client Mode** - settings for Client Mode.

8. Configure the ***System*** screen and the modes (AP or AP/Router) you will use.
   - The ***System*** screen is described in the following section.
   - ***AP Mode*** settings are detailed in Chapter 3.
   - ***AP/Router Mode*** settings are described in Chapters 4 and 5.
   - ***Client Mode*** settings are detailed in Chapter 6.

System Screen

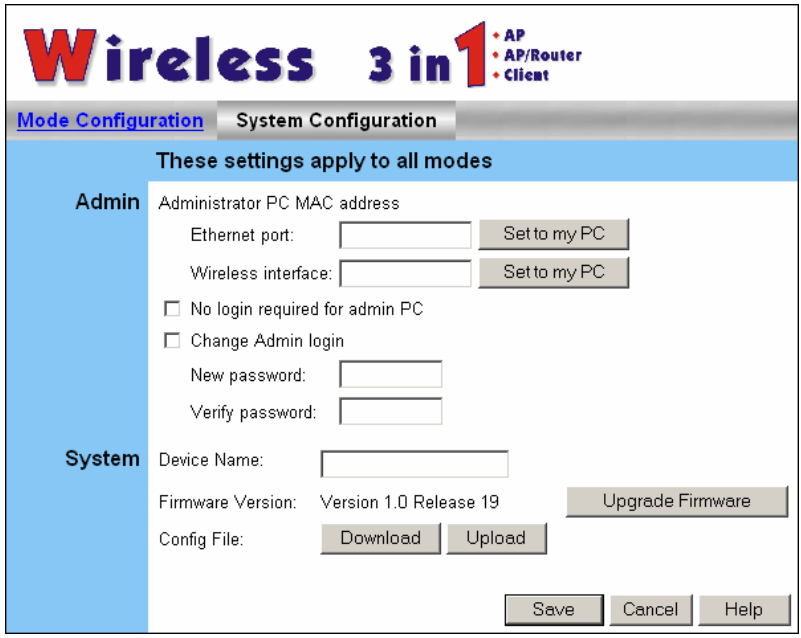


Figure 2: System Screen

Data - System Configuration

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

No login…	If you check this, and provide the MAC address of your PC (see above), then you will not be prompted for the password when you connect using your 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	This login is required to change any settings on the Wireless 3-in-1 Companion. (By default, the password is blank, so the first time you connect, you are not prompted for the password.) Check this box if you wish 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 Wireless 3-in-1 Companion. 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 have downloaded 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 to 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.

Config File Screen

This feature allows you to download the current settings from the Wireless 3-in-1 Companion, and save them to a file on your PC.

You can restore a previously-downloaded configuration file to the Wireless 3-in-1 Companion, by uploading it to the Wireless 3-in-1 Companion.

This screen also allows you to set the Wireless 3-in-1 Companion back to its factory default configuration. Any existing settings will be deleted.

An example ***Config File*** screen is shown below.

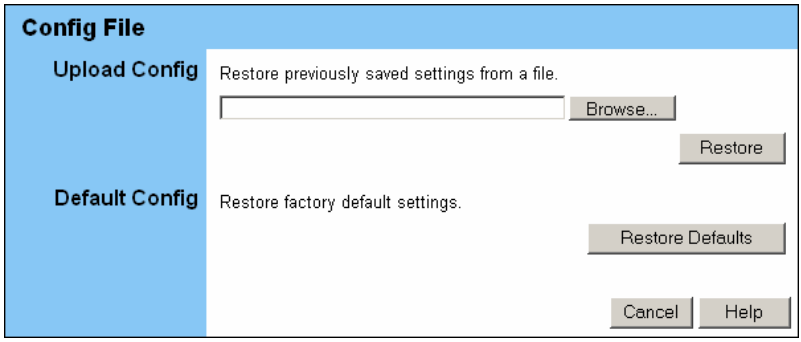


Figure 3: Config File Screen

Data - Config File Screen

Backup Config	Use this to download a copy of the current configuration, and store the file on your PC. Click *Download* to start the download.
Restore Config	This allows you to restore a previously-saved configuration file back to the Wireless 3-in-1 Companion. 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 Wireless 3-in-1 Companion to its factory default settings. **WARNING !** This will delete ALL of the existing settings.

Upgrade Firmware

The firmware (software) in the Wireless 3-in-1 Companion can be upgraded using your Web Browser.

You must first download the upgrade file, then select *Upgrade* on the *Administration* menu. You will see a screen like the following.

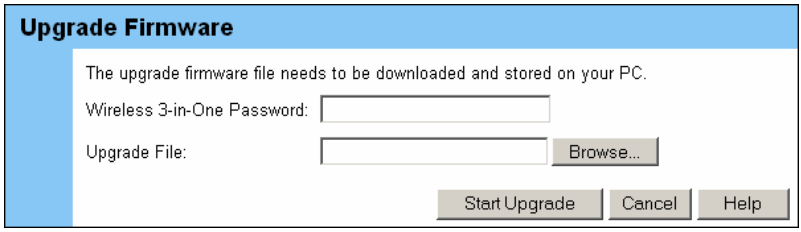


Figure 4: Upgrade Firmware Screen

To perform the Firmware Upgrade:

1. Click the "Browse" button and navigate to the location of the upgrade file.
2. Select the upgrade file. Its name will appear in the *Upgrade File* field.
3. Click the "Start Upgrade" button to commence the firmware upgrade.

The Wireless 3-in-1 Companion is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the Wireless 3-in-1 Companion will be lost.

Chapter 3
Setup - AP Mode

This Chapter provides Setup details for the AP mode of the Wireless 3-in-1 Companion.

Overview

You can NOT connect to the Wireless 3-in-1 Companion while it is in AP (Access Point) mode. Configuration for AP mode must be performed while in Config Mode.

Note:

By default, the Wireless 3-in-1 Companion will allow both 802.11b and 802.11g connections.

Connecting

1. Use the mode selector switch on the side on the Wireless 3-in-1 Companion to select "Config" mode.
2. Power up and wait for the Wireless LED to turn on. This indicates the Wireless 3-in-1 Companion is ready.
3. Establish a Wired or Wireless connection to the 3-in-1.
   - **Wired** - connect a standard LAN cable from your PC's 10/100BaseT Ethernet port to the Ethernet port on the Wireless 3-in-1 Companion.
   - **Wireless** - select the wireless network with the SSID `default`
4. Start your Web browser.
5. In the "Location" or "Address" bar, enter the following:

   `config.ap`

   Note: This will work only while in **Config** mode.
6. If the admin password has been set (on the ***System*** screen), you will be prompted for the username and password.
   - Enter `admin` for the user name.
   - Enter the current password.
7. You will then see the ***Mode Configuration*** screen.
   Click the "Config" button for **AP Mode**, to view the ***AP Setup*** screen.

AP Setup Screen

This screen is reached by clicking the "Config" button for AP Mode on the ***Mode Configuration*** screen.

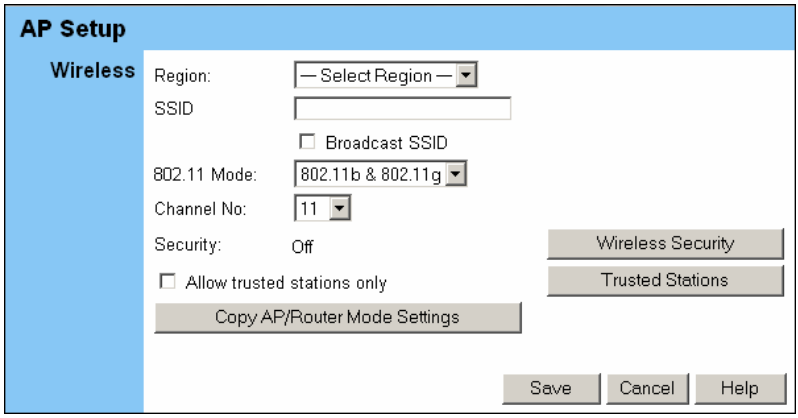


Figure 5: AP Setup Screen

Data - AP Setup Screen

Wireless	
Region	The regions other than North America can not be set up by the users.
SSID	• If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier). • You can change the SSID to your preferred value. • AP Mode and AP/Router mode must use different SSIDs. Using the same SSID for both modes would confuse Wireless clients.
Broadcast SSID	If Enabled, the SSID will broadcast its name to all Wireless Stations. On your PC, the Wireless 3-in-1 Companion will then be listed as an "Available Wireless Network", using the SSID above. You can then select this wireless network, and your PC will then adopt this SSID
802.11 Mode	Select the desired mode: • **g & b** - Both 802.11.g and 802.11b Wireless stations will be able to use the Wireless 3-in-1 Companion. • **g only** - Only 802.11g Wireless stations can use the Wireless 3-in-1 Companion.
Channel No.	The channel only can use 1-11 in USA, 1-13 in Eroupe.

Security	The current security setting for wireless connections is displayed. The default value is Off, meaning no security.
Wireless Security Button	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 this Access Point. To use this feature: • Enable this 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 screen to this screen. • This is only useful if you have already configured the ***AP/Router Setup*** screen. • The SSID will not be copied. Each mode must use a different SSID. Using the same SSID for different modes would confuse wireless clients.

Wireless Security Screen

This screen is accessed by clicking the *Wireless Security* button on the ***AP Setup*** screen.

The default security setting is *Disabled*. No configuration is required. Data is not encrypted before transmission.

WEP Wireless Security

The following image shows the Wireless Security screen when WEP is selected.

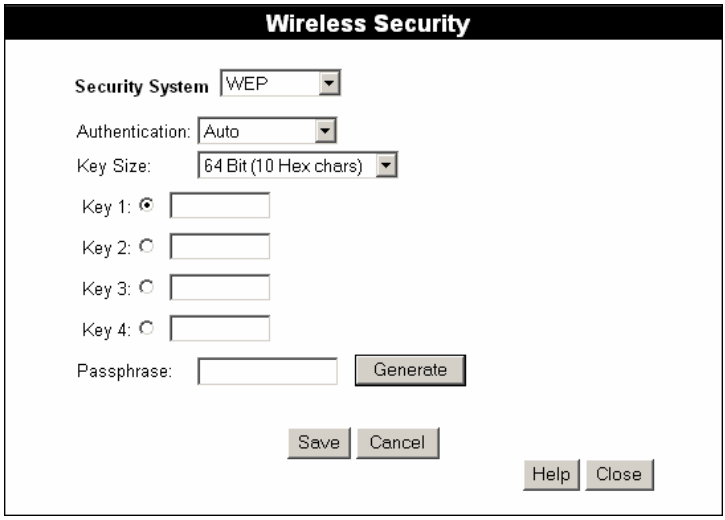


Figure 6 Wireless Security (AP Mode - WEP)

Data - WEP Wireless Security

Security System	Select the desired option: • Disabled • WEP • WPA-PSK The screen will change according to the current selection. The settings below are only visible if WEP is selected.
Key Size	Select the desired option. Wireless Stations must use the same setting. • **64 Bit (10 Hex chars)** - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 64 Bit Encryption, the key size is Hex 10 chars. • **128 Bit (26 Hex chars)** - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 128 Bit Encryption, the key size is 26 Hex chars. Note: Hex chars are 0~9 and A~F.
Authentication Type	Normally, this should be left at the default value of "Automatic". If changed to "Open System" or "Shared Key", ensure that your Wireless Stations use the same setting.
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.
Key Value	Enter the key value or values you wish to use. The **Default Key** is required, the others are optional.
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

The following image shows the Wireless Security screen when WPA-PSK is selected.

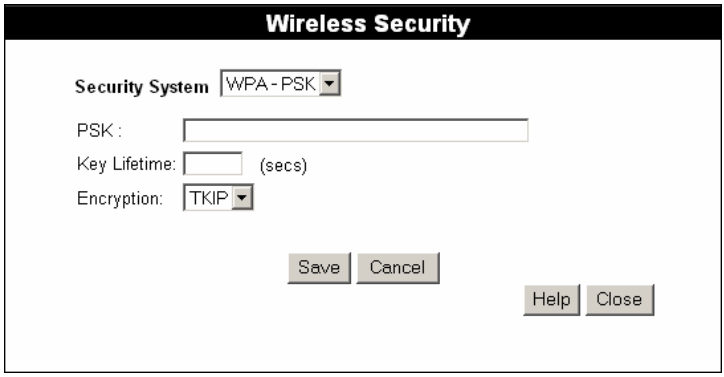


Figure 7: Wireless Security - WPA-PSK

Data - WPA-PSK Wireless Security

Security System	Select the desired option: • Disabled • WEP • WPA-PSK The screen will change according to the current selection. The settings below are only visible if WPA-PSK is selected.
PSK	Enter the PSK (Pre-shared Key), sometimes called the network key. Wireless clients must use the same key.
WPA Encryption	Select the desired encryption algorithm. Wireless stations must use the same setting..

Trusted Wireless Stations Screen

This screen is accessed by clicking the *Trusted Stations* button on the ***AP Setup*** screen.

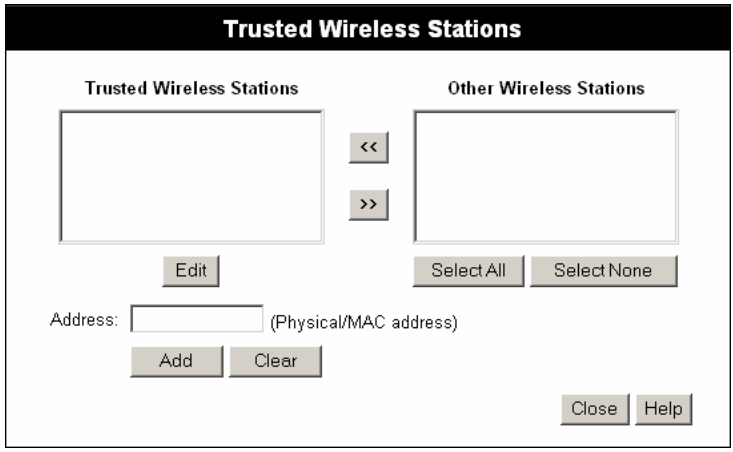


Figure 8: Trusted Wireless Stations (AP Mode)

Data - Trusted Wireless Stations

Trusted Wireless Stations	This lists any Wireless Stations which you have designated as “Trusted”.
Other Wireless Stations	This list any Wireless Stations detected by the Access Point, which you have not designated as "Trusted".
Address	The MAC (physical) address of the Trusted Wireless Station. Use this when adding or editing 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, and click the " << " button. • Enter the Address (MAC or physical address) of the wireless station, and click the "Add " 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	De-select any Stations currently selected 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.

Chapter 4
Setup - AP/Router Mode

This Chapter provides Setup details for the AP/Router mode of the Wireless 3-in-1 Companion.

Overview

In AP/Router mode, the Wireless 3-in-1 Companion provides the following services:

- Wireless Access Point
- DHCP Server
- Shared IP address
- Firewall Protection for Wireless Stations.

To configure AP/Router mode, you can connect while in **Config mode** or in **AP/Router mode**.

- To connect in **Config mode**, use the method described in *Initial Configuration*.
- To connect while in **AP/Router mode**, use the method below

Connecting while in AP/Router Mode

Ensure that your PC has established a Wireless connection to the Wireless 3-in-1 Companion before commencing this procedure.

1. Start your Web browser.
2. In the "Location" or "Address", enter "HTTP://" and the current IP address for the Wireless LAN, as set on the *AP/Router* screen. The default value is 192.168.0.1:
   `HTTP://192.168.0.1`
3. If the admin password has been set (on the ***System*** screen), you will be prompted for the username and password.
   - Enter `admin` for the user name.
   - Enter the current password.
4. You will then see the ***Mode Configuration*** screen.
   Click the "Configure" button for **AP/Router Mode**.
   You will the see the ***AP/Router Setup*** Screen.

Note:

By default, the Wireless 3-in-1 Companion will allow both 802.11b and 802.11g connections.

AP/Router Setup Screen

This screen is reached by clicking the "Config" button for AP/Router Mode on the ***Mode Configuration*** screen.

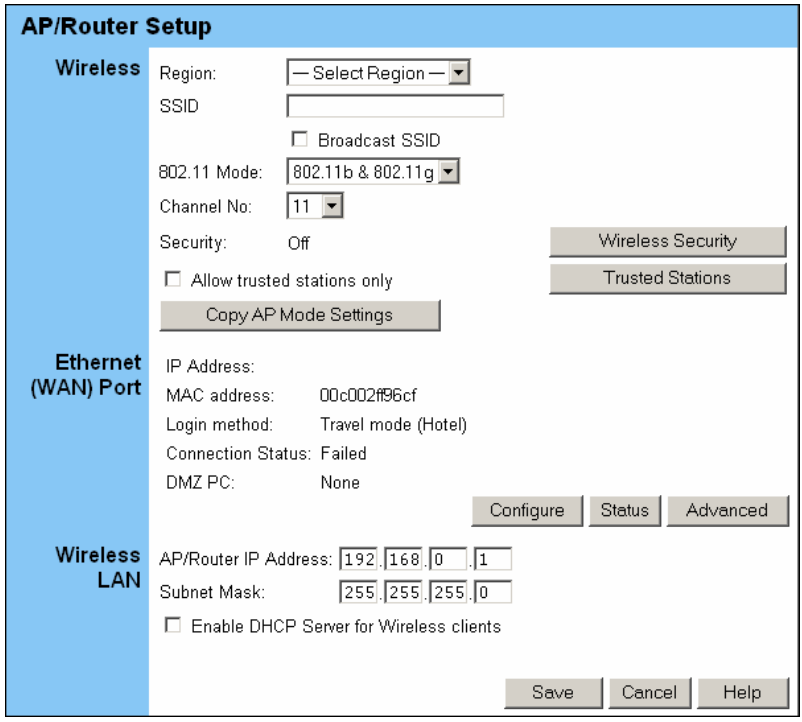


Figure 9: AP/Router Setup Screen

Data - AP/Router Setup

Wireless	
Region	The regions other than North America can not be set up by the users.
SSID	• If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier). • You can change the SSID to your preferred value. • AP Mode and AP/Router mode must use different SSIDs. Using the same SSID for both modes would confuse Wireless clients.
Broadcast SSID	If Enabled, the SSID will broadcast its name to all Wireless Stations. On your PC, the Wireless 3-in-1 Companion will then be listed as an "Available Wireless Network", using the SSID above. You can then select this wireless network, and your PC will then adopt this SSID

802.11 Mode	Select the desired mode: • **g & b** - Both 802.11.g and 802.11b Wireless stations will be able to use the Wireless 3-in-1 Companion. • **g only** - Only 802.11g Wireless stations can use the Wireless 3-in-1 Companion.
Channel No.	The channel only can be use 1-11 in USA, 1-13 in Eroupe.
Security	The current security setting for wireless connections is displayed. The default value is Off, meaning no security.
Wireless Security Button	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 this Access Point. To use this feature: • Enable this 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 screen to this screen. • This is only useful if you have already configured the ***AP Setup*** screen. • 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 Wireless 3-in-1 Companion is not in AP/Router mode. • The Wireless 3-in-1 Companion is in AP/Router mode, but there is no active connection on the Ethernet (WAN) port. **Note**: In AP/Router mode, the Wireless 3-in-1 Companion 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.

Login Method	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 Wireless 3-in-1 Companion 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 Wireless 3-in-1 Companion 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 Wireless 3-in-1 Companion 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 Wireless 3-in-1 Companion 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 Wireless 3-in-1 Companion. • The default value is *Enabled*. • **It is strongly recommended that this feature be enabled**. Do not disable this feature unless you have a good reason to do so.

Wireless Security Screen

This screen is accessed by clicking the *Wireless Security* button on the ***AP/Router Setup*** screen.

The default security setting is *Disabled*. No configuration is required. Data is not encrypted before transmission.

WEP Wireless Security

The following image shows the Wireless Security screen when WEP is selected.

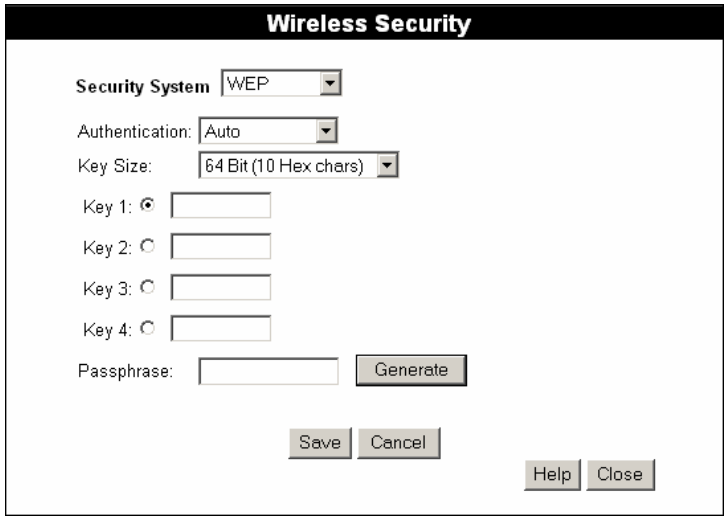


Figure 10 Wireless Security (AP Mode - WEP)

Data - WEP Wireless Security

Security System	Select the desired option: • Disabled • WEP • WPA-PSK The screen will change according to the current selection. The settings below are only visible if WEP is selected.
Key Size	Select the desired option. Wireless Stations must use the same setting. • **64 Bit (10 Hex chars)** - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 64 Bit Encryption, the key size is Hex 10 chars. • **128 Bit (26 Hex chars)** - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 128 Bit Encryption, the key size is 26 Hex chars. Note: Hex chars are 0~9 and A~F.
Authentication Type	Normally, this should be left at the default value of "Automatic". If changed to "Open System" or "Shared Key", ensure that your Wireless Stations use the same setting.
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.
Key Value	Enter the key value or values you wish to use. The **Default Key** is required, the others are optional.
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

The following image shows the Wireless Security screen when WPA-PSK is selected.

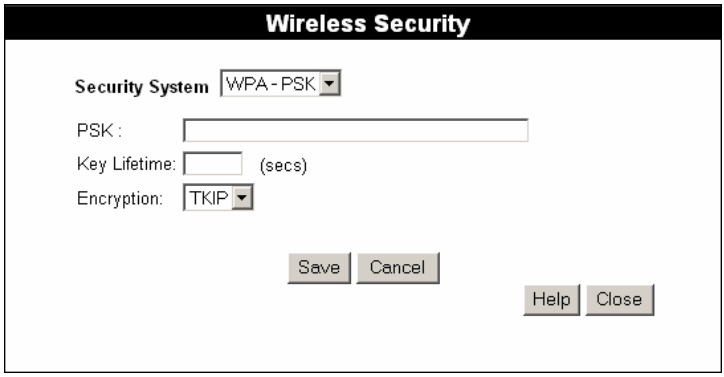


Figure 11: Wireless Security - WPA-PSK

Data - WPA-PSK Wireless Security

Security System	Select the desired option: • Disabled • WEP • WPA-PSK The screen will change according to the current selection. The settings below are only visible if WPA-PSK is selected.
PSK	Enter the PSK (Pre-shared Key), sometimes called the network key. Wireless clients must use the same key.
WPA Encryption	Select the desired encryption algorithm. Wireless stations must use the same setting..

Trusted Wireless Stations Screen

This screen is accessed by clicking the *Trusted Stations* button on the ***AP/Router Setup*** screen.

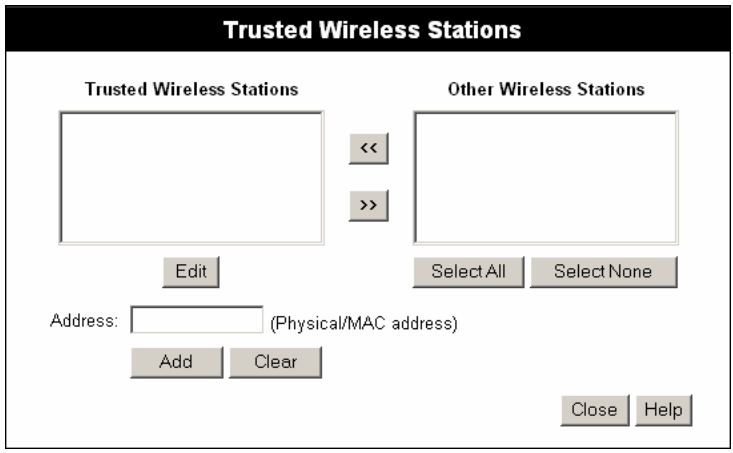


Figure 12: Trusted Wireless Stations (AP Mode)

Data - Trusted Wireless Stations

Trusted Wireless Stations	This lists any Wireless Stations which you have designated as “Trusted”.
Other Wireless Stations	This list any Wireless Stations detected by the Access Point, which you have not designated as "Trusted".
Address	The MAC (physical) address of the Trusted Wireless Station. Use this when adding or editing 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, and click the " << " button. • Enter the Address (MAC or physical address) of the wireless station, and click the "Add " 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	De-select any Stations currently selected 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, ready for new input.

Ethernet (WAN) Port Configuration

By default, the Wireless 3-in-1 Companion will try to obtain an IP address automatically on the Ethernet (WAN) port.

If this does not work in the current environment, click the "Configure" button to change the settings for the Ethernet (WAN) Port.

Travel Mode Connection

The default connection method is "Travel Mode (Hotel)" as shown below.

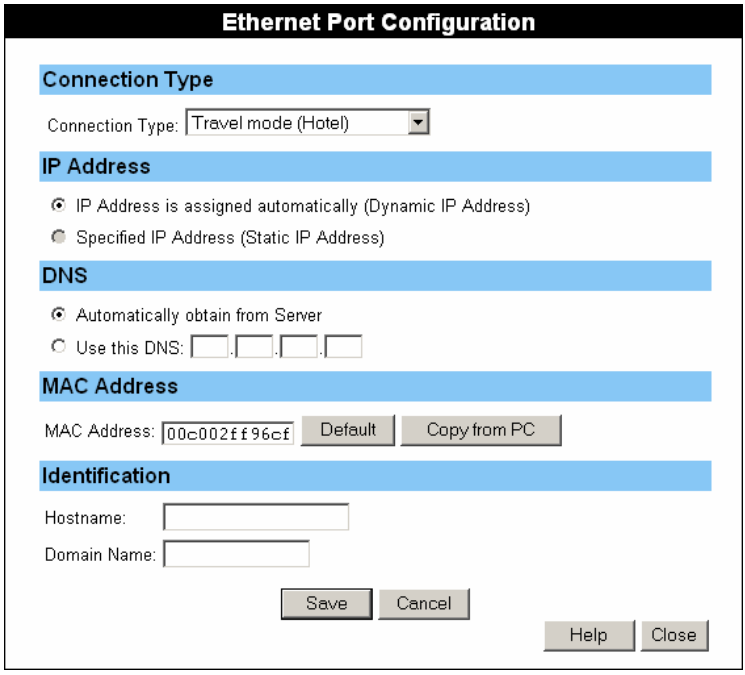


Figure 13: Wan Port Configuration - Travel Mode

Data - Ethernet Port (Travel Mode)

Connection Type	
Connection Type	The default 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. 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 IP Address - The address of the router or gateway on the LAN or WAN you are connecting to.
DNS	
Automatically obtain from Serve	The DNS (Domain Name Server) address is normally obtained automatically from the DHCP Server which provides the IP address. Note that if using a fixed IP address, then no Server is used, so 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 Specified (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 Wireless 3-in-1 Companion, or from the Wireless 3-in-1 Companion 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 have provided some software to connect and login. If using the Wireless 3-in-1 Companion, 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 ask the administrator of the LAN or WAN to which you are connecting.

The following image and table shows all available settings.

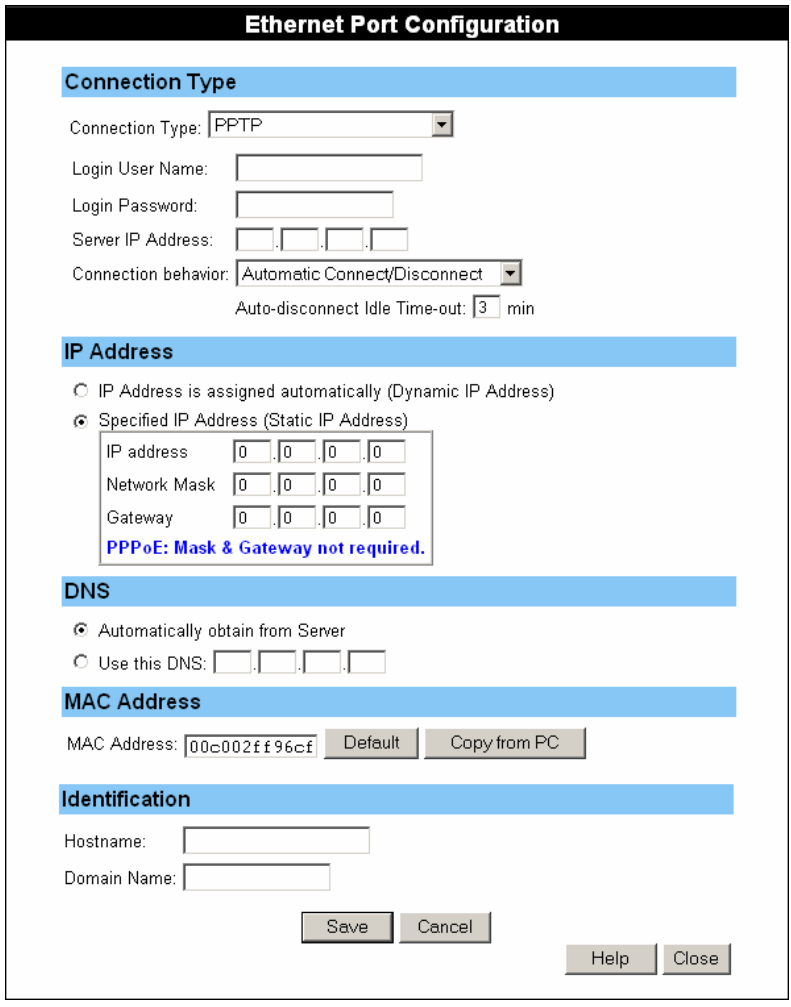


Figure 14: Ethernet Port Configuration - All Settings

Data - Ethernet Port

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 Wireless 3-in-1 Companion, 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. 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 which provides the IP address. Note that if using a fixed IP address, then no Server is used, so 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 Wireless 3-in-1 Companion, or from the Wireless 3-in-1 Companion to your PC.
Identification	
Hostname	If using a dynamic IP address, this name is provided to the DHCP Server. Normally, it does not matter what name you use. 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

Ethernet (WAN) Port Status

To check the status of the Ethernet (WAN) port connection, click the *Status* button. This will open a sub-window; the screen you will see depends on the connection method currently in use.

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.

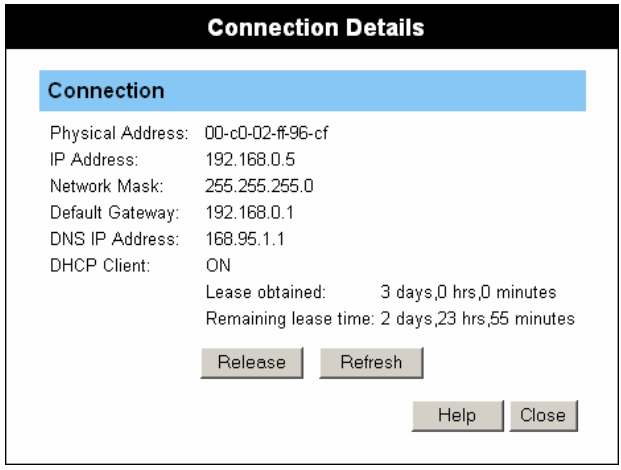


Figure 15: Connection Details - Fixed/Dynamic IP Address

Data - Fixed/Dynamic IP address Screen

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 **Button will display EITHER "Release" OR "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 Wireless 3-in-1 Companion, 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 Wireless 3-in-1 Companion (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 using PPPoE (PPP over Ethernet), a screen like the following example will be displayed when the *Status* button is clicked.

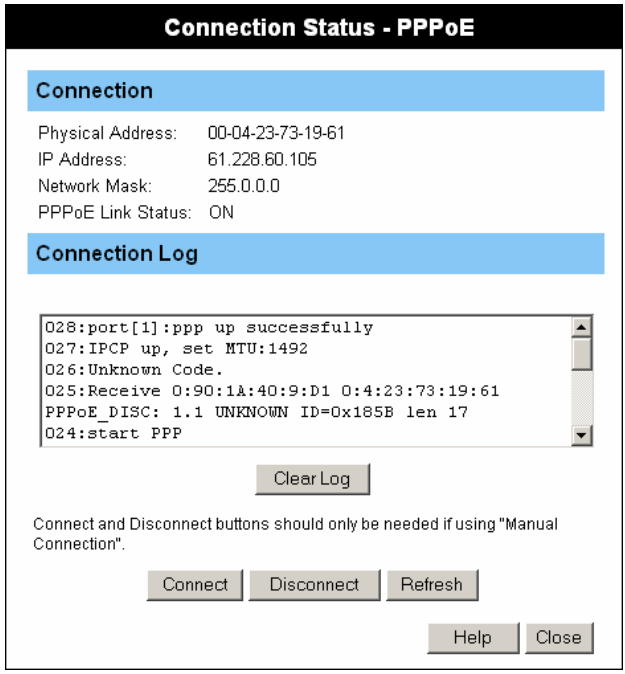


Figure 16: PPPoE Status Screen

Data - PPPoE Screen

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.

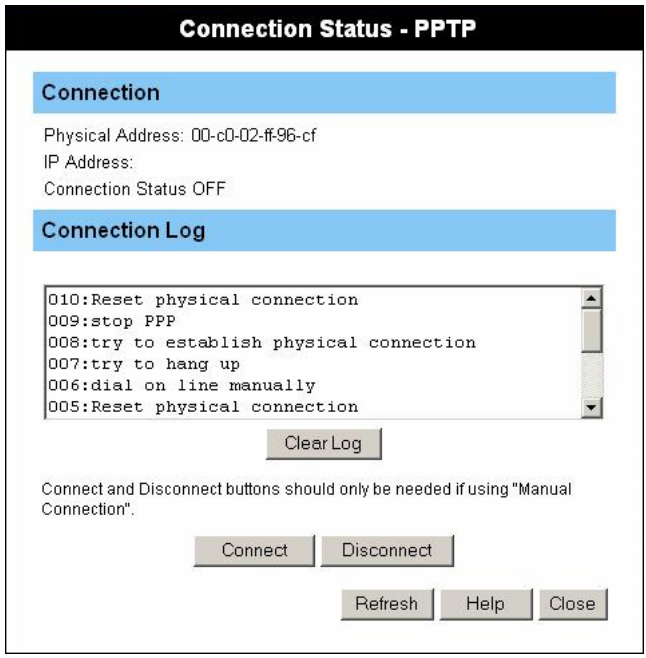


Figure 17: PPTP Status Screen

Data - PPTP Screen

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.

Connection Status - L2TP

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

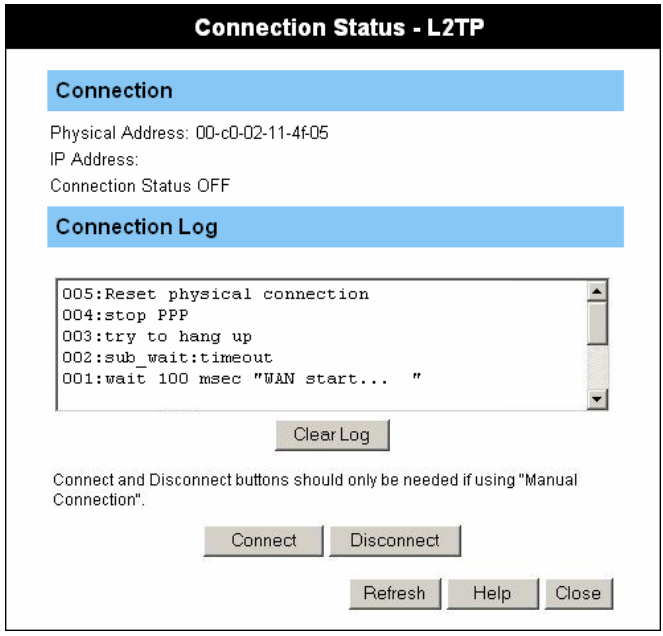


Figure 18: L2TP Status Screen

Data - L2TP Screen

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.

Chapter 5

AP/Router Mode - Advanced Features

This Chapter explains when and how to use the Wireless 3-in-1 Companion's "Advanced" Features in AP/Router mode

Overview

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.

Advanced Internet Screen

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.

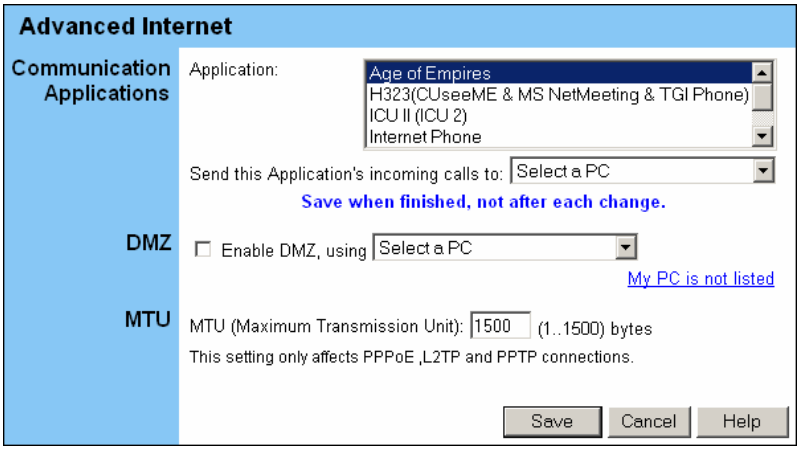


Figure 19: Internet Screen

Communication Applications

Most applications are supported transparently by the Wireless 3-in-1 Companion. But sometimes it is not clear which PC should receive an incoming connection. This problem could arise with the ***Communication Applications*** listed on this screen.

If this problem arises, you can use this screen to set which PC should receive an incoming connection, as described below.

Communication Applications	
Application	This 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 incoming calls ..	This 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 "Save" after each change; you can set the destination PC for each application, then "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 Support. • 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.

Port Forwarding

This feature, sometimes called *Virtual Servers*, allows you to make Servers on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

- Your Server does not have a valid external IP Address.
- Attempts to connect to devices on your LAN are blocked by the firewall in this device.

The "Port Forwarding" feature solves these problems and allows Internet users to connect to your servers, as illustrated below.

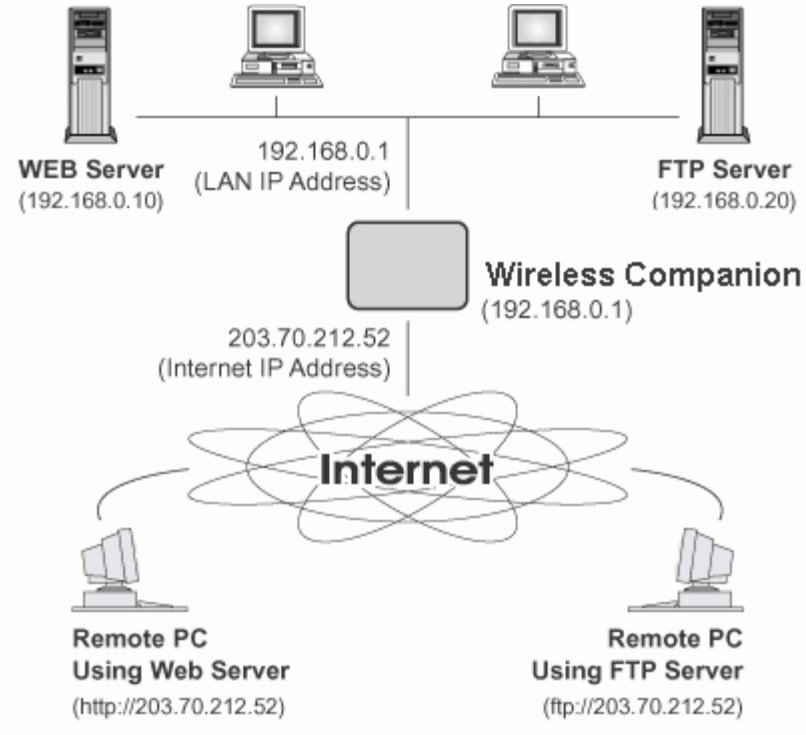


Figure 20: Port Forwarding

IP Address seen by Internet Users

Note that, in this illustration, both Internet users are connecting to the same IP Address, but using different protocols.

To Internet users, all virtual Servers on your LAN have the same IP Address. This IP Address is allocated by your ISP.

This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers.

However, you can use the *DDNS (Dynamic DNS)* feature to allow users to connect to your Port Forwarding using a URL, instead of an IP Address.

Port Forwarding Screen

The *Port Forwarding* screen is reached by the *Port Forwarding* link. An example screen is shown below.

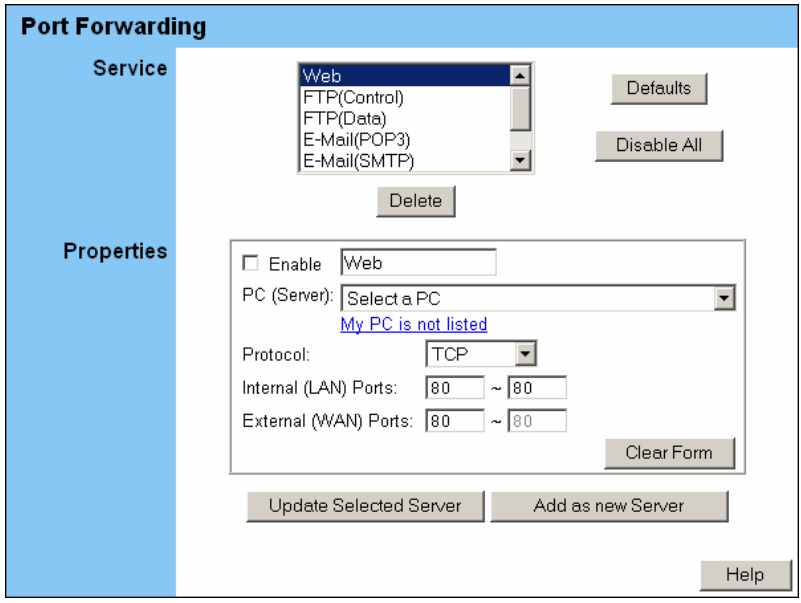


Figure 21: Port Forwarding Screen

This screen lists a number of pre-defined Servers, and allows you to define your own Servers. Details of the selected Server are shown in the "Properties" area.

Data - Port Forwarding Screen

Service	
Service	This lists a number of pre-defined Services, plus any Services you have defined. Details of the selected Service are shown in the "Properties" area..
Properties	
Enable	Use this to 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 from traffic on the local 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 their 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 can not 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.

For each entry, the PC must be running the appropriate Server software.

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.

From the WAN or Internet, ALL Port Forwarding have the same IP Address - the IP address assigned to the WAN port.

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:
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.

Dynamic DNS (Domain Name Server)

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 Wireless 3-in-1 Companion's DDNS screen.
4. The Wireless 3-in-1 Companion 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.

Dynamic DNS Screen

Select *DDNS* to see a screen like the following:

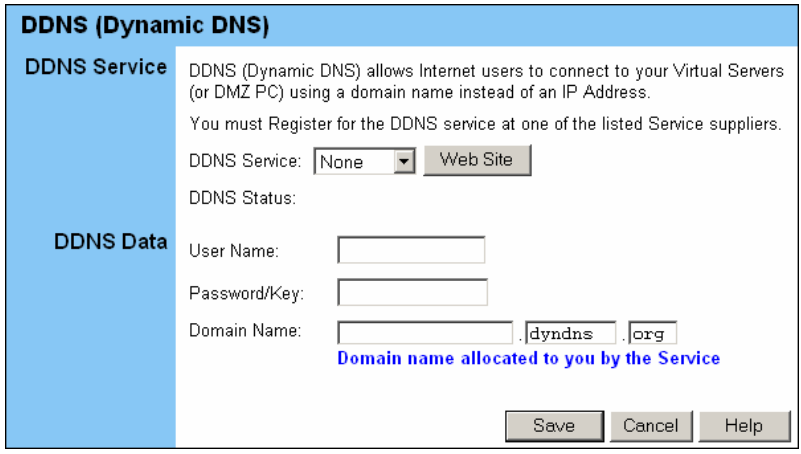


Figure 22: DDNS Screen

Data - Dynamic DNS Screen

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. You can reach the Service provider's Web Site by selecting them in the list and clicking the "Web Site" button. • Apply for a Domain Name, and ensure it is allocated to you. • Details of your DDNS account (Name, password, Domain name) must then be entered and saved on this screen. • This device will then automatically ensure that your current IP

	Address is recorded by the DDNS Service Provider. (You do NOT need to use the "Client" program provided by some DDNS Service providers.) • From the Internet, users will now be able to connect to your Servers (as defined by your Port Forwarding setup) or DMZ PC using your Domain name.
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.

Network Diagnostics

This screen allows you to perform a "Ping" or a "DNS lookup". These activities can be useful in solving network problems.

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

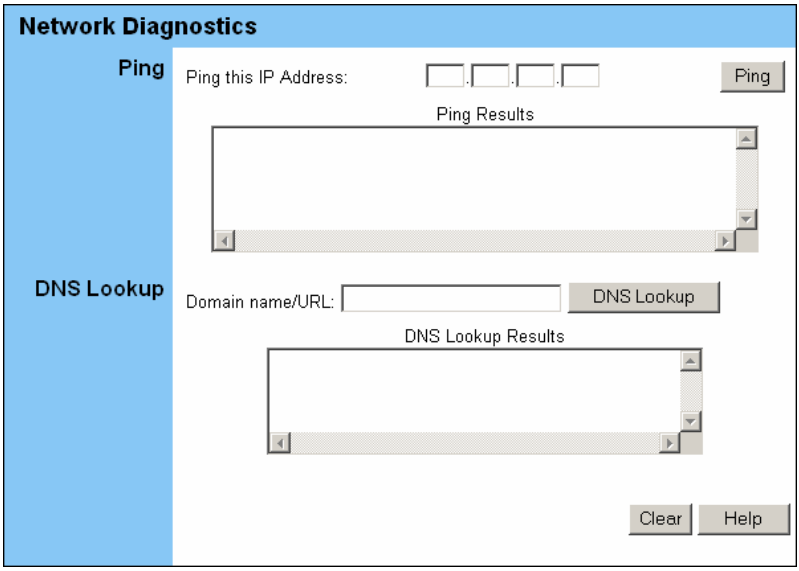


Figure 23: Network Diagnostics Screen

Data - Network Diagnostics Screen

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.

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.

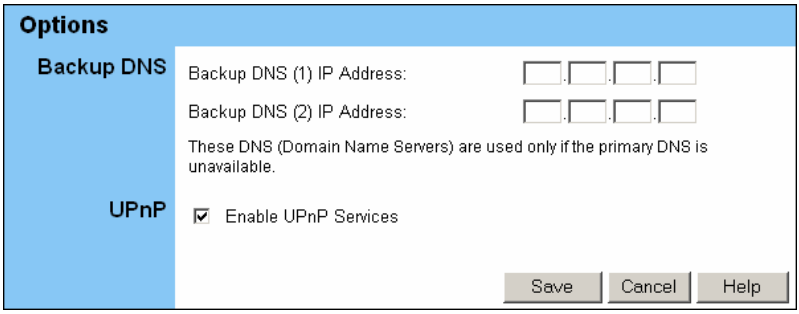


Figure 24: Options Screen

Data - Options Screen

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.

PC Database

The PC Database is used whenever you need to select a PC (e.g. for the "DMZ" PC). It eliminates the need to enter IP addresses. Also, you do not need to use fixed IP addresses on your Wireless LAN.

PC Database Screen

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

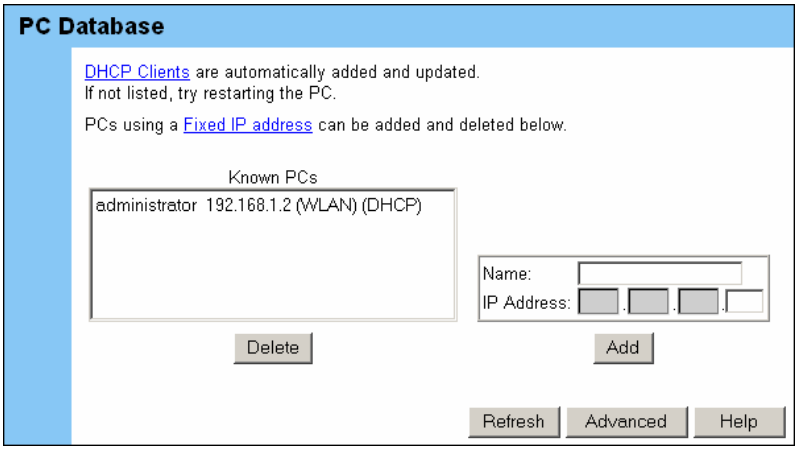


Figure 25: PC Database

- PCs which are "DHCP Clients" are automatically added to the database, and updated as required.
- By default, non-Server versions of Windows act as "DHCP Clients"; this setting is called "Obtain an IP Address automatically".
- The Wireless 3-in-1 Companion 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.

Data - PC Database Screen

Known PCs	This 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.

Advanced PC Database

This screen is displayed if the *Advanced* button on the ***PC Database*** is clicked. It provides more control than the standard ***PC Database*** screen.

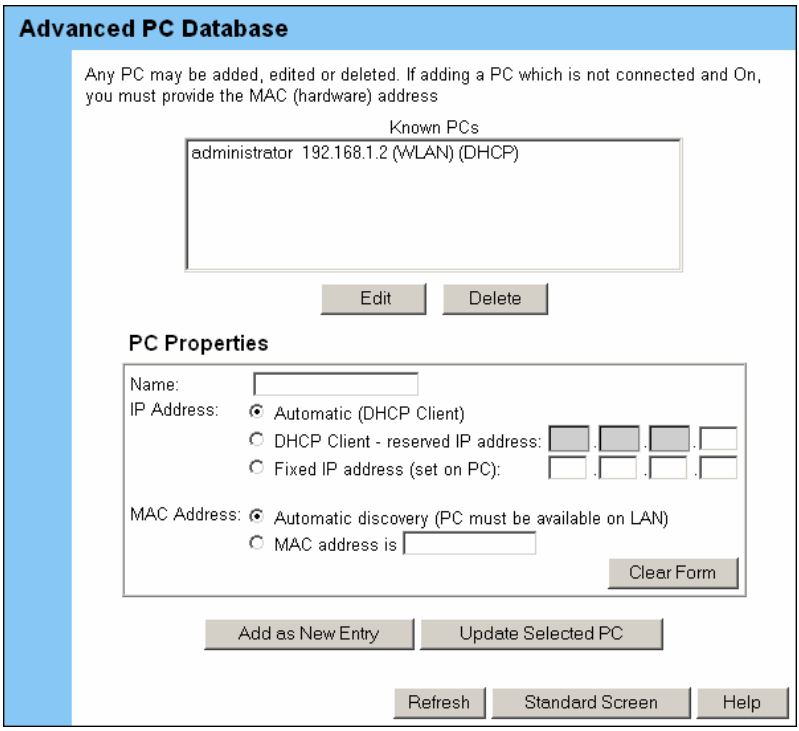


Figure 26: Advanced PC Database

Data - Advanced PC Database

Known PCs	This 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 Wireless 3-in-1 Companion 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 Wireless 3-in-1 Companion 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 Wireless 3-in-1 Companion'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 Wireless 3-in-1 Companion 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 Wireless 3-in-1 Companion uses this to provide a unique identifier for each PC. Because of this, the MAC address can NOT 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.

Security

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

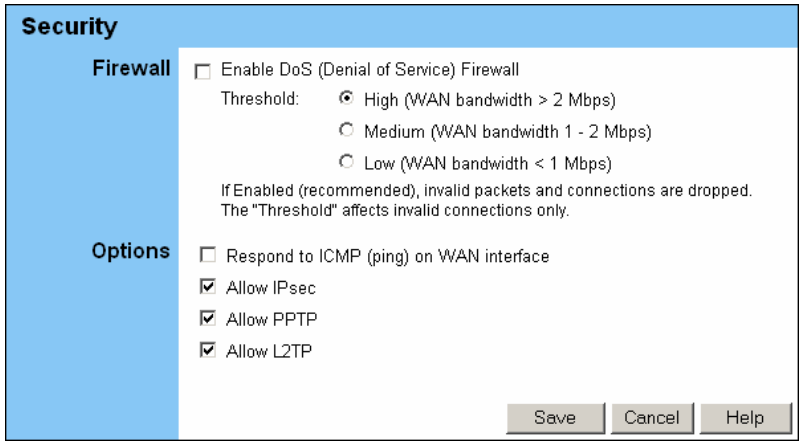


Figure 27: Security Screen

Data - Security Screen

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 can not 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 Wireless 3-in-1 Companion 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.

Chapter 6
Setup - Client Mode

This Chapter details configuration for Client Mode.

Overview

You can NOT connect to the Wireless 3-in-1 Companion while it is in Client mode. Configuration for Client mode must be performed while in Config Mode.

Connecting

1. Use the mode selector switch on the side on the Wireless 3-in-1 Companion to select "Config" mode.
2. Power up and wait for the Wireless LED to turn on. This indicates the Wireless 3-in-1 Companion is ready.
3. Establish a Wired or Wireless connection to the 3-in-1.
   - **Wired** - connect a standard LAN cable from your PC's 10/100BaseT Ethernet port to the Ethernet port on the Wireless 3-in-1 Companion.
   - **Wireless** - select the wireless network with the SSID `default`
4. Start your Web browser.
5. In the "Location" or "Address" bar, enter the following:

   `config.ap`

   Note: This will work only while in **Config** mode.
6. If the admin password has been set (on the ***System*** screen), you will be prompted for the username and password.
   - Enter `admin` for the user name.
   - Enter the current password.
7. You will then see the ***Mode Configuration*** screen.
   Click the "Config" button for **Client Mode**, to view the ***Client Setup*** screen.

Client Mode Setup

The screen for Client Mode is reached by clicking the "Config" button for Client Mode on the ***Mode Configuration*** screen.

In client mode, you can create a Profile for each Wireless network you use regularly.

- A "Profile" contains all settings for the Wireless network, including the security settings.
- Only one (1) Profile can be enabled at any time.
- If the Wireless network defined by the currently-enabled profile is not available, then no wireless connection will be made.

Client Mode Setup Screen

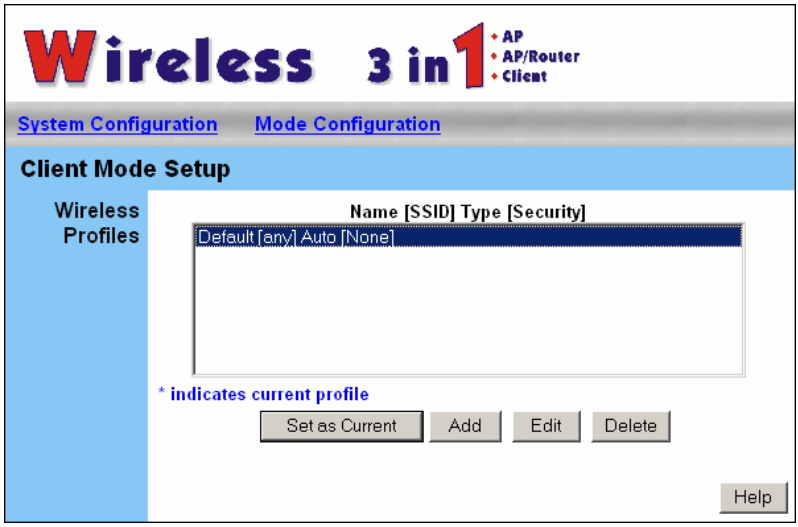


Figure 28: Client Mode Setup Screen

Data - Client Mode Setup Screen

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 wil be disabled. • **Add** - Create a new Profile. This will display the • **Edit** - Change the settings for the selected profile. • **Delete** - Delete the selected profile.

Wireless Client Profile Screen

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

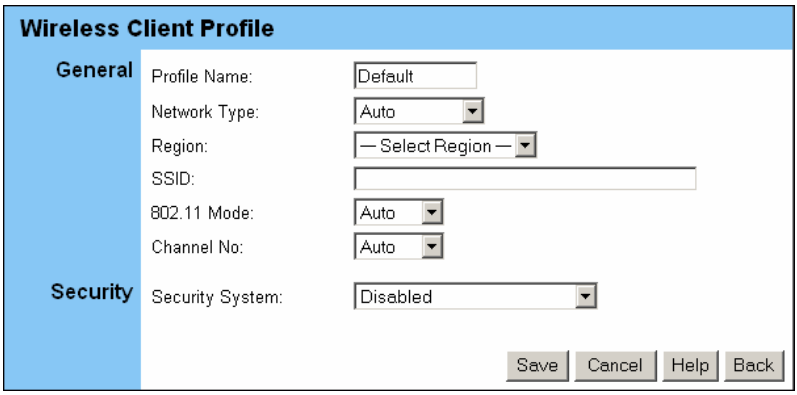


Figure 29: Wireless Client Profile

Data - Wireless Client Profile

General	
Profile Name	Enter a suitable name for this profile. Each profile must have a unique name.
Network Type	Select the desired option: • **Auto** - this device will attempt to join a Wireless network with the same SSID, regardless of whether the network is using Infra-structure mode or Ad hoc mode. • **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.

SSID	Enter the SSID of the wireless network you wish to join. • If 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.
802.11 mode	Select the desired option: • **Auto** - This station will auto-select the correct mode to allow communication. • **802.11b** - Only a 802.11b connection will be used. • **802.11g** - Only a 802.11g connection will be used.
Channel No.	This field determines which operating frequency will be used. • If the network type is "Auto" or "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	
Authentication	Normally this can be left at the default value of "Automatic." If that fails, select the appropriate value - "Open System" or "Shared Key." Check your wireless card's documentation to see what method to use.

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.
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).
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.
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 7
Operation and Usage

This Chapter details the operation of the Wireless 3-in-1 Companion and the status screens.

Overview

The mode can be changed ONLY by using the Mode switch on the side of the Wireless 3-in-1 Companion.

This switch has 4 positions:

1. AP Mode
2. AP/Router Mode
3. Config Mode
4. Reserved

Set Chapter 1 for details about each mode, and some tips on which mode to use in different environments.

Changing Modes

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

- Whenever the mode is changed, the Wireless 3-in-1 Companion 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 Wireless 3-in-1 Companion.

Using AP Mode

1. Use a standard LAN cable to connect the Ethernet port on the Wireless 3-in-1 Companion to the desired LAN.
2. Use the mode selector switch on the side on the Wireless 3-in-1 Companion to select "AP" mode.
3. Wait for the restart to be completed, and the Wireless LED to come On.
4. On your PC, select the wireless LAN matching the SSID of the Wireless 3-in-1 Companion in AP mode.
   The default SSID for AP mode is `default_AP`
5. If necessary, configure your PC's wireless interface to match the settings of the Wireless 3-in-1 Companion's AP mode.
6. You should then be able to connect to the LAN via the Wireless 3-in-1 Companion.
   - You can check the status of your PC's wireless interface to see that your PC has obtained an IP address.
   - This IP address must come from a server on the LAN; the Wireless 3-in-1 Companion itself is transparent.

If the Ethernet port is not connected to a functional LAN, then your PC will "self-assign" an IP address.

Using AP/Router Mode

1. Use a standard LAN cable to connect the Ethernet port to the desired LAN or WAN.

   Note:

   To avoid potential problems, you should NOT change the LAN/WAN connection from the Wireless 3-in-1 Companion to your PC, or vice versa. Doing so may cause the connection to fail.
2. Use the mode selector switch on the side on the Wireless 3-in-1 Companion to select "AP/Router" mode.
3. Wait for the restart to be completed, and the Wireless LED to turn On.
4. On your PC, select the wireless LAN matching the SSID of the Wireless 3-in-1 Companion in AP/Router mode.
   - The default SSID for AP/Router mode is `default_Router`
   - If necessary, configure your PC's wireless interface to match the settings of the Wireless 3-in-1 Companion's AP/Router mode.
   - You can check the status of your PC's wireless interface to see that your PC has obtained an IP address. If it has, then the Wireless connection to the Wireless 3-in-1 Companion is working correctly.
5. You should now be able to access the LAN or WAN.
   If you can't, you can connect to the Wireless 3-in-1 Companion (while still in AP/Router mode) to check its status and configuration.

Connecting in AP/Router Mode

1. Start your Web browser
2. In the "Location" or "Address", enter "HTTP://" and the current IP address for the Wireless LAN, as set on the *AP/Router* screen. The default value is 192.168.0.1:
   `HTTP://192.168.0.1`
3. If the password has been set (by default, it is blank), you will be prompted for the username and password.
   - Enter `admin` for the user name.
   - Enter the current password.
4. You will then see the ***Mode Configuration*** screen.
   Click the "Configure" button for **AP/Router Mode**.
   You will see a screen like the following.

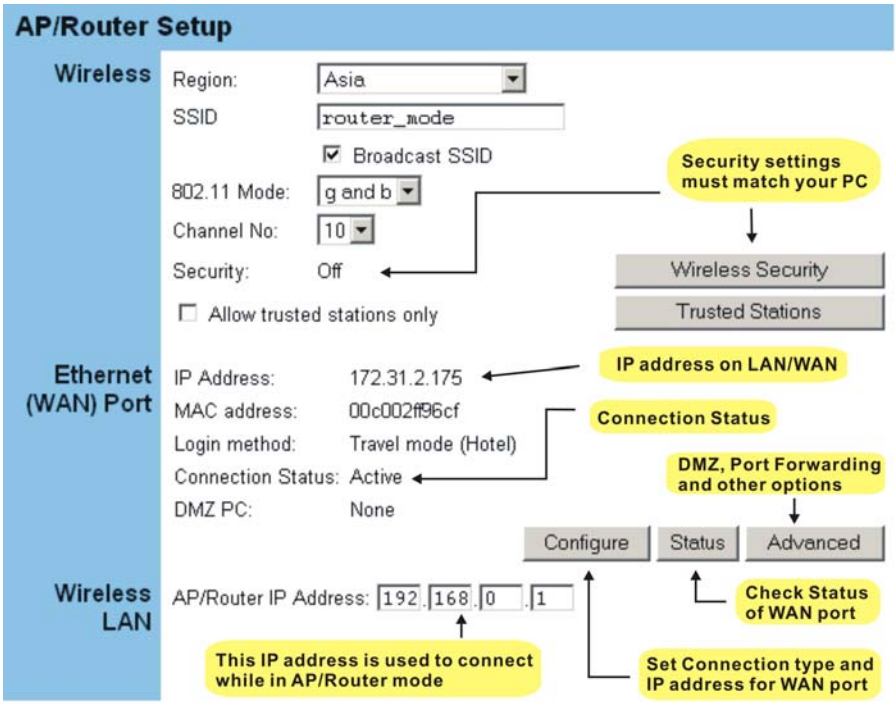


Figure 30: AP/Router Setup (Annotated)

5. Check the Ethernet (WAN) port status and settings.
   - If the Wireless 3-in-1 Companion has not obtained a valid IP address, click the "Configure" button and change the settings as required. Check with the LAN administrator if necessary, to determine the correct settings.
   - If the LAN/WAN is using the same IP address range as the Wireless LAN, you need to change the *Wireless LAN AP/Router IP address* to use a different address range.
   - If the connection is working, but some applications do not function correctly, you may need to change some "Advanced" settings. See Chapter 5 for details of the "Advanced" settings.

Using Client Mode

In client mode, the Wireless 3-in-1 Companion's Ethernet port must be connected to your PC's Ethernet port.

Before using client mode, ensure that the Client Mode configuration is correct.

- Configuration must be performed in Config mode. Admin connections are not possible while in Client mode.
- See Chapter 6 for details of Client mode setup.

If the configuration is correct, the procedure for using client mode is as follows:

1. Use a standard LAN cable to connect the Ethernet port on the Wireless 3-in-1 Companion to your PC.
2. Use the mode selector switch on the side on the Wireless 3-in-1 Companion to select "Client" mode.
3. Wait for the restart to be completed, and the Wireless LED to come On.
4. The Wireless 3-in-1 Companion will then connect, if possible, to the Wireless LAN specified by the current Client Profile.
    - You cannot connect to the Wireless 3-in-1 Companion while in Client Mode. You must specify the desired Wireless LAN using Config mode.
    - In Client Mode, the Wireless 3-in-1 Companion is transparent; it does not have an IP address.
5. You can check the "Properties" of your PC's Ethernet connection to see if it has obtained a valid IP address:
    - If using **Infrastructure** mode (connecting to an Access Point), the IP address must be a valid IP address on the LAN to which the Access Point is connected.
    - If using **Ad-hoc** mode, the IP address should be self-assigned ("Auto-configuration"). If other PCs in the Ad-hoc Wireless LAN behave the same way, everyone will have compatible IP addresses.

Appendix A
Troubleshooting

This Appendix covers the most likely problems and their solutions.

Overview

This chapter covers some common problems that may be encountered while using the Wireless 3-in-1 Companion and some possible solutions to them. If you follow the suggested steps and the Wireless 3-in-1 Companion still does not function properly, contact your dealer for further advice.

General Problems

Problem 1: **Can't connect to the Wireless 3-in-1 Companion to configure it.**

Solution 1: Try using the wired Ethernet connection and the Wireless 3-in-1 Companion's IP address.

1. Connect a LAN cable from the Wireless 3-in-1 Companion to the Ethernet port on your PC.
2. Set the Wireless 3-in-1 Companion to "Config" mode.
3. Restart the Wireless 3-in-1 Companion.
4. 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.)
5. Start your Web browser.
6. Enter the Address as: `HTTP://192.168.0.1`

Wireless Access - AP or AP/Router Mode

Problem 1: **My PC can't locate the Wireless Access Point.**

Solution 1:

- 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 Wireless 3-in-1 Companion.
  Remember that the connection range can be as little as 50 feet in poor environments.

Problem 2: **On my PC, I can locate the Wireless 3-in-1 Companion, but I can't establish a connection.**

Solution 2:

- 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 Wireless 3-in-1 Companion must have the same settings for Wireless security. The default setting for the Wireless 3-in-

1 Companion is disabled, so your wireless station should also have Wireless security disabled.
If Wireless security is enabled on the Wireless 3-in-1 Companion, Wireless stations must use the same settings as the Wireless 3-in-1 Companion.

- If the Wireless 3-in-1 Companion 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 3: **Wireless connection speed is very slow.**

Solution 3: 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:

- Wireless 3-in-1 Companion location.
  Try adjusting the location and orientation of the Wireless 3-in-1 Companion.
- 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 Wireless 3-in-1 Companion.

Router Mode

Problem 1: **When I enter a URL or IP address I get a time out error.**

Solution 1: 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 Wireless 3-in-1 Companion. 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 Wireless 3-in-1 Companion is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.

Problem 2: **Some applications do not run properly when using the Wireless 3-in-1 Companion.**

Solution 2: The Wireless 3-in-1 Companion 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.

Appendix B
About Wireless LANs

This Appendix provides some background information about using Wireless LANs (WLANs).

Modes

Wireless LANs can work in either of two (2) modes:

- Ad-hoc
- Infrastructure

Ad-hoc Mode

Ad-hoc mode does not require an Access Point or a wired (Ethernet) LAN. Wireless Stations (e.g. notebook PCs with wireless cards) communicate directly with each other.

Infrastructure Mode

In Infrastructure Mode, one or more Access Points are used to connect Wireless Stations (e.g. Notebook PCs with wireless cards) to a wired (Ethernet) LAN. The Wireless Stations can then access all LAN resources.

Access Points can only function in "Infrastructure" mode, and can communicate only with Wireless Stations which are set to "Infrastructure" mode.

BSS/ESS

BSS

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).

Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other.

ESS

A group of Wireless Stations, and multiple Access Points, all using the same ID (ESSID), form an Extended Service Set (ESS).

Different Access Points within an ESS can use different Channels. In fact, to reduce interference, it is recommended that adjacent Access Points SHOULD use different channels.

As Wireless Stations are physically moved through the area covered by an ESS, they will automatically change to the Access Point which has the least interference or best performance. This capability is called **Roaming**. (Access Points do not have or require Roaming capabilities.)

Channels

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channel are available. If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference.
- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)
- If using "Ad-hoc" mode (no Access Point), all Wireless stations should be set to use the same Channel. However, most Wireless stations will still scan all Channels to see if there is an existing "Ad-hoc" group they can join.

WEP

WEP (Wired Equivalent Privacy) is a standard for encrypting data before it is transmitted.

This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.

If WEP is used, the Wireless Stations and the Access Point must have the same settings for each of the following:

WEP	Off, 64 Bit, 128 Bit
Key	For 64 Bit encryption, the Key value must match. For 128 Bit encryption, the Key value must match
WEP Authentication	Open System or Shared Key.

Wireless LAN Configuration

To allow Wireless Stations to use the Access Point, the Wireless Stations and the Access Point must use the same settings, as follows:

Mode — On client Wireless Stations, the mode must be set to "Infrastructure". (The Access Point is always in "Infrastructure" mode.)

SSID (ESSID) — Wireless Stations should use the same SSID (ESSID) as the Access Point they wish to connect to. Alternatively, the SSID can be set to "any" or null (blank) to allow connection to any Access Point.

WEP — The Wireless Stations and the Access Point must use the same settings for WEP (Off, 64 Bit, 128 Bit).

WEP Key: If WEP is enabled, the Key must be the same on the Wireless Stations and the Access Point.

WEP Authentication: If WEP is enabled, all Wireless Stations must use the same setting as the Access Point (either "Open System" or "Shared Key").

Appendix C
Specifications

Multi-Function Wireless 3-in-1 Companion

Model	Wireless 3-in-1 Companion
Dimensions	70 mm (W) * 105 mm(D) * 22 mm (H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	1 * 10/100BaseT Ethernet 1 * Wireless Interface
LEDs	3
Power Adapter	5 V DC External

Wireless Interface

Standards	IEEE802.11g WLAN, JEIDA 4.2, roaming support
Frequency	2.4 to 2.4835GHz (Industrial Scientific Medical Band)
Channels	Maximum 14 Channels, depending on regulatory authorities
Modulation	DSSS BPSK/QPSK/CCK, OFDM/CCK
Data Rate	Up to 54 Mbps
Coverage Area	Indoors : 10m @54Mbps, 80m @6Mbps or lower Outdoors : 30m @54Mbps, 200m @6Mbps or lower
Security	WEP 64Bit, WEP 128Bit, WPA-PSK
Output Power	14 dBm +-2(typical)
Receiver Sensitivity	-80 dBm Min.

Regulatory Approvals

CE Standards

This product complies with the 99/5/EEC directives, including the following safety and EMC standards:

- EN300328-2
- EN301489-1/-17
- EN60950

CE Marking Warning

This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.