

Register your product and get support at
www.philips.com/welcome

CAW7740N



EN Wireless Router

PHILIPS

Table of contents		
1	Important	2
1.1	Safety information	2
1.2	Network range & speed information	2
1.3	Conformity	2
1.4	Recycling and disposal	2
1.5	FCC Radiation Exposure Statement	2
1.6	Software licenses	2
1.7	Disclaimer	2
2	Your Wireless Router	3
2.1	What's in the box	3
2.2	What else will you need	3
2.3	Overview of the front side of the wireless router	4
2.4	Overview of the rear side of the wireless router	4
3	Getting started	5
3.1	Install	5
3.2	Connect	5
3.3	Connection overview	6
3.4	Install a WiFi device	6
3.4.1	Install a Wireless USB adapter CCU7740N	6
3.4.2	Install another WiFi device	6
3.5	Install another WPS device	7
3.5.1	via the PIN method	7
3.5.2	via the PBC method	7
3.5.3	via the Manual configuration	7
4	Configuring the Wireless Router	8
4.1	Log on the webpages	8
4.2	Webpages' menu structure	8
4.3	SYSTEM	8
4.3.1	Time zone	8
4.3.2	Password Settings	9
4.3.3	Remote management	9
4.4	WAN	9
4.4.1	Dynamic IP Address	9
4.4.2	PPPoE	9
4.4.3	Static IP Address	10
4.4.4	Clone MAC Address	10
4.4.5	DNS	10
4.5	LAN	10
4.6	WIRELESS	10
4.6.1	Channel and SSID	10
4.6.2	Access control	11
4.6.3	Security	11
4.6.4	WPS	11
4.7	NAT	12
4.7.1	Address Mapping	12
4.7.2	Virtual server	12
4.7.3	Special Applications	13
4.7.4	NAT Mapping Table	13
4.8	FIREWALL	13
4.8.1	Access Control	13
4.8.2	MAC Filter	14
4.8.3	URL blocking	14
4.8.4	Schedule rule	14
4.8.5	Intrusion detection	14
4.8.6	DMZ	15
4.9	UPnP	15
4.10	DDNS	15
4.11	TOOLS	15
4.11.1	Configuration Tools	16
4.11.2	Firmware Upgrade	16
4.11.3	Reset	16
4.12	STATUS	16
4.13	SET UP WIZARD	16
4.13.1	Getting started	16
4.13.2	Time zone	17
4.13.3	Wireless settings	17
4.13.4	Connection type settings	17
5	Technical data	18
6	Frequently asked questions	19

1 Important

Take time to read this user manual before you use your Wireless Router. It contains important information and notes regarding your Wireless Router.

1.1 Safety information

Warning

- This equipment must only be powered with the Power Adapter provided in the box.
- For use only with power supply "Leader: MU12-2120100-C5" and/or "Jentec: AH1212-E".
- Always use the cables provided with the product.
- Radio equipment for wireless applications is not protected against disturbance from other radio services.
- Do not expose the system to excessive moisture, rain, sand or heat sources.
- The product should not be exposed to dripping or splashing.
- No object filled with liquids, such as vases, should be placed on the product.
- Keep the product away from domestic heating equipment and direct sunlight.
- Allow a sufficient amount of free space all around the product for adequate ventilation.
- Do not open this product. Contact your ISP/cable provider helpdesk.

1.2 Network range & speed information

- The environment: Radio signals can travel further outside of buildings, and if the wireless components are in direct line of sight to one another. Putting wireless components in high places helps avoid physical obstacles and provides better coverage.
- Building construction such as metal framing and concrete or masonry walls and floors will reduce radio signal strength. Avoid putting wireless components next to large solid objects; or next to large metal object such as computers, monitors, and appliances.
- Wireless signal range, speed, and strength can be affected by interference from neighbouring wireless networks and devices. Electro-magnetic devices such as televisions, radios, microwave ovens, and cordless phones, especially those with frequencies in the 2.4GHz range, may also interfere with wireless transmission.
- Standing or sitting too close to wireless equipment can also affect radio signal quality.
- Adjusting the antenna: Do not place antennas next to large pieces of metal, because this might cause interference.

1.3 Conformity

We, Philips declare that the product is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. You can find the Declaration of Conformity on www.p4c.philips.com.

Following this Directive, this product can be brought into service in the following states:

B ✓	DK ✓	E ✓	GR ✓	F ✓
IRL ✓	I ✓	L ✓	NL ✓	A ✓
P ✓	SU ✓	S ✓	UK ✓	N ✓
D ✓	CH ✓	TR ✓		

1.4 Recycling and disposal

Disposal instructions for old products:

The WEEE directive (Waste Electrical and Electronic Equipment Directive ; 2002/96/EC) has been put in place to ensure that products are recycled using best available treatment, recovery and recycling techniques to ensure human health and high environmental protection. Your product is designed and manufactured with high quality materials and components, which can be recycled and reused.

Do not dispose of your old product in your general household waste bin.

Inform yourself about the local separate collection system for electrical and electronic products marked by this symbol.



Use one of the following disposal options:

- Dispose of the complete product (including its cables, plugs and accessories) in the designated WEEE collection facilities.
- If you purchase a replacement product, hand your complete old product back to the retailer. He should accept it as required by the WEEE directive.

Packaging information:

Philips has marked the packaging with standard symbols designed to promote the recycling and appropriate disposal of any waste.

 A financial contribution has been paid to the associated national recovery & recycling system.

 The labeled packaging material is recyclable.

1.5 FCC Radiation Exposure Statement

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

1.6 Software licenses

This product contains open source software packages. An overview of these packages, the licences and/or notices that apply to them, and the source code for a number of these packages are available in the on-line product documentation, which is visible on www.p4c.philips.com.

1.7 Disclaimer

This product is provided by "Philips" "as is" and without any express or implied warranty of any kind of warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed.

In no event shall Philips be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services ; loss of information, data, or profits ; or business interruption) howsoever caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of inability to use this product, even if advised of the possibility of such damages. Philips further does not warrant the accuracy or completeness of the information, text, graphics, links or other items transmitted by this product.

2 Your Wireless Router

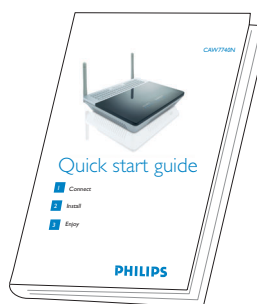
Congratulations on your purchase and welcome to Philips!

To fully benefit from the support that Philips offers, register your product at www.philips.com/welcome.

2.1 What's in the box



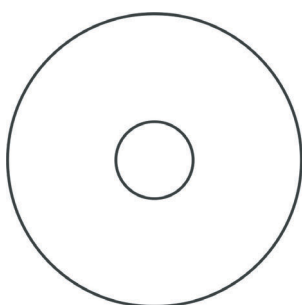
Wireless Router



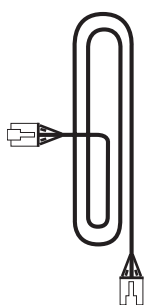
Quick start guide



Power adapter



Installation CDRom



Ethernet cable
(RJ-45)

2.2 What else will you need



A desktop or a laptop with free
USB port and an Ethernet
connector



A modem

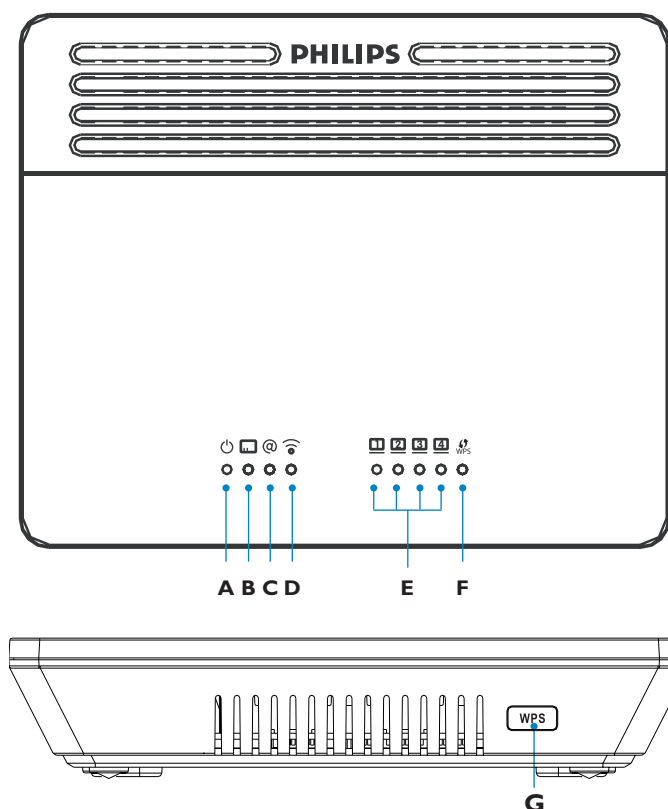


A web browser



An Internet connection

2.3 Overview of the front side of the wireless router



A

ON: Power on, normal operation
OFF: Power off or failure

B

ON: WAN connection is OK
Blinking: Send/Receive data
OFF: Connection is not established

C

ON: Internet connection is up
Blinking: Data transferring
OFF: Internet connection is down or failure

D

ON: Wireless link is up
Blinking: Send/Receive data
OFF: Wireless disable or failure

E

ON: Ethernet connection is established
Blinking: Send/Receive data
OFF: Connection is not established

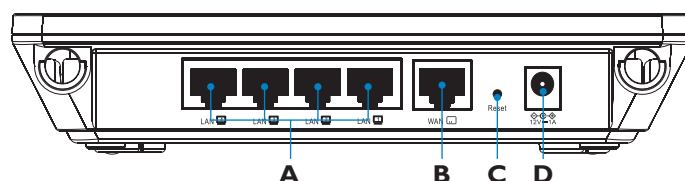
F

ON: Success
Flash Flash: In progress
Blinking: Fail
OFF: No connection

G button

Push and hold this button for 3 seconds to install another WPS device on your network, see 4.6.4.

2.4 Overview of the rear side of the wireless router



A LAN ports

10/100 Ethernet ports (RJ-45). Connect devices to your local area network on these ports (i.e., a PC, hub, or switch)

B WAN port

Connect your modem to this port

C Reset button

Use this button to reset the power and restore the default factory settings. To reset without losing configuration settings, see 4.11.3

D Power Inlet

Connect the included power adapter to this inlet

Warning

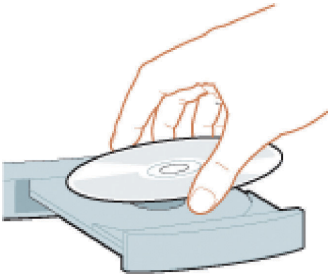
Using the wrong type of power adapter may damage the Wireless Router.

For use only with power supply "Leader: MU12-2120100-C5" and/or "Jentec: AH1212-E".

3 Getting started

3.1 Install

- 1 Insert the installation CD into the PC's CDROM (or DVDROM) drive



- The installation program will start automatically

- 2 Follow instructions on the screen

Note

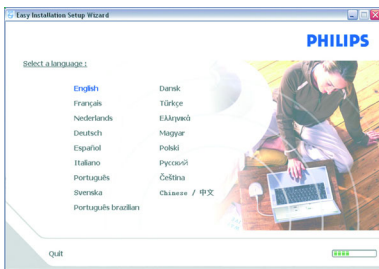
If for some reason the installation does not start automatically:

- 1 Click on Windows **START** and then **RUN**
- 2 Type **explorer** and navigate to the CD ROM (or DVDROM) drive
- 3 Double-click on **Setup.exe**

Tip

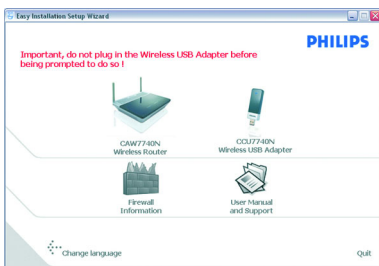
By default, the language of your operating system will be chosen, but you have 10 seconds if you want to select another one.

- 3 Click on the required language



- The next screen will be displayed automatically

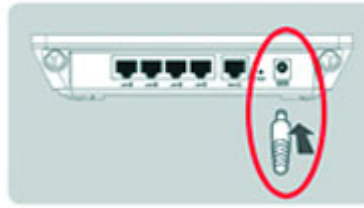
- 4 Click on the picture of the CAW7740N Wireless Router



- The next screen will be displayed automatically

3.2 Connect

- 1 Connect the supplied power adapter to the 12V=1A port



- 2 Connect the power adapter to the electricity supply socket



- Power light will turn on

- 3 If your computer is already connected via Ethernet, then disconnect this cable from your computer



- 4 Connect this Ethernet cable to the WAN port on the CAW7740N



- WAN light will turn on

- 5 Take the Ethernet cable provided in the box



- 6 Connect this Ethernet cable to the LAN1 port



7 Connect the other side of this Ethernet cable to your computer

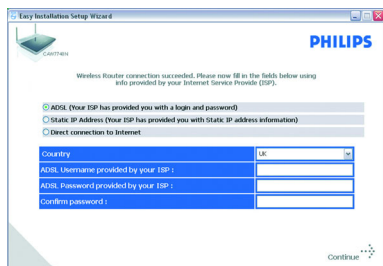


- light will turn on

Note

Depending on your modem settings, you might have the following screen displayed

8 Fill in the fields using the information provided by your Internet Service Provider (ISP)



9 Then click on **Continue**

- A progress bar screen will be displayed, your settings will be saved and you will be connected to Internet
- Once the installation completed, the following screen will be displayed



Note

This screen is the Philips support site. It is a live Internet page, subject to change. The screen displayed may differ from the one shown.

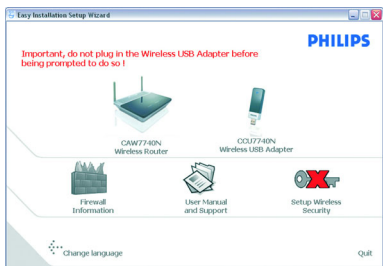
10 Click on **Menu** if you want to go back to the menu screen

Tip

Your WiFi network is running but not secured

11 Click on **Menu** if you want to go back to the menu screen

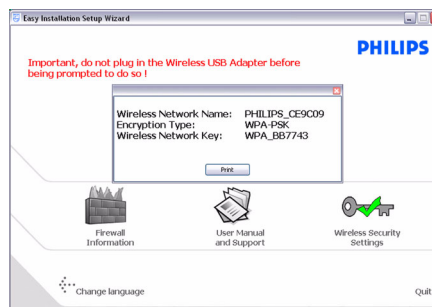
12 Click on **Set Encryption**



- Your WiFi network will be secured by generating automatically an encryption key and a network name (SSID)

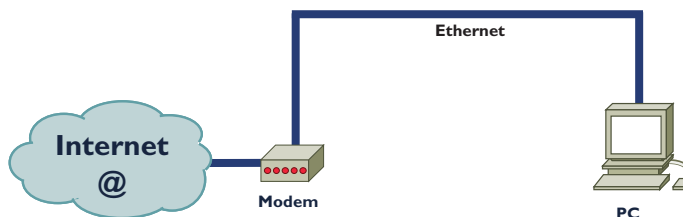
Note

At any time you can retrieve your wireless security settings using your installation CDROM on the computer where you installed your gateway and by clicking on the security icon of the menu page.

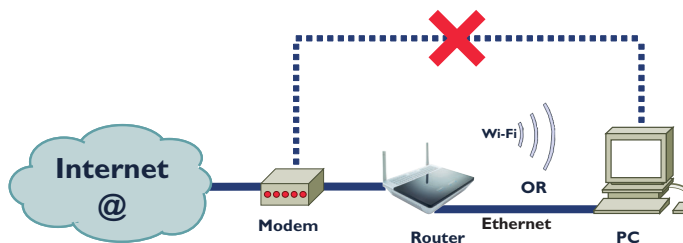


3.3 Connection overview

Your connection before the installation of the router:



Your connection after the installation of the router:



3.4 Install a WiFi device

If you want to install a WiFi device you have to retrieve your wireless security settings using your installation CDROM on the computer where you installed your gateway and by clicking on the security icon of the menu page.

3.4.1 Install a Wireless USB adapter CCU7740N

If you have bought the starter kit CKW7740N, the Wireless USB adapter CCU7740N is part of the box content. In that case you just have to insert the installation CDROM, provided with your CKW7740N, and follow the instructions on the screen. You can either install your Wireless USB adapter on the same PC than the Wireless Router or on another PC.

3.4.2 Install another WiFi device

1 Refer to the manual of the other WiFi device

Note

If you have previously secured your network (see 3.2 step 12) through the easy installation, the name of your network (SSID) will be "PHILIPS_XXXXXX".

If not secured previously through the easy installation, the SSID will be "philips_install".

In case you have given another name to your network, bear in mind that this name will be displayed instead of the "PHILIPS_XXXXXX" or "philips_install".

Note

At any time you can retrieve your wireless security settings using your installation CDROM on the computer where you installed your gateway and by clicking on the security icon  of the menu page.

3.5 Install another WPS device

You can install another WPS device on your network in any of the three following ways:

3.5.1 via the PIN method

- 1** Check that your Wireless router and that the other WPS device are connected and ON
- 2** On your Internet Browser, enter `http://192.168.1.2` in the address field and click on **GO** to access the webpages
- 3** Click on the **WIRELESS** tab on the left side of the page and select **PIN** to open the corresponding subpage
- 4** Enter the PIN from the client device (the other WPS device) and click **START PIN**
 - *The other WPS device is installed on your network*

3.5.2 via the PBC method

- 1** Check that your Wireless router and that the other WPS device are connected and ON
- 2** Push and hold the WPS button, located on the front side on your router, for 3 seconds
- 3** Push and hold the WPS button of the other WPS device for 3 seconds (refer to the manual of the other WPS device for location)
 - *The other WPS device is installed on your network*

OR

- 1** Check that your Wireless router and that the other WPS device are connected and ON
- 2** On your Internet Browser, enter `http://192.168.1.2` in the address field and click on **GO** to access the webpages
- 3** Click on the **WIRELESS** tab on the left side of the page and select **PBC** to open the corresponding subpage
- 4** Click on **START PBC**
 - *The other WPS device is installed on your network*

Note

The push and hold procedure on the two WPS buttons (router and other WPS device) has to be done within a two minutes' interval.

3.5.3 via the Manual configuration

This method enables you to configure client devices without WPS function.

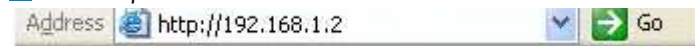
- 1** On your Internet Browser, enter `http://192.168.1.2` in the address field and click on **GO** to access the webpages
- 2** Click on the **WIRELESS** tab on the left side of the page and select **Manual** to open the corresponding subpage
- 3** Take note of the settings displayed and configure your non-WPS device accordingly
 - *Your non-WPS device is installed on your network*

4 Configuring the Wireless Router

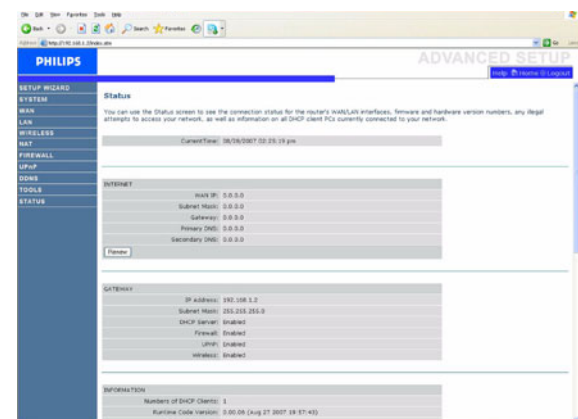
Advanced users may want to change the configuration of their Wireless Router. This chapter explains how to access the configuration webpages, show you the structure of these webpages and it describes them.

4.1 Log on the webpages

- 1 Open your Internet Browser
- 2 Enter `http://192.168.1.2` in the address field



- 3 Click on **GO**
 - The following webpage will be displayed



Note

The only default language is English.

- 4 To access the required webpage, click on the corresponding tab on the left side of the page.

4.2 Webpages' menu structure

The table below describes the menu tree of the webpages.

SET UP WIZARD	Getting started
	Time zone
	Wireless settings
	Connection Type Settings
	Dynamic IP

Note

It is highly recommended to use the Easy Install program available on the provided CDROM instead of the SET UP WIZARD pages

SYSTEM	Time zone
	Password Settings
	Remote Management

WAN	Dynamic IP Address
	PPPoE
	Static IP Address
	Clone MAC Address
	DNS

LAN	
------------	--

WIRELESS	Channel and SSID
	Access control
	Security
	WEP
	WPA
	802.1X
	WPS
	PIN
	PBC
	Manual

NAT	Address Mapping
	Virtual Server
	Special Applications
	NAT Mapping Table

FIREWALL	Access Control
	MAC Filter
	URL blocking
	Schedule rule
	Intrusion Detection
	DMZ

UPnP	
-------------	--

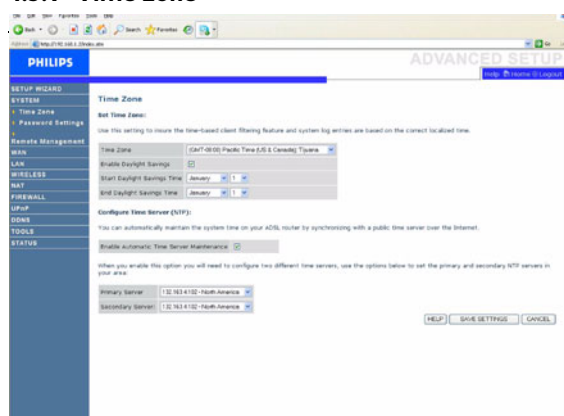
DDNS	
-------------	--

TOOLS	Configuration Tools
	Firmware Upgrade
	Reset

STATUS	
---------------	--

4.3 SYSTEM

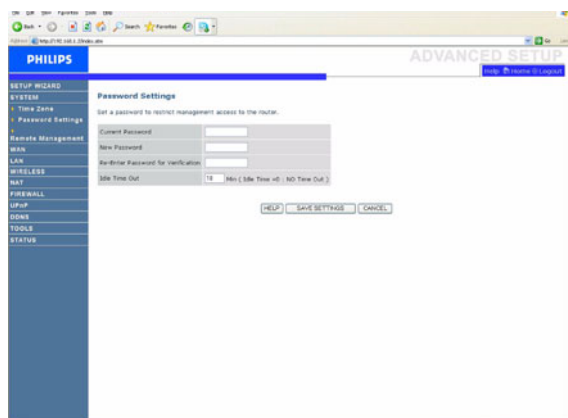
4.3.1 Time zone



Select your local time zone from the drop down list. This information is used for log entries and client filtering.

If you want to automatically synchronize the Wireless Router with a public time server, check the box to Enable Automatic Time Server Maintenance. Select the desired servers from the drop down menu.

4.3.2 Password Settings



Use this page to change the password for accessing the management interface of the Wireless Router.

Passwords can contain from 3-12 alphanumeric characters and are case sensitive.

Note

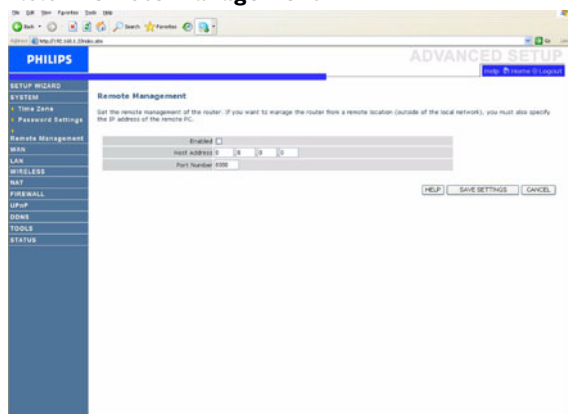
If you lost the password, or you cannot gain access to the user interface, press the reset button on the rear panel, holding it down for at least five seconds to restore the factory defaults. By default, there is no password to login to the user interface.

Warning

When you reset the Wireless Router using the reset button, all configuration settings will be lost, also your ISP setting (Internet Service Provider).

Enter a maximum Idle Time Out (in minutes) to define a maximum period of time for which the login session is maintained during inactivity. If the connection is inactive for longer than the maximum idle time, it will perform system logout, and you have to log in again to access the management interface. (Default: 10 minutes)

4.3.3 Remote management



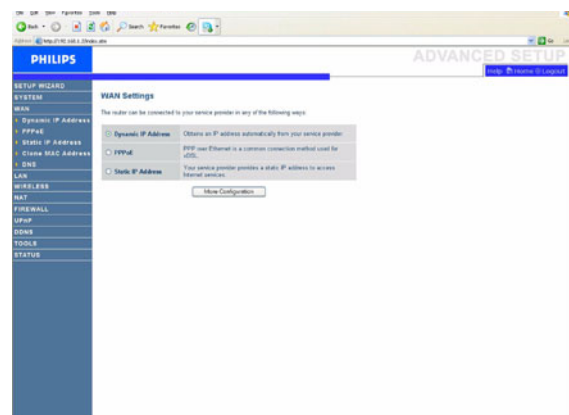
By default, management access is only available to users on your local network. However, you can also manage the Wireless Router from a remote host by entering the IP address of a remote computer on this screen. Check the Enabled check box, and enter the IP address of the Host Address and click "SAVE SETTINGS".

Note

If you check Enable and specify an IP address of 0.0.0.0, any remote host can manage the Wireless Router.

For remote management via WAN IP address you need to connect using port 8080. Simply enter WAN IP address followed by :8080, for example, 212.120.68.20:8080.

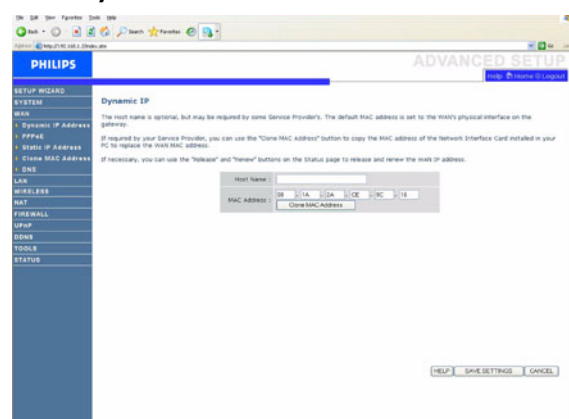
4.4 WAN



The router can be connected to your Internet Service Provider (ISP) in any of the following ways:

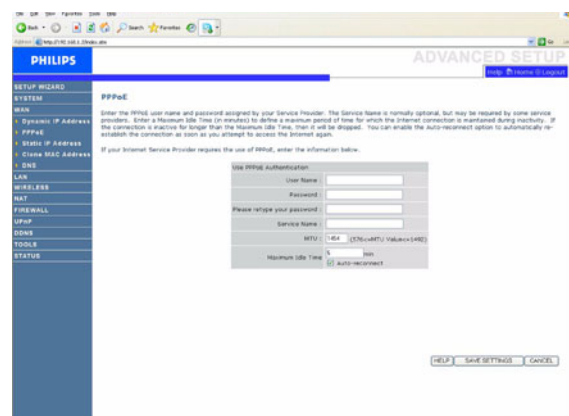
- Dynamic IP Address
- PPPoE
- Static IP address

4.4.1 Dynamic IP Address



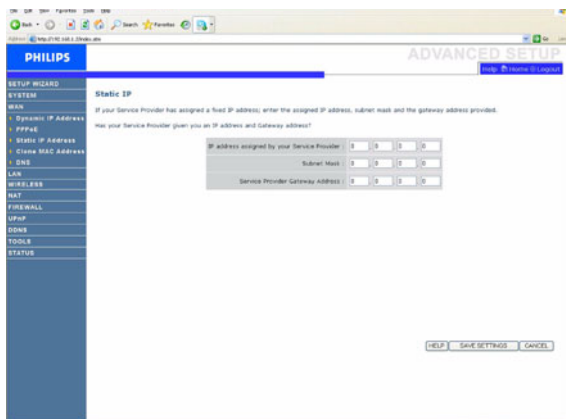
This page allows you to obtain an IP address automatically from your Service Provider.

4.4.2 PPPoE



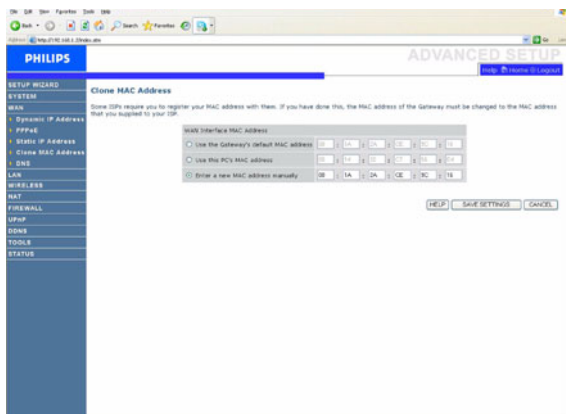
PPPoE is a common connection method used for xDSL.

4.4.3 Static IP Address



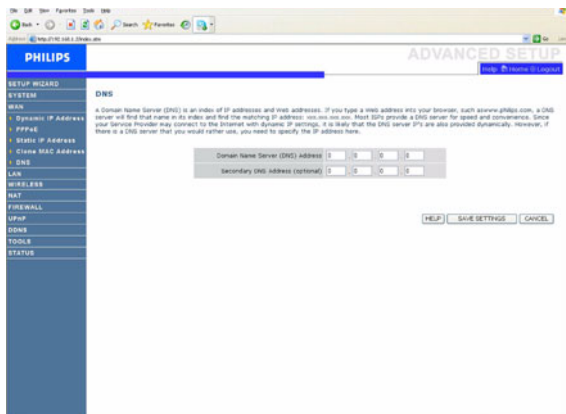
Your ISP provides a static IP address to access Internet services.

4.4.4 Clone MAC Address



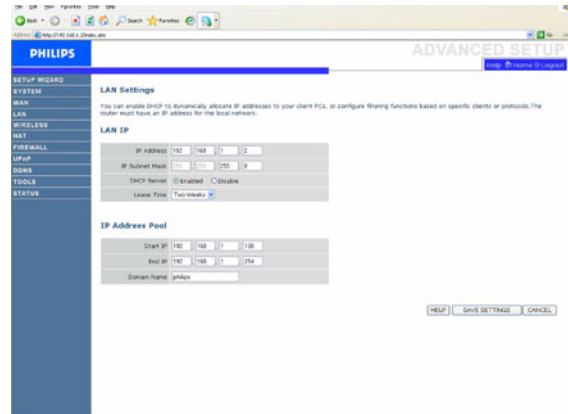
Some ISP's require you to register your MAC address with them. If you have done this, the MAC address of the router must be changed to the MAC address that you supplied to your ISP.

4.4.5 DNS



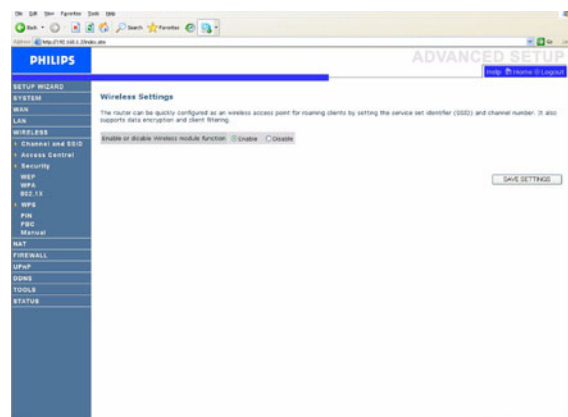
Domain Name Servers (DNS) are used to map a domain name (e.g., www.philips.com) with the IP address (e.g., 64.147.25.20). The DNS address is usually configured automatically. If this is not the case, one or more DNS address will be provided to you by your ISP. However, if there is a DNS server that you would rather use, you need to specify the IP address here.

4.5 LAN



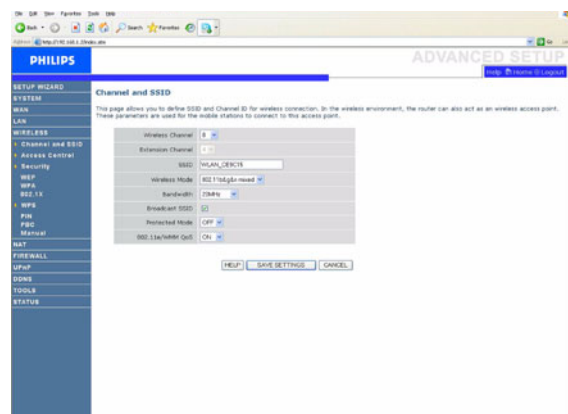
You can enable DHCP to dynamically allocate IP addresses to your client PCs, or configure filtering functions based on specific clients or protocols. The router must have an IP address for the local network.

4.6 WIRELESS



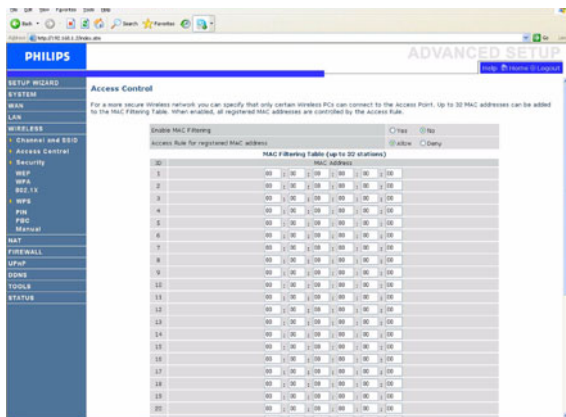
The router can be quickly configured as a wireless access point for roaming clients by setting the service set identifier (SSID) and channel number. It also supports data encryption and client filtering. Check the box to enable the wireless module function.

4.6.1 Channel and SSID



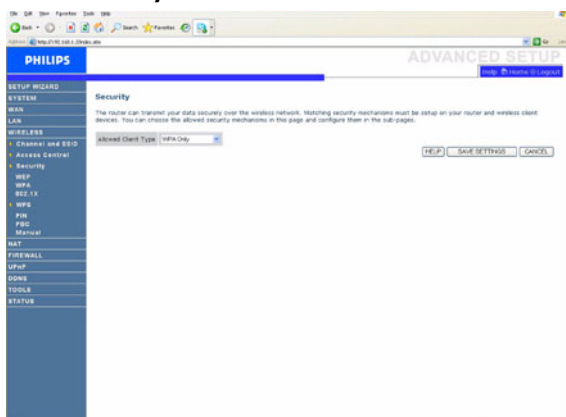
You must specify a common radio channel and SSID (Service Set ID) to be used by the Wireless Router and all of its wireless clients. Make sure you configure all of its clients to the same values.

4.6.2 Access control



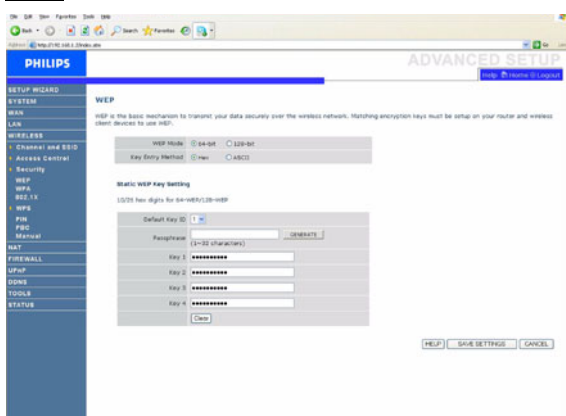
Access Control allows users to define the outgoing traffic permitted or not-permitted through the WAN interface. The default is to permit all outgoing traffic.

4.6.3 Security



The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages.

WEP



If you use WEP to protect your wireless network, you need to set the same parameters for the Wireless Router and all your wireless clients.

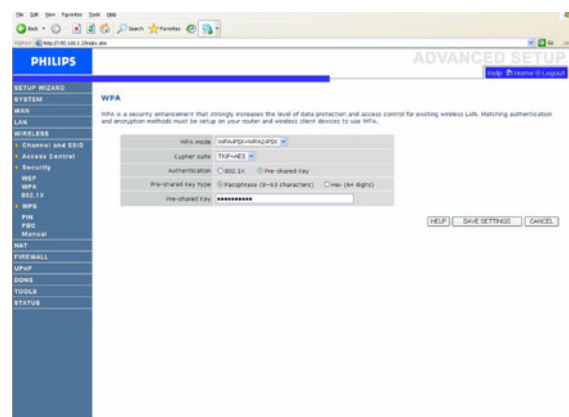
You may automatically generate encryption keys or manually enter the keys. To generate the key automatically with passphrase, check the Passphrase box, enter a string of characters. Select the default key from the drop down menu. Click "SAVE SETTINGS".

Note

The passphrase can consist of up to 32 alphanumeric characters.

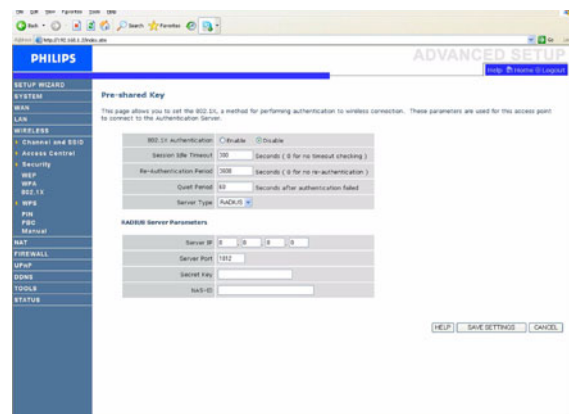
To manually configure the encryption key, enter five hexadecimal pairs of digits for each 64-bit key, or enter 13 pairs for the single 128-bit key. (A hexadecimal digit is a number or letter in the range 0-9 or A-F). Note that WEP protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network or over the Internet.

WPA



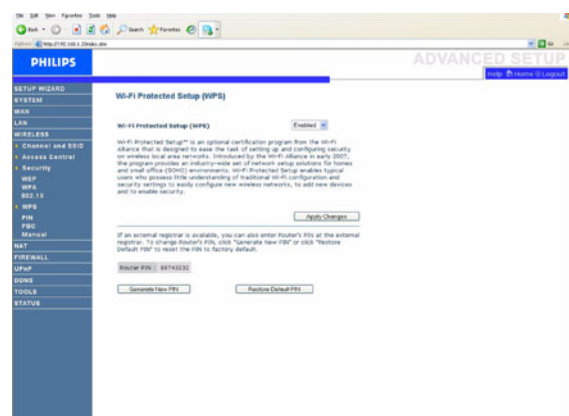
Wi-Fi Protected Access (WPA) combines temporal key integrity protocol (TKIP) and 802.1x mechanisms. It provides dynamic key encryption and 802.1x authentication service.

802.1X



If 802.1x is used in your network, then you should enable this function for the Wireless Router. These parameters are used for the Wireless Router to connect to the authentication server.

4.6.4 WPS

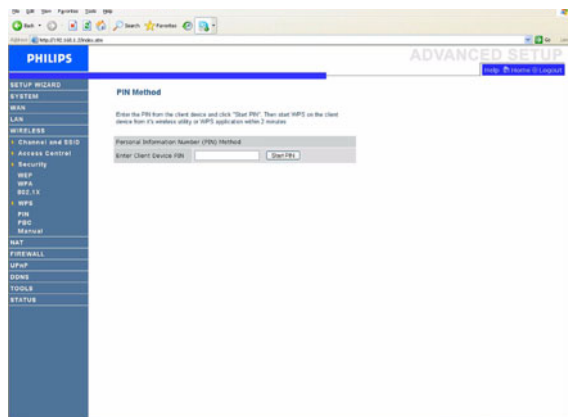


Wi-Fi Protected Setup (WPS) enables typical users who possess little understanding of traditional Wi-Fi configuration and security settings to easily configure new wireless networks, to add new devices and to enable security.

WPS can be done in any of the following ways:

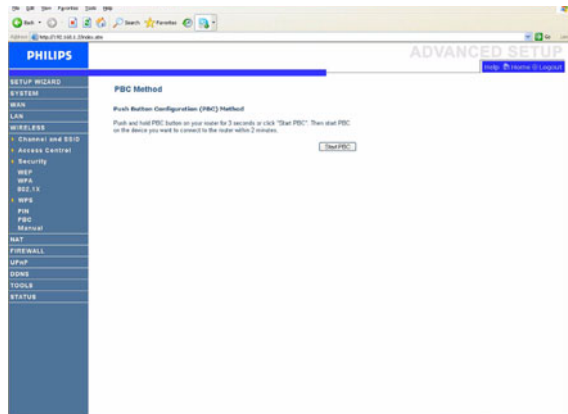
- PIN method
- PBC method
- Manual method

PIN



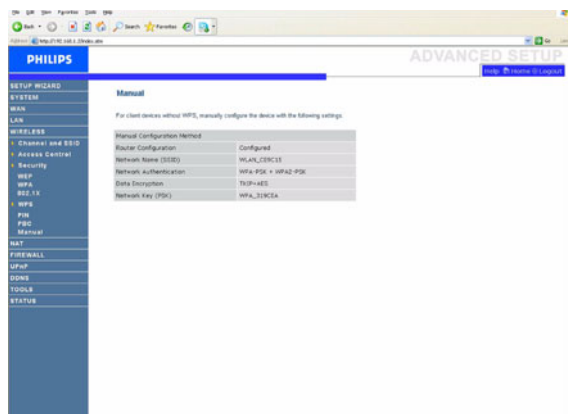
Enter the PIN from the client device and click **Start PIN**.

PBC



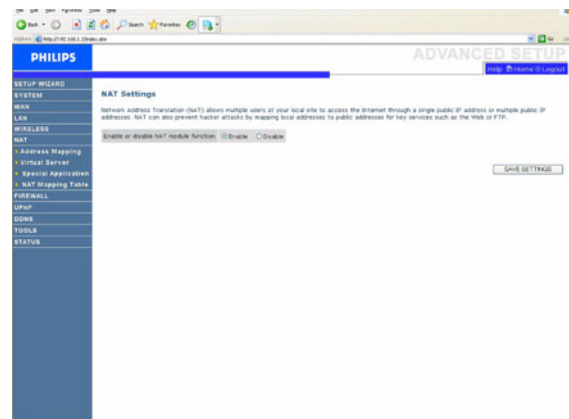
Push and hold the WPS button, located on the front side on your router, for 3 seconds or click **Start PBC**

Manual



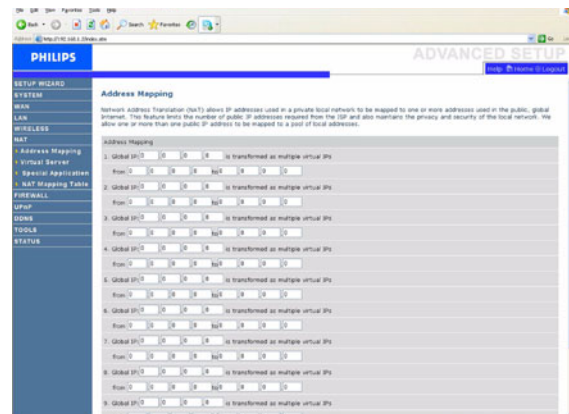
This method enables you to configure client devices without WPS function.

4.7 NAT



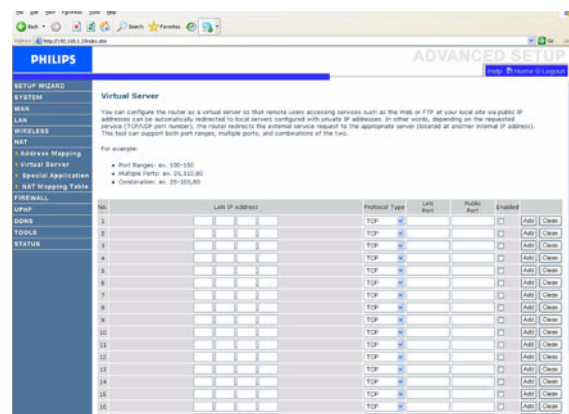
Network Address Translation allows multiple users to access the Internet sharing one public IP. Check the box to enable the NAT module function.

4.7.1 Address Mapping



Allows one or more public IP addresses to be shared by multiple internal users. This also hides the internal network for increased privacy and security. Enter the Public IP address you wish to share into the Global IP field. Enter a range of internal IPs that will share the global IP into the "from" field.

4.7.2 Virtual server

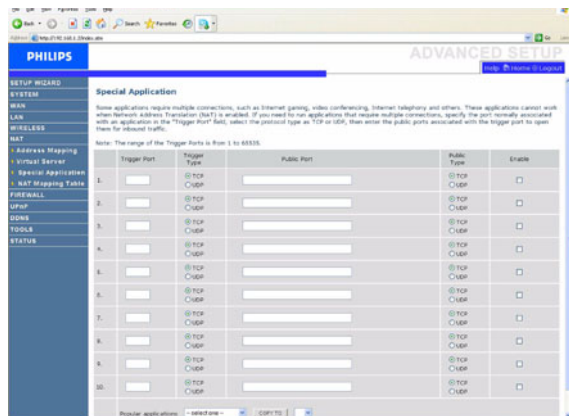


If you configure the Wireless Router as a virtual server, remote users accessing services such as web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the Wireless Router redirects the external service request to the appropriate server (located at another internal IP address).

For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.2.2/80, then all HTTP requests from outside users will be transferred to 192.168.2.2 on port 80. Therefore, by just entering the IP address provided by the ISP, Internet users can access the service they need at the local address to which you redirect them.

A list of ports is maintained at the following link:
<http://www.iana.org/assignments/ports-numbers>

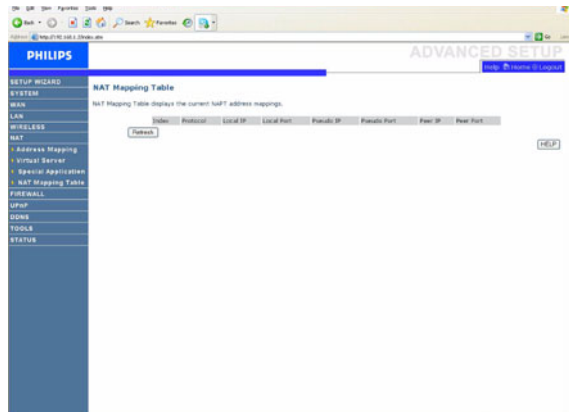
4.7.3 Special Applications



Some applications require multiple connections, such as Internet gaming, video-conferencing, and Internet telephony.

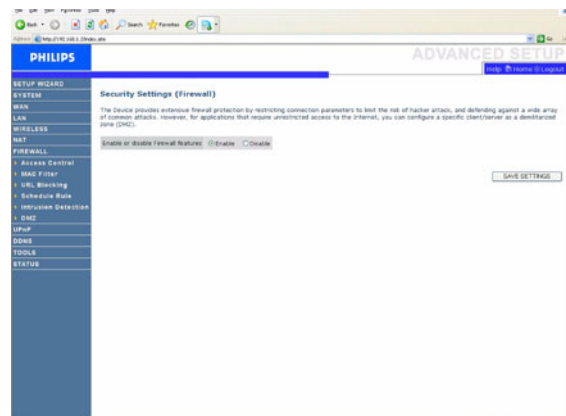
These applications may not work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, use these pages to specify the additional public ports to be opened for each application.

4.7.4 NAT Mapping Table



This page displays the current NAPT (Network Address Port Translation) address mappings.

4.8 FIREWALL



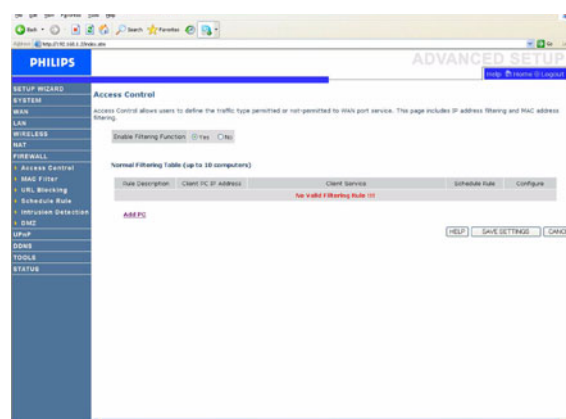
The Wireless Router's firewall inspects packets at the application layer, maintains TCP and UDP session information including time-outs and the number of active sessions, and provides the ability to detect and prevent certain types of network attacks.

Network attacks that deny access to a network device are called Denial-of-Service (DoS) attacks. DoS attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

The Wireless Router firewall function protects against the following DoS attacks: IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.

The firewall does not significantly affect system performance, so we advise leaving it enabled to protect your network. Select Enable and click the "SAVE SETTINGS" button to open the Firewall submenus.

4.8.1 Access Control

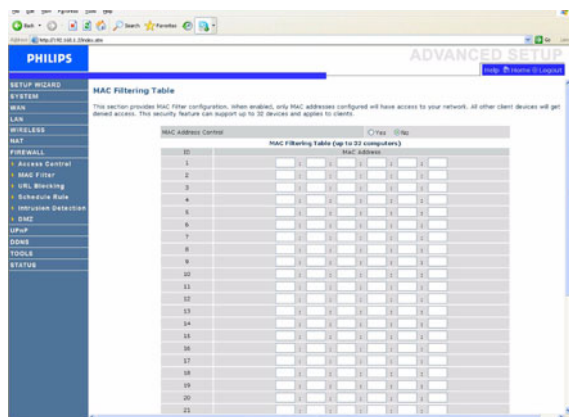


Access Control allows users to define the outgoing traffic permitted or not-permitted through the WAN interface. The default is to permit all outgoing traffic.

To add the PC to the filtering table:

- 1- Click "Add PC" on the Access Control screen
- 2- Define the appropriate settings for client PC services
- 3- Click "OK" and then click "SAVE SETTINGS" to save your settings

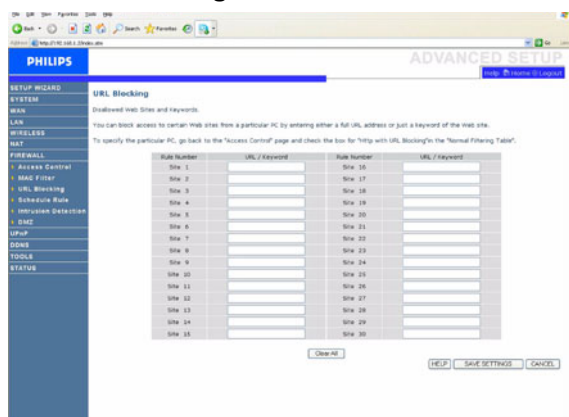
4.8.2 MAC Filter



The Wireless Router can also limit the network access based on the MAC address. The MAC Filtering Table allows the Wireless Router to enter up to 32 MAC addresses that are allowed to access to the WAN port.

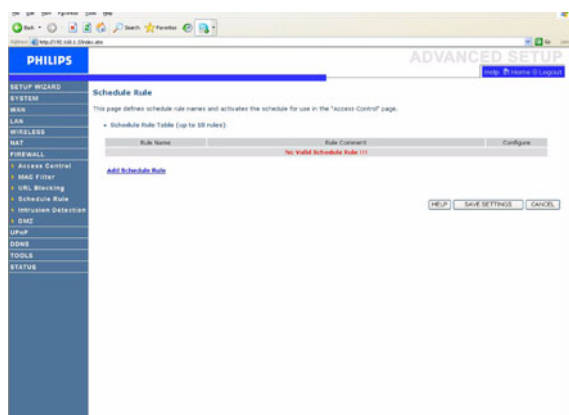
- 1- Click Yes to enable, or No to disable this function
- 2- Enter the MAC address in the space provided and click "Save Settings" to confirm

4.8.3 URL blocking



The Wireless Router allows the user to block access to web sites by entering either a full URL address or just a keyword. This feature can be used to protect children from accessing violent or pornographic web sites.

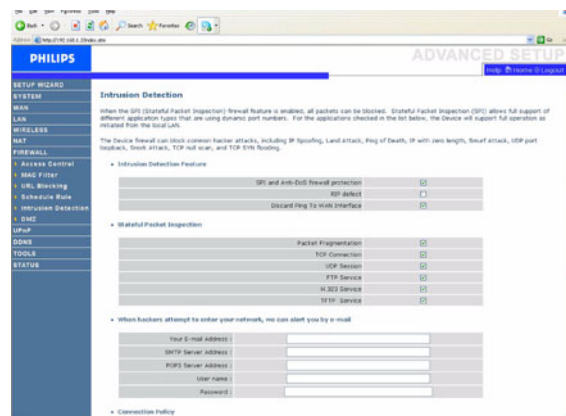
4.8.4 Schedule rule



You may filter Internet access for local clients based on rules. Each access control rule may be activated at a scheduled time. Define the

time schedule on this page, and apply the rule on the Access Control page.

4.8.5 Intrusion detection



Intrusion Detection Feature

Stateful Packet Inspection (SPI) and Anti-DoS firewall protection (Default: Enabled) - The Intrusion Detection Feature of the Wireless Router limits access for incoming traffic at the WAN port. When the SPI feature is turned on, all incoming packets will be blocked except for those types marked in the Stateful Packet Inspection section.

RIP Defect (Default: Disabled) - If an RIP request packet is not acknowledged to by the router, it will stay in the input queue and not be released. Accumulated packets could cause the input queue to fill, causing severe problems for all protocols. enabling this feature prevents the packets from accumulating.

Discard Ping to WAN (Default: Disabled) - Prevent a ping on the Wireless Router's WAN port from being routed to the network.

Scroll down to view more information.

Stateful Packet Inspection

This is called a "Stateful" packet inspection because it examines the contents of the packet to determine the state of the communications; i.e., it ensures that the stated destination computer has previously requested the current communication. This is a way of ensuring that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions. In addition to being more rigorous in their inspection of packets, stateful inspection firewalls also close off ports until connection to the specific port is requested.

When particular types of traffic are checked, only the particular type of traffic initiated from the internal LAN will be allowed. For example, if the user only checks "FTP Service" in the Stateful Packet Inspection section, all incoming traffic will be blocked except for FTP connections initiated from the local LAN.

Stateful Packet Inspection allows you to select different application types that are using dynamic port numbers. If you wish to use the Stateful Packet Inspection (SPI) to block packets, click on the Yes radio button in the "Enable SPI and Anti-DoS firewall protection" field and then check the inspection type that you need, such as Packet Fragmentation, TCP Connection, UDP Session, FTP Service, H.323 Service, or TFTP Service.

When hackers attempt to enter your network, the router can alert you by e-mail

If the mail server needs to authenticate your identification before sending out any e-mail, please fill related information in POP3 server, username and password fields. Otherwise leave the three fields blank.

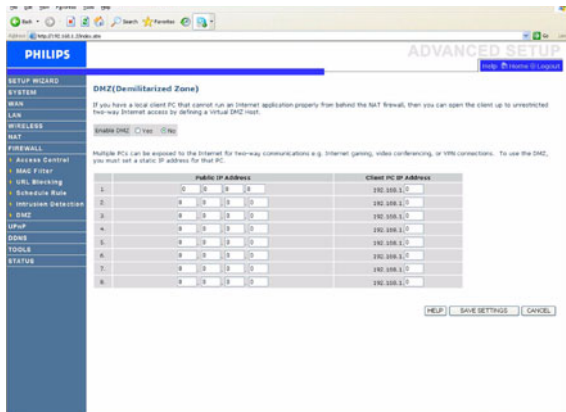
Connection Policy

Enter the appropriate values for TCP/UDP sessions as described in the following table.

Note

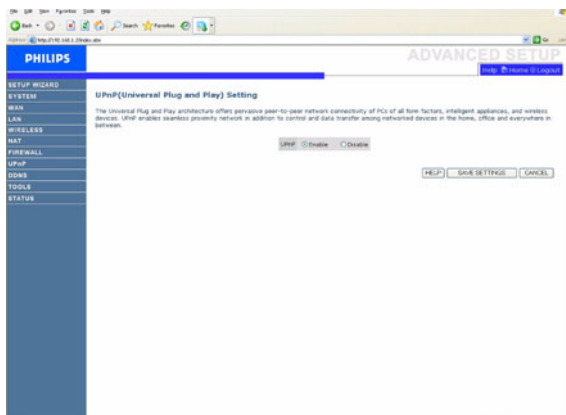
The firewall does not significantly affect system performance, so we advise enabling the prevention features to protect your network.

4.8.6 DMZ



If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. Enter the IP address of a DMZ (Demilitarized Zone) host on this screen. Adding a client to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort.

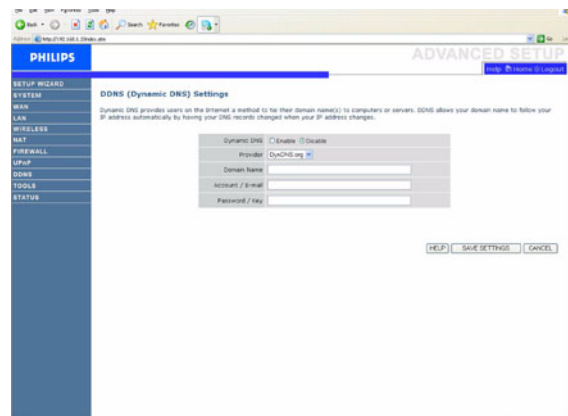
4.9 UPnP



UPNP (Universal Plug and Play) settings

With Universal Plug and Play, a device can automatically join a network, obtain an IP address, communicate its capabilities, and learn about the presence and capabilities of other devices. Devices can then directly communicate with each other. This further enables peer-to-peer networking.

4.10 DDNS



DDNS (Dynamic DNS) settings

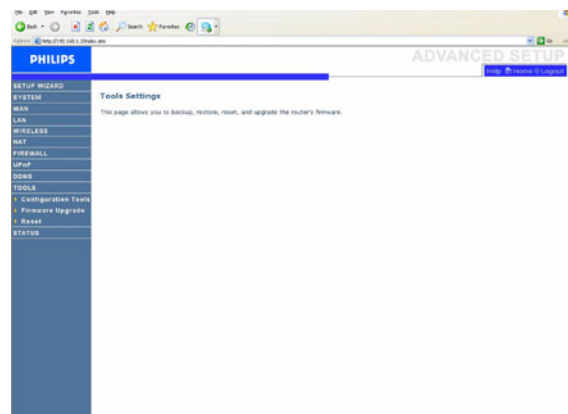
DDNS text "Domain Name" is a series of alphanumeric strings separated by periods that maps to the address of a network connection and identifies the owner of the address.

Dynamic DNS provides users on the Internet with a method to tie their domain name to a computer or server. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

The Server Configuration section automatically opens the TCP port options checked in the Virtual Server section. Simply enter in the IP Address of your server, such as a web server, and then click on the port option HTTP Port 80 so users can access your web server from the Internet connection.

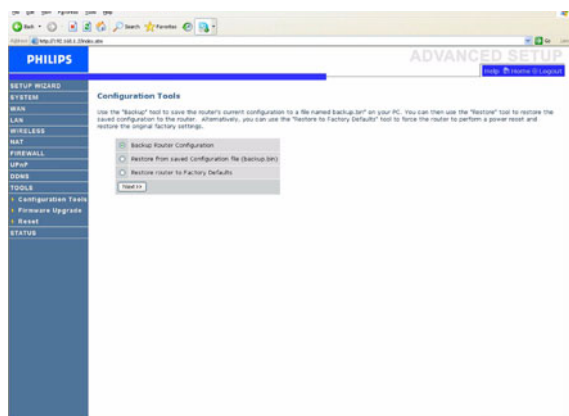
This DNS feature is powered by a DDNS service provider. With a DDNS connection you can host your own web site, email server, FTP site, and more at your own location even if you have a dynamic IP address. (Default: Disable)

4.11 TOOLS



Use the Maintenance menu to backup the current configuration, restore a previously saved configuration, restore factory settings, update firmware, and reset the Wireless Router.

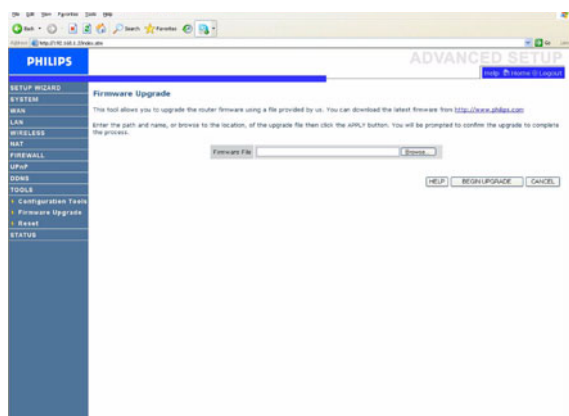
4.11.1 Configuration Tools



Choose a function and click Next>>.

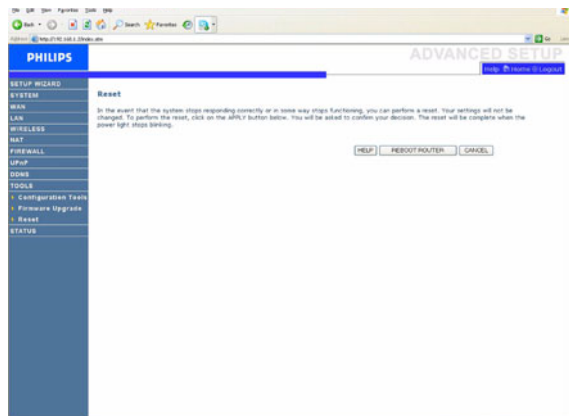
Backup allows you to save the Wireless Router's configuration to a file. Restore can be used to restore the saved backup configuration file. Restore to Factory Defaults resets the Wireless Router to the original settings. You will be asked to confirm your decision.

4.11.2 Firmware Upgrade



Use the Firmware Upgrade screen to update the firmware or user interface to the latest versions. Download the upgrade file from www.philips.com/support (Model CAW7740N), and save it to your hard drive. Then click "Browse..." to look for the downloaded file. Click "BEGIN UPGRADE". Check the Status page Information section to confirm that the upgrade process was successful.

4.11.3 Reset

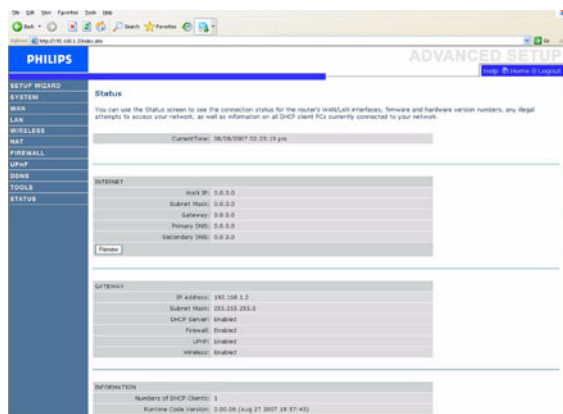


Click "REBOOT ROUTER" to reset the Wireless Router. If you perform a reset from this page, the configuration will not be changed back to the factory default settings.

Note

If you use the Reset button on the rear panel, the Wireless Router performs a power reset. Press the button for over five seconds, and the factory default settings will be restored.

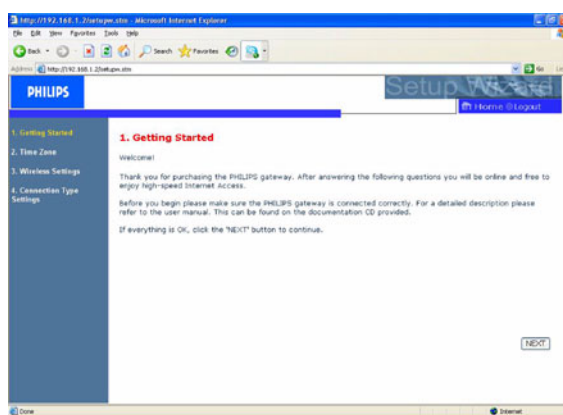
4.12 STATUS



The Status page displays WAN/LAN connection status, firmware, and hardware version numbers, illegal attempts to access your network, as well as information on DHCP clients connected to your network. The security log may be saved to a file by clicking "Save" and choosing a location.

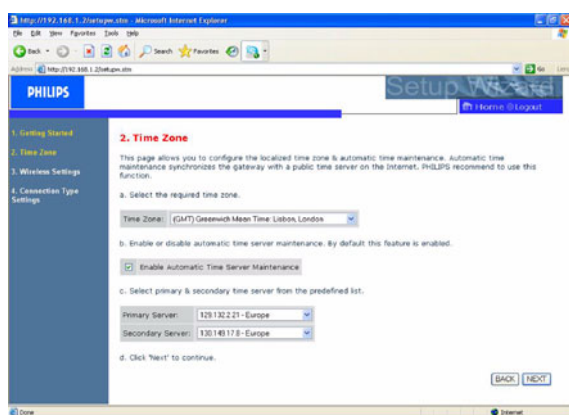
4.13 SET UP WIZARD

4.13.1 Getting started



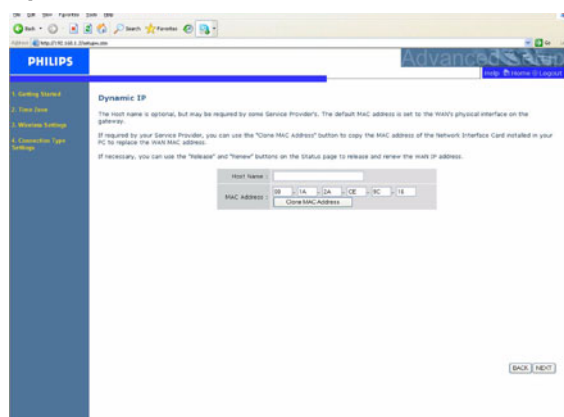
Make sure the router is connected correctly. For a detailed description, refer to the user manual. This can be found on the Installation CD provided.

4.13.2 Time zone



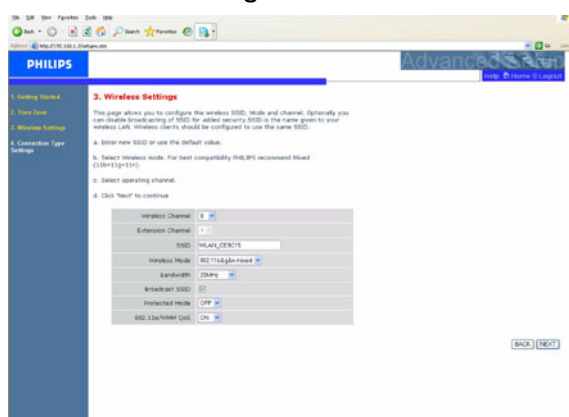
This page allows you to configure the local time zone and automatic time maintenance. Automatic time maintenance synchronizes the router with a public time server on the Internet.

Dynamic IP



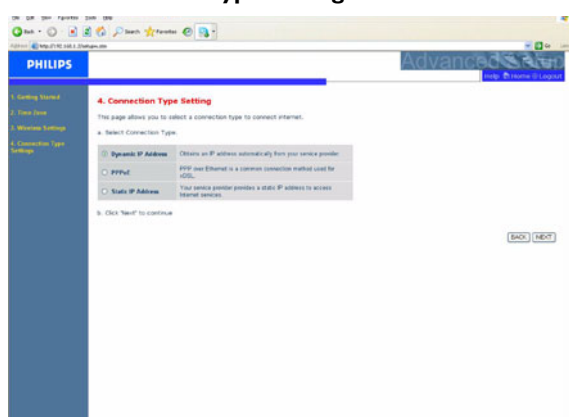
This page allows you to obtain an IP address automatically from your Service Provider.

4.13.3 Wireless settings



In step 2 you can change the Wireless settings of the Wireless Router. For easy installation it is advised to keep the default settings. If you later would like to change any of the wireless settings you can do so via the menu in the Wireless Router.

4.13.4 Connection type settings



This page allows you to select a connection type to connect Internet (see 4.4).

Ports

- Four 10/100Mbps RJ-45 Ports

Management Features

- Firmware upgrade via web based management
- Web based management (configuration)
- Power indicators
- Event and history logging
- Network ping

Security Features

- Password protected configuration access
- User authentication (PAP/CHAP) with PPP
- Firewall NAT NAT
- VPN pass through (IPSec-ESP Tunnel mode, L2TP, PPTP)

Wireless Security

- WEP 64/128 bit
- WPA/WPA2
- WPA/WPA2-Personal (PSK)
- WPA-PSK with TKIP
- WPA2-PSK with AES
- WPA-PSK + WPA2-PSK with TKIP+AES, AES, or TKIP
- WPS: PIN and PBC methods

LAN Features

- IEEE 802.1d (self-learning transparent Bridging)
- DHCP Server
- DNS Proxy
- Static Routing, RIPv1 and RIPv2

Radio Features

- Wireless RF module Frequency Band
 - 802.11n Radio: 2.4GHz
 - 802.11g Radio: 2.4GHz
 - 802.11b Radio: 2.4GHz
- Europe - ETSI
- 2412~2472MHz (Ch1-Ch13)

Modulation Type

- 802.11n Draft-2.0: OFDM (BPSK, QPSK, 16- and 64-QAM)
- 802.11g: OFDM (BPSK, QPSK, 16- and 64-QAM)
- 802.11b: CCK (11 Mbps, 5.5 Mbps), DQPSK (2 Mbps)

Operating Channels IEEE 802.11n

- 13 channels (ETSI)

Operating Channels IEEE 802.11g

- 13 channels (ETSI)

Operating Channels IEEE 802.11b

- 13 channels (Europe)

Transmit Power and Sensitivity

Tx Output Power: (Typical)

- 11b: 18.5 +/- 1 dBm
- 11g: 14.5 +/- 1 dBm@54Mbps
- 11n: 14.5 +/- 1 dBm

Rx Sensitivity: (Typical)

- -84 dBm @ 11 Mbps
- -72 dBm @ 54 Mbps
- -64 dBm @ 64-QAM, 20MHz channel spacing
- -61 dBm @ 64-QAM, 40MHz channel spacing

Environmental

Complies with the following standards:

Temperature: IEC 68-2-14

- 0 to 40 degrees C (Standard Operating)
- -20 to 70 degrees C (non-operation)

Humidity

- 5% to 95% (non-condensing)

IEEE standards

- IEEE 802.3, 802.3u, 802.11g, 802.1d

Standards, Conformance Electromagnetic, Compatibility

- CE, ETS 300 328, ETS 300 836 (Wireless)
- EN50081, EN50082, EN61000-3-2, EN61000-3-3 (EMC)
- Vista, WPS

Safety

- EN60950

6 Frequently asked questions

In this chapter you will find the most frequently asked questions and answers about your Wireless Router.

Set-up

I cannot connect using the Web browser

- Check that you have a valid network connection to your Wireless Router
- Check all parameter settings with your Internet provider
- Check Internet Explorer* configuration:
 - Go to Start and select the Control Panel.
 - In the Control Panel select Internet Options
 - Ensure that **Always dial my default connection** is not ticked*depends on your Web browser

I forgot (or lost) the password. How do I reset my Wireless Router (Factory Defaults) ?

- Make sure the Wireless Router is ON
- Use a pen to push the recessed reset button on the rear panel, holding it down for at least five seconds
- Release the reset button and the Wireless Router restarts

Warning

When you reset the Wireless Router using the reset button, all configuration settings will be lost, also your ISP setting (Internet Service Provider).

A Wireless PC cannot associate with my Wireless Router

- Make sure that the WiFi function of your Wireless Router is enabled
- Make sure the Wireless PC has the same SSID setting as your Wireless Router. See webpage "Channel and SSID".
- You need to have the same security settings on the Wireless PC and your Wireless Router. See "Security".

Product behaviour

The signal does not switch on.

- Make sure that the electrical power supply is plugged into a wall outlet
- Make sure that the coaxial jack of the electrical power supply adapter is plugged into your Wireless Router
- Make sure you are using the correct power supply for your Wireless Router
- However, if your Wireless Router power is OFF after running for a while, check for power loss or overcharge. (If your wall outlet has a switch is it in position ON ?)
- If you still cannot isolate the problem, then the external power supply may be defective. In this case, contact Technical Support for assistance

The signal is OFF.

- Make sure that your Modem Ethernet cable (RJ45) is plugged into the WLAN port of your Wireless Router and to your modem.

The signal is always OFF.

- Confirm with your Internet Service Provider that your Internet service is active
- Confirm your Internet setting with your Internet Service Provider

The signals ... do not switch ON. Cannot ping the Wireless Router from the attached LAN.

- If you are using the Ethernet connection, verify that your TCP/IP is properly installed and configured on your PC.
- Make sure the Ethernet cable (RJ45) is firmly connected to your Wireless Router.

- Make sure you are using the correct cable type for your Ethernet equipment
- Verify that the IP address is properly configured. For most applications, you should use the Wireless Router DHCP function to dynamically assign IP address to hosts on the attached LAN. However, if you manually configure IP address on the LAN, verify that the same network address and subnet mask are used for both the Wireless Router and any attached LAN devices.

The Wireless network is often interrupted.

- Move your Wireless PC closer to the Wireless Router to find a better signal. If the signal is still weak, you can change the angle of the antenna. There may be interference, possibly caused by microwave ovens, a Wireless TV link or wireless phones. Adapt the location of the interference sources or of the Wireless Router.
- You can change the wireless channels on the Wireless Router. See webpage "Channel and SSID".

The Wireless Router is hot.

- This is a normal behaviour
- Make sure to never cover the cooling slots



Copyright © 2007 Koninklijke Philips Electronics N.V.

All rights reserved.

Trademarks are the property of Koninklijke Philips Electronics N.V. or their respective owners.

Specifications are subject to change without notice.

Document order number: 3111 285 40871

