

TP-LINK®

User Guide

TL-WR340G

TL-WR340GD

54Mbps Wireless Router



COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. **TP-LINK®** is a registered trademark of TP-LINK TECHNOLOGIES CO., LTD. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-LINK TECHNOLOGIES CO., LTD. Copyright © 2011 TP-LINK TECHNOLOGIES CO., LTD.

All rights reserved.

<http://www.tp-link.com>

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 or more of the following measures:

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

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- 1) This device may not cause harmful interference.
- 2) This device must accept any interference received, including interference that may cause undesired operation.

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

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. 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."

CE Mark 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.

National Restrictions

2400.0-2483.5 MHz

Country	Restriction	Reason/remark
Bulgaria		General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy		If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation		Only for indoor applications

Note: Please don't use the product outdoors in France.

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: **54Mbps Wireless Router**

Model No.: **TL-WR340G/TL-WR340GD**

Trademark: **TP-LINK**

We declare under our own responsibility that the above products satisfy all the technical regulations applicable to the product within the scope of Council Directives:

Directives 1999/5/EC

The above product is in conformity with the following standards or other normative documents:

ETSI EN 300 328 V1.7.1: 2006

ETSI EN 301 489-1 V1.8.1:2008& ETSI EN 301 489-17 V1.3.2:2008

EN 61000-3-2:2006

EN 61000-3-3:1995+A1:2001+A2:2005

EN60950-1:2006

Recommendation 1999/519/EC

EN62311:2008

Directives 2004/108/EC

The above product is in conformity with the following standards or other normative documents

EN 55022:2006 +A1:2007

EN 55024:1998+A1:2001+A2:2003

EN 61000-3-2:2006

EN 61000-3-3:1995+A1:2001+A2:2005

Directives 2006/95/EC

The above product is in conformity with the following standards or other normative documents

EN60950-1:2006

Person is responsible for marking this declaration:



Yang Hongliang

Product Manager of International Business

CONTENTS

Package Contents	1
Chapter 1. Introduction	2
1.1 Product Overview	2
1.2 Main Features	2
Chapter 2. Hardware Installation	4
2.1 The Front Panel	4
2.2 The Back Panel	5
2.3 System Requirements	5
2.4 Installation Environment Requirements	6
2.5 Connecting the Device	6
2.6 Configure PC	7
Chapter 3. Quick Installation Guide	10
3.1 TCP/IP Configuration	10
3.2 Quick Installation Guide	10
Chapter 4. Software Configuration	15
4.1 Login	15
4.2 Status	15
4.3 Quick Setup	16
4.4 Network	17
4.4.1 WAN	17
4.4.2 LAN	25
4.4.3 MAC Clone	26
4.5 Wireless	26
4.5.1 Wireless Settings	27
4.5.2 Security Settings	29
4.5.3 MAC Filtering	31
4.5.4 Wireless Advanced	33
4.5.5 Wireless Statistics	34
4.6 DHCP	35
4.6.1 DHCP Settings	35
4.6.2 DHCP Clients List	36
4.6.3 Address Reservation	36
4.7 Forwarding	38
4.7.1 Virtual Servers	38

4.7.2	Port Triggering.....	39
4.7.3	DMZ.....	41
4.7.4	UPnP.....	42
4.8	Security.....	43
4.8.1	Firewall.....	43
4.8.2	IP Address Filtering.....	44
4.8.3	Domain Filtering.....	45
4.8.4	MAC Address Filtering.....	47
4.8.5	Remote Management.....	48
4.8.6	Advanced Security.....	49
4.9	Static Routing.....	50
4.10	IP Qos.....	52
4.11	IP & MAC Binding Setting.....	53
4.11.1	Binding Setting.....	53
4.11.2	ARP List.....	54
4.12	Dynamic DNS.....	55
4.12.1	Dyndns.org DDNS.....	55
4.12.2	Oray.net DDNS.....	56
4.12.3	Comexe.cn DDNS.....	57
4.13	System Tools.....	58
4.13.1	Time.....	58
4.13.2	Diagnostic.....	59
4.13.3	Firmware.....	60
4.13.4	Factory Defaults.....	61
4.13.5	Backup & Restore.....	62
4.13.6	Reboot.....	62
4.13.7	Password.....	63
4.13.8	Syslog.....	63
4.13.9	Statistics.....	64
	Appendix A: FAQ.....	65
	Appendix B: Configuring the PC.....	69
	Appendix C: Specifications.....	72
	Appendix D: Glossary.....	73

Package Contents

The following contents should be found in your box:

- One TL-WR340G/TL-WR340GD 54Mbps Wireless Router
- One AC power Adapter for TL-WR340G/TL-WR340GD 54Mbps Wireless Router
- Quick Installation Guide
- One Resource CD for TL-WR340G/TL-WR340GD 54Mbps Wireless Router, including:
 - This Guide
 - Easy Setup Assistant
 - Other Helpful Information

Note:

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact with your distributor.

Conventions

The Router or TL-WR340G/TL-WR340GD, or device mentioned in this User guide stands for TD-WR340G/TL-WR340GD 54Mbps Wireless Router without any explanations.

Parameters provided in the pictures are just references for setting up the product, which may differ from the actual situation.

You can set the parameters according to your demand.

Note:

The two devices of TL-WR340G and TL-WR340GD are shared with this User Guide, we use TL-WR340G for example.

The differences between them are:

- TL-WR340G router with a fixed antenna;
- TL-WR340GD router with a detachable antenna.

Chapter 1. Introduction

Thank you for choosing the TL-WR340G/TL-WR340GD 54Mbps Wireless Router.

1.1 Product Overview

Thank you for choosing the TL-WR340G/TL-WR340GD 54Mbps Wireless Router. This router provides dedicated solution for Small Office/Home Office (SOHO) networks. With your network all connected, your local wired or wireless network can share Internet access, files and fun for multiple PCs through one ISP account. In addition, this device supports Bridge mode which can make two APs communicate with each other wirelessly.

It is an easy Web-based setup for installation and management. Even though you may not be familiar with the router, this guide will make configuring the router easy. Before installing the router, please look through this guide to know all the router's functions.

1.2 Main Features

- Complies with IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u standards.
- 1 10/100M Auto-Negotiation RJ45 WAN port, 4 10/100M Auto-Negotiation RJ45 LAN ports, supporting Auto MDI/MDIX.
- Shares data and Internet access for users, supporting PPPoE, Dynamic IP, Static IP, 802.1X + Dynamic IP, 802.1X + Static IP, BigPond Cable, L2TP, PPTP, Dual Access Internet access.
- Ignores Ping packets from WAN or LAN ports.
- Connecting Internet on demand and disconnecting from the Internet when idle for PPPoE.
- Built-in NAT and DHCP server supporting static IP address distributing.
- Built-in firewall supporting IP address filtering, Domain Name filtering, and MAC address filtering.
- Provides WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security.
- Provides 64/128/152-bit WEP encryption security and wireless LAN ACL (Access Control List).
- Supports Flow Statistics.
- Supports firmware upgrade.
- Supports Web management.
- Supports Virtual Server, Special Application and DMZ host.
- Supports UPnP, Dynamic DNS, Static Routing, VPN Pass-through.
- Supports ICMP-FLOOD, UDP-FLOOD, and TCP-SYN-FLOOD filter.
- Supports 54/48/36/24/18/12/9/6Mbps or 11/5.5/2/1Mbps data transfer rates.

- Supports connecting/disconnecting from the Internet on a specified time of day.
- Supports access control, parents and network administrators can establish restricted access policies based on time of day for children or staff.

Chapter 2. Hardware Installation

2.1 The Front Panel



Figure 2-1

The Router's LEDs are located on the front panel (View from left to right).

LED Explanation:

Name	Status	Indication
PWR	Off	No Power
	On	Power on
SYS	Off	The Router has an error
	On	The Router is initializing
	Flashing	The Router is working properly
WLAN	Off	The Wireless function is disabled
	Flashing	The Wireless function is enabled
WAN/1-4 (LAN)	Off	There is no device linked to the corresponding port
	On	There are devices linked to the corresponding ports but no data transmitted or received.
	Flashing	Sending or receiving data over corresponding port

2.2 The Back Panel

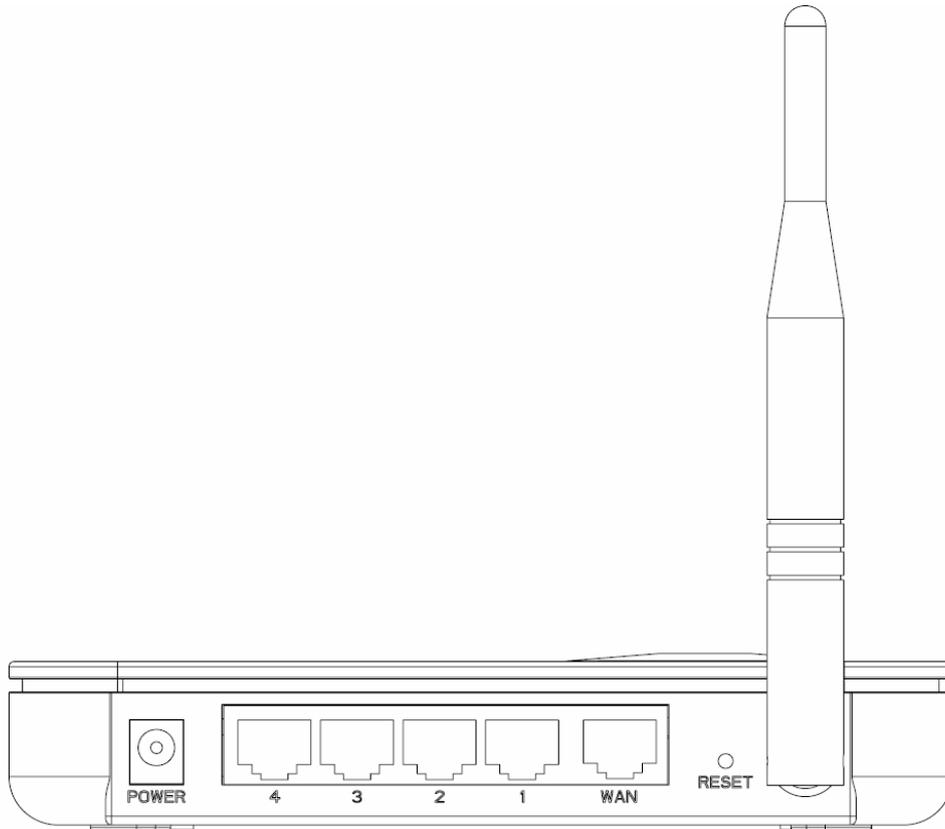


Figure 2-2

The following parts are located on the rear panel (View from left to right).

- **POWER:** The Power plug is where you will connect the power adapter.
- **1, 2, 3, 4 (LAN):** Through these ports, you can connect the Router to your PCs and the other Ethernet network devices.
- **WAN:** RJ45 WAN port for connecting the router to a cable/DSL Modem, or Ethernet.
- **RESET:** There are two ways to reset the Router's factory defaults. With the router powered on, use a pin to press and hold the Reset button until the SYS LED becomes quick-flash from slow-flash (about 5 seconds), and then release the button and wait the router to reboot to its factory default settings, or restore the default setting from "System Tools - Factory Defaults" of the Router's Web-based Utility.
- **Antenna:** Used for wireless operation and data transmit.

2.3 System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable Modem that has an RJ45 connector (you do not need it if you connect the router to the Ethernet)

- Each PC in the LAN needs a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- TCP/IP protocol must be installed on each PC
- Web browser, such as Microsoft Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later

2.4 Installation Environment Requirements

- The Product should not be located where it will be exposed to moisture or excessive heat.
- Place the Router in a location where it can be connected to the various devices as well as to a power source.
- Make sure the cables and power cord are placed safely out of the way so they do not create a tripping hazard.
- Designed to go up to 100 meters indoors and up to 300 meters outdoors for wireless connection.
- The Router can be placed on a shelf or desktop.

2.5 Connecting the Device

Before installing the Router, please make sure your broadband service provided by your ISP is available. If there is any problem, please contact with your ISP. After that, please install the Router according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

1. Locate an optimum location for the Router. The best place is usually near the center of the area in which your PC will be wirelessly connected. The place had better accord with the Installation Environment Requirements.
2. Adjust the direction of the antenna. Normally, upright is a good direction.
3. Connect the PC(s) and each Switch/Hub in your LAN to the LAN Ports on the router, shown in Figure 2-3. (If you have the wireless NIC and want to use wireless function, you can skip this step.)
4. Connect the DSL/Cable Modem to the WAN port on the router, shown in Figure 2-3.
5. Connect the AC power adapter to the AC power socket on the router, and the other end into an electrical outlet. The router will start to work automatically.
6. Power on your PC and Cable/DSL Modem.

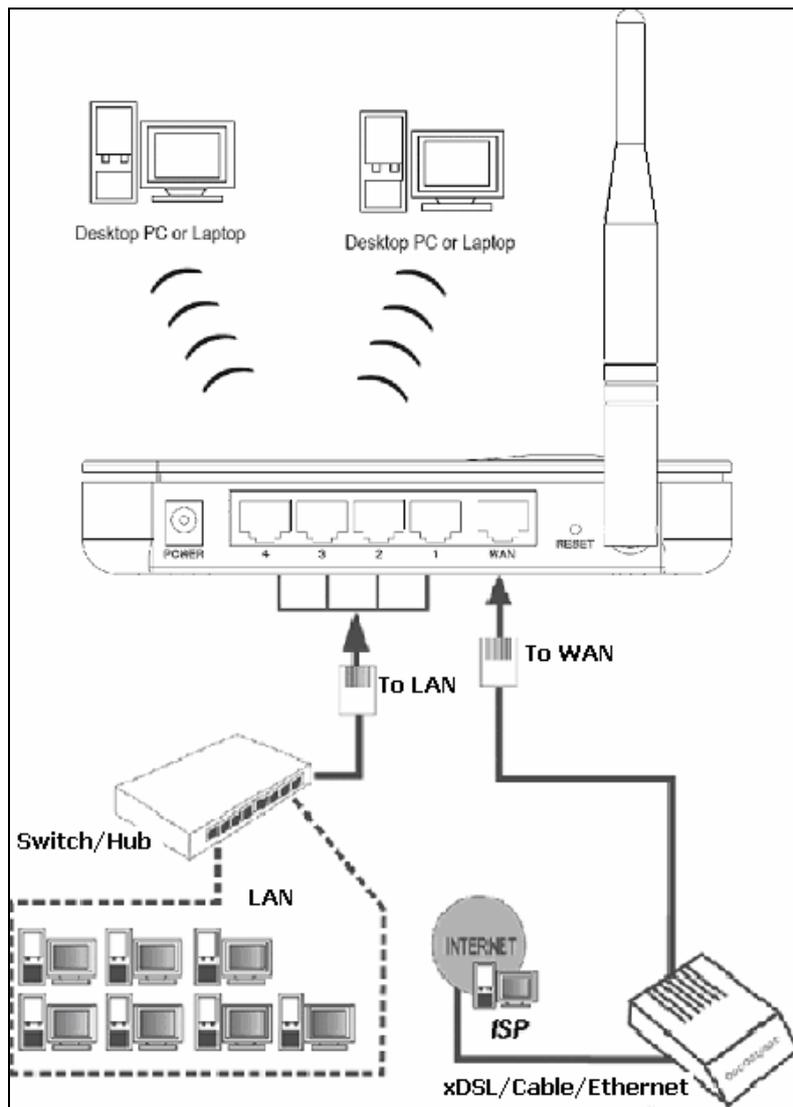


Figure 2-3 Hardware Installation of the Router

2.6 Configure PC

Your PC needs a network adapter. You may directly connect your adapter to the Router, or you may connect your adapter to a Hub/Switch, and then connect the Hub/Switch to the Router.

Follow the instructions below to configure a computer running Windows XP to be a DHCP client.

1. From the **Start** menu on your desktop, go to **Settings**, and then click on Network Connections.

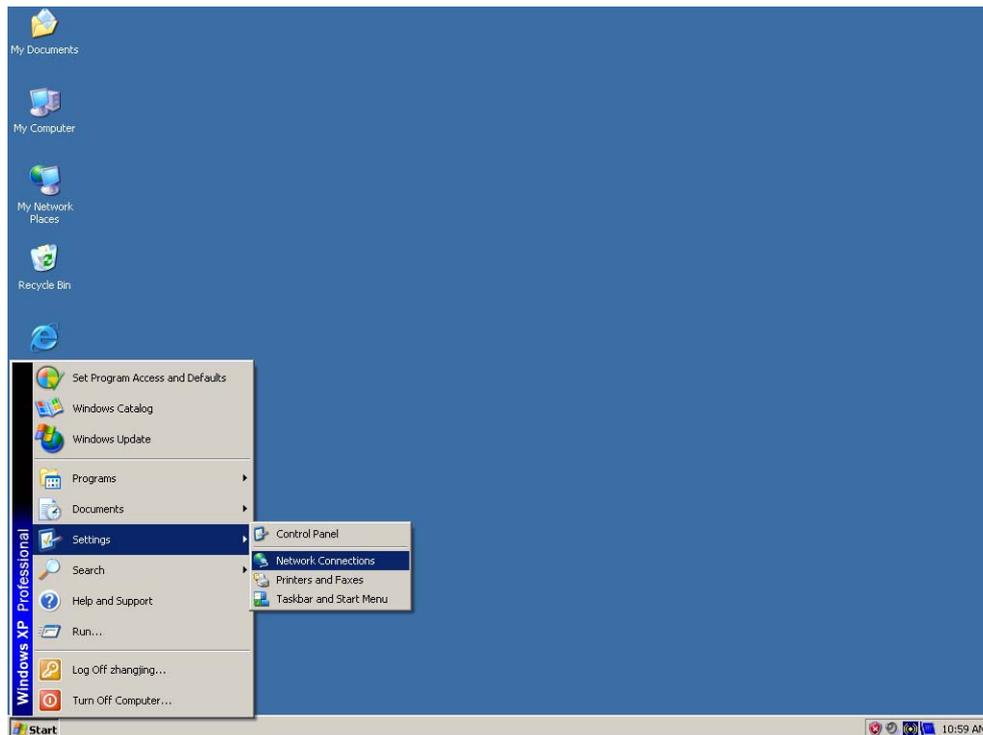


Figure 2-4

2. In the **Network Connections** window, right-click on LAN (Local Area Connection), then click **Properties**.

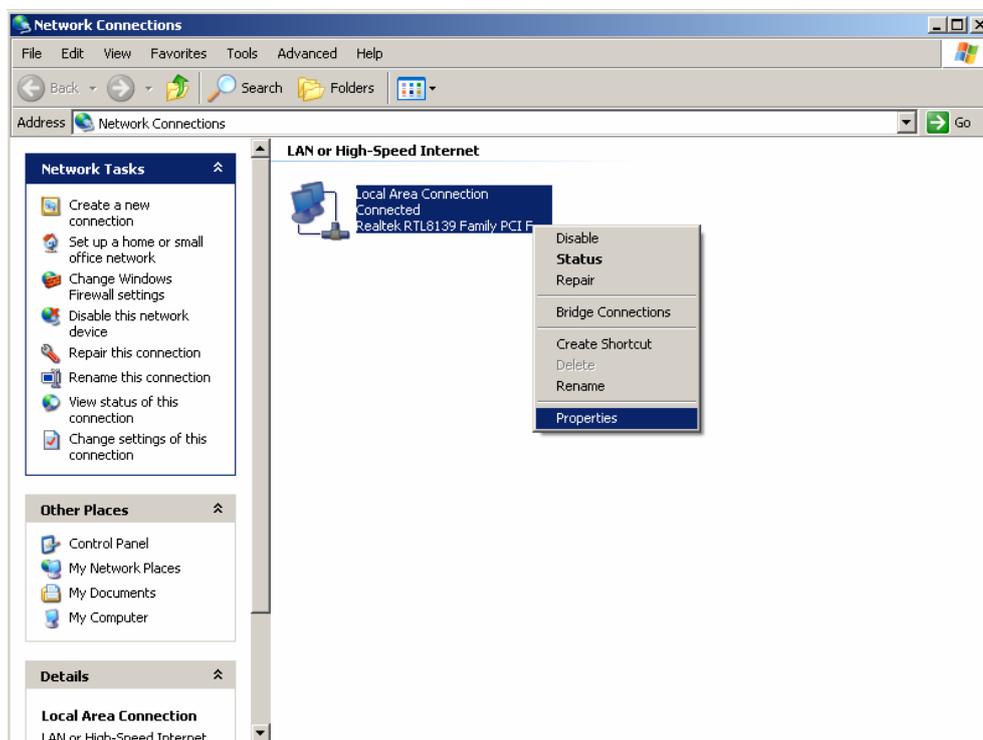


Figure 2-5

3. In the **General** tab of **Internet Protocol (TCP/IP) Properties** menu, highlight **Internet Protocol (TCP/IP)** under **This connection uses the following items** by clicking on it once. Click on the **Properties** button.

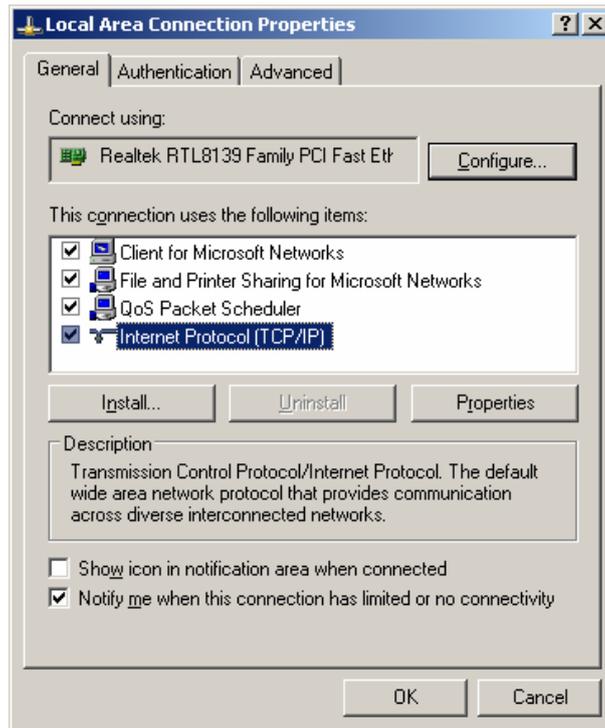


Figure 2-6

4. Select **Obtain an IP address automatically** by clicking the radio-button. Click **OK**.

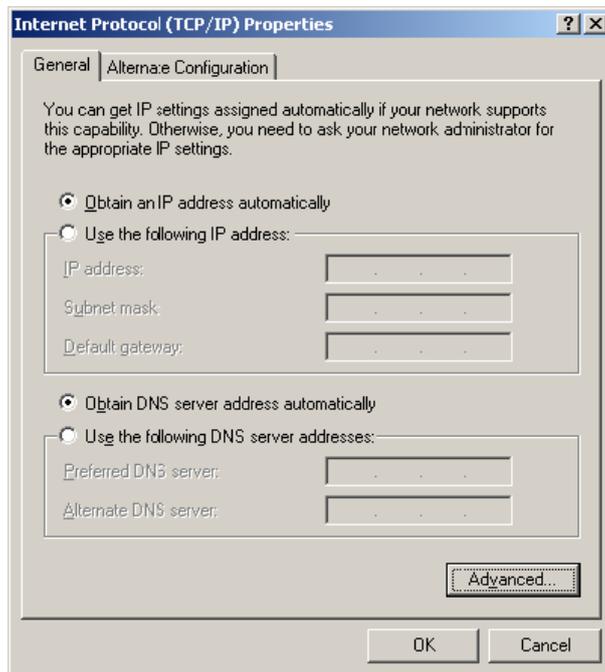


Figure 2-7

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your TL-WR340G 54Mbps Wireless Router using **Quick Setup Wizard** within minutes.

3.1 TCP/IP Configuration

Connect the local PC to the LAN ports of the Router. And then you can configure the IP address for your PC in the following way.

- 1) Set up the TCP/IP Protocol in **Obtain an IP address automatically** mode on your PC. If you need instructions as to how to do this, please refer to [Appendix B: "Configuring the PC"](#).
- 2) Then the built-in DHCP server will assign IP address for the PC.

3.2 Quick Installation Guide

With a Web-based utility, it is easy to configure and manage the TL-WR340G 54Mbps Wireless Router. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

1. To access the configuration utility, open a web-browser and type in the default access <http://tplinklogin.net> in the address field of the browser.

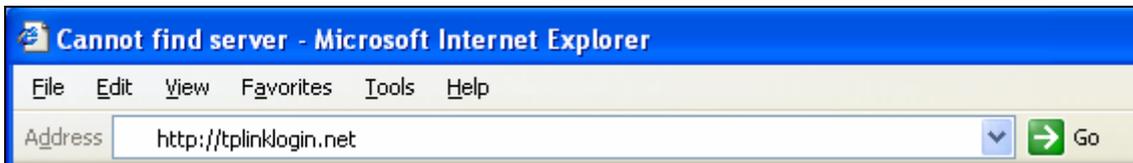


Figure 3-1 Log in the Router

After a moment, a login window will appear, similar to the Figure 3-2. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.



Figure 3-2 Login Windows

Note:

If the above screen does not pop up, it means that your Web-browser has been set to a proxy. Go to Tools menu>Internet Options>Connections>LAN Settings, in the screen that appears, cancel the Using Proxy checkbox, and click **OK** to finish it.

2. After successfully log in, you can click the **Quick Setup** menu to quickly configure your Router.

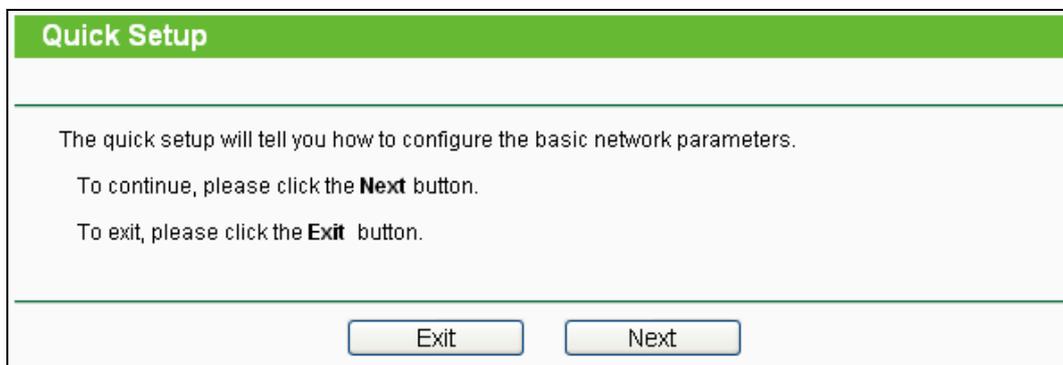


Figure 3-3 Quick Setup

3. Click **Next**, and then Choose **WAN Connection Type** page will appear, shown in Figure 3-4.

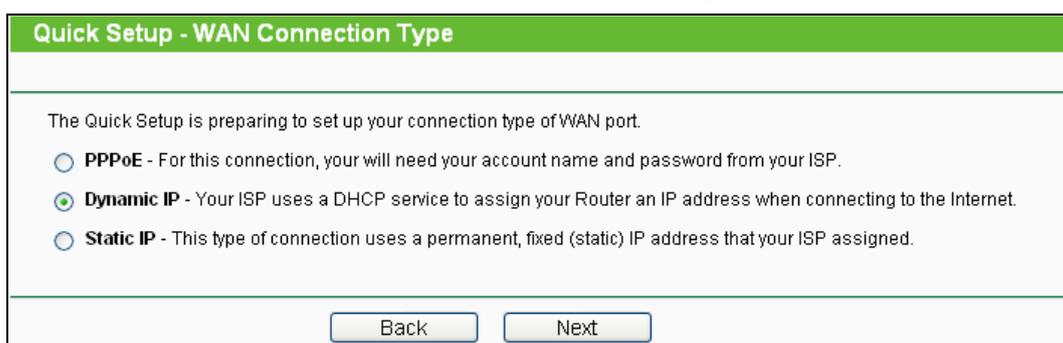
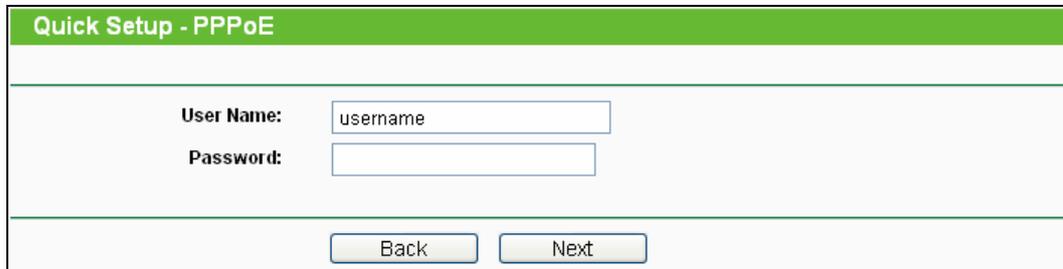


Figure 3-4 WAN Connection Type

The Router supports three popular ways **PPPoE**, **Dynamic IP** and **Static IP** to connect to the Internet.

4. Select your connection type.

- 1) If the connection type selected is **PPPoE**, the next screen will appear as shown in Figure 3-5.



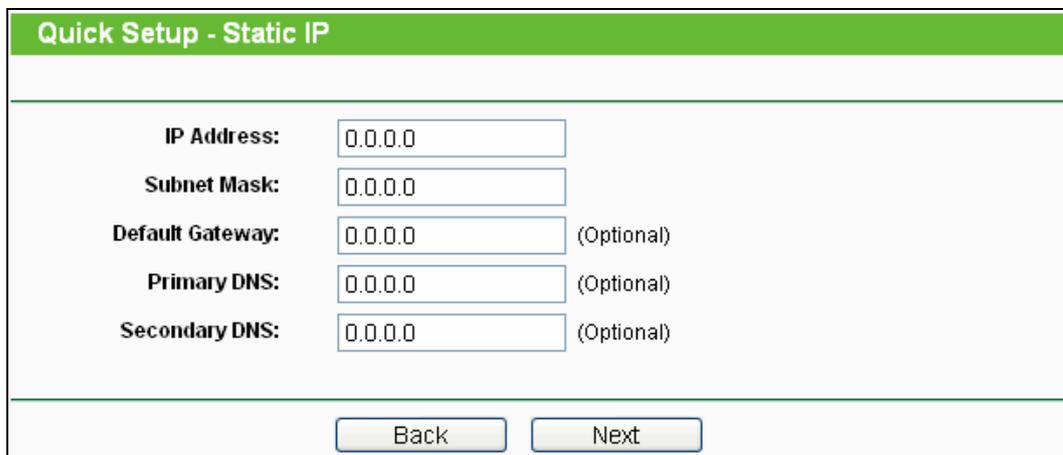
Quick Setup - PPPoE	
User Name:	<input type="text" value="username"/>
Password:	<input type="password"/>
<input type="button" value="Back"/> <input type="button" value="Next"/>	

Figure 3-5 Quick Setup - PPPoE

- **User Name/Password** - Enter the **User Name** and **Password** provided by your ISP. These fields are case sensitive. If you have difficulty with this process, please contact your ISP.

2) If the connection type selected is **Dynamic IP**, the next screen will appear as shown in Figure 3-7. Then you can go on with the wireless configuration.

3) If the connection type selected is **Static IP**, the next screen will appear as shown in Figure 3-6.



Quick Setup - Static IP	
IP Address:	<input type="text" value="0.0.0.0"/>
Subnet Mask:	<input type="text" value="0.0.0.0"/>
Default Gateway:	<input type="text" value="0.0.0.0"/> (Optional)
Primary DNS:	<input type="text" value="0.0.0.0"/> (Optional)
Secondary DNS:	<input type="text" value="0.0.0.0"/> (Optional)
<input type="button" value="Back"/> <input type="button" value="Next"/>	

Figure 3-6 Quick Setup - Static IP

- **IP Address** - This is the WAN IP address as seen by external users on the Internet (including your ISP). Enter the IP address into the field.
- **Subnet Mask** - The Subnet Mask is used for the WAN IP address, it is usually 255.255.255.0.
- **Default Gateway** - Enter the gateway IP address into the box if required.
- **Primary DNS** - Enter the DNS Server IP address into the box if required.
- **Secondary DNS** - If your ISP provides another DNS server, enter it into this field.

5. Click **Next** to continue, the **Wireless** settings page will appear as shown in Figure 3-7.

Figure 3-7 Quick Setup – Wireless

- **Wireless Radio** - Enable or disable the wireless radio choosing from the pull-down list.
- **SSID** - Enter a value of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security, the default SSID is set to be TP-LINK_XXXXXX (XXXXXX indicates the last unique six numbers of each Router's MAC address). This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the Router can be used. It may be illegal to use the wireless function of the Router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

 **Note:**

Limited by local law regulations, version for North America does not have region selection option.

- **Channel** - This field determines which operating frequency will be used. The default channel is set to Auto. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Mode** - This field determines the wireless mode which the Router works on.
- **Wireless Security** - You can select one of the following security options.
 - **Disable Security** - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Router without encryption.

It is recommended strongly that you choose one of following options to enable security.

- **WPA-PSK/WPA2-PSK** - Select WPA based on pre-shared passphrase.
- **PSK Password** - You can enter **ASCII** or **Hexadecimal** characters.

For **ASCII**,the length should be between 8 and 63 characters.

For **Hexadecimal**,the length should be between 8 and 64 characters.

Please note that the key is case sensitive.

- **No Change** - If you choose this option, wireless security configuration will not change.

These settings are only for basic wireless parameters. For advanced settings, please refer to [Section 4.5: "Wireless"](#).

6. Click the **Next** button. You will then see the **Finish** page.

If you don't make any change on the **Wireless** page, you will see the **Finish** page as shown in Figure 3-8. Click the **Finish** button to finish the **Quick Setup**.

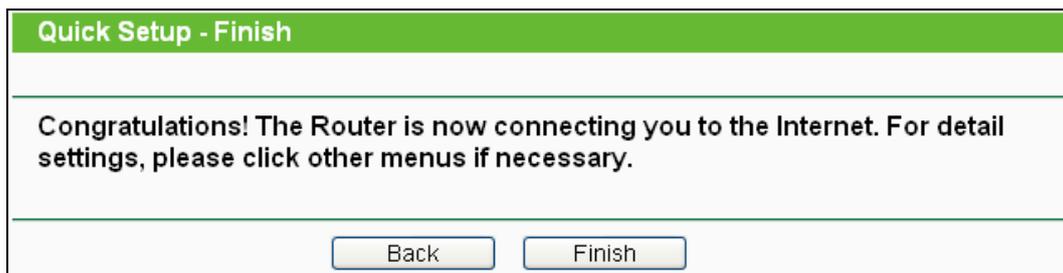


Figure 3-8 Quick Setup - Finish

If there is something changed on the **Wireless** page, you will see the **Finish** page as shown in Figure 3-9. Click the **Reboot** button to make your wireless configuration take effect and finish the **Quick Setup**.

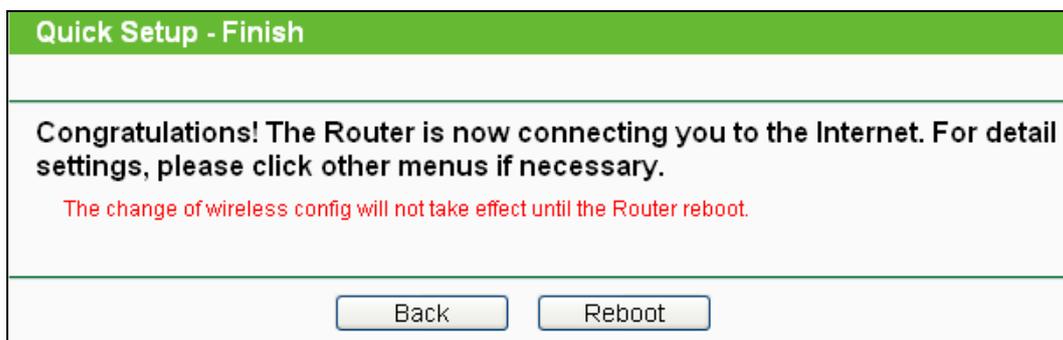


Figure 3-9 Quick Setup - Finish

Chapter 4. Software Configuration

This User Guide recommends using the “Quick Installation Guide” for first-time installation, For advanced users, if you want to know more about this device and make use of its functions adequately, you need to read this chapter and configure advanced settings through the Web-based Utility.

4.1 Login

After your successful login, you can configure and manage the device. There are main menus on the left of the web-based utility. Submenus will be available after you click one of the main menus. On the right of the web-based utility, there are the detailed explanations and instructions for the corresponding page. To apply any settings you have altered on the page, please click the **Save** button.

4.2 Status

The Status page displays the router's current status and configuration. All information is read-only.

- **LAN** - This field displays the current settings or information for the LAN, including the **MAC address, IP address and Subnet Mask**.
- **Wireless** - This field displays basic information or status for wireless function, including **Wireless Radio, SSID, Channel, Mode, Wireless MAC address, and IP address**.
- **WAN** - These parameters apply to the WAN port of the router, including **MAC address, IP address, Subnet Mask, Default Gateway, DNS server** and **WAN connection type**. If PPPoE is chosen as the WAN connection type, the **Disconnect** button will be shown here while you are accessing the Internet. You can also cut the connection by clicking the button. If you have not connected to the Internet, just click **Connect** to establish the connection.
- **Traffic Statistics** - This field displays the router's traffic statistics.
- **System Up Time** - The total up time of the router from when it was switched on or reset.

Status		
Firmware Version:	4.17.9 Build 110329 Rel.45392n	
Hardware Version:	WR340G 4.0 00000000	
LAN		
MAC Address:	00-03-7F-FF-FF-FE	
IP Address:	192.168.1.1	
Subnet Mask:	255.255.255.0	
Wireless		
Wireless Radio:	Enable	
Name (SSID):	TP-LINK_FFFFE	
Channel:	Automatic (Current channel 11)	
Mode:	11bg mixed	
MAC Address:	00-03-7F-FF-FF-FE	
WDS Status:	Disable	
WAN		
MAC Address:	00-03-7F-FF-FF-FF	
IP Address:	0.0.0.0	Dynamic IP
Subnet Mask:	0.0.0.0	
Default Gateway:	0.0.0.0	<input type="button" value="Renew"/> Obtaining network parameters...
DNS Server:	0.0.0.0 , 0.0.0.0	
Traffic Statistics		
	Received	Sent
Bytes:	410	2112
Packets:	2	32
System Up Time:	0 day(s) 00:04:37	<input type="button" value="Refresh"/>

Figure 4-1 Router Status

4.3 Quick Setup

Please refer to [Quick Installation Guide](#).

4.4 Network

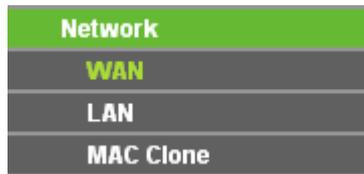


Figure 4-2 the Network menu

There are three submenus under the Network menu (shown in Figure 4-2): **WAN**, **LAN** and **MAC Clone**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.4.1 WAN

You can configure the WAN port parameters on this page.

First, please choose the WAN Connection Type (Dynamic IP/Static IP/PPPoE/Russia PPPoE /L2TP/Russia L2TP/PPTP/Russia PPTP) for Internet. The default type is **Dynamic IP**. If you aren't given any login parameters (fixed IP Address, logging ID, etc), please select **Dynamic IP**. If you are given a fixed IP (static IP), please select **Static IP**. If you are given a user name and a password, please select the type of your ISP provided (PPPoE/L2TP/PPTP). If you are not sure which connection type you use currently, please contact your ISP to obtain the correct information.

1. If you choose **Dynamic IP**, the router will automatically get IP parameters from your ISP. You can see the page as follows (Figure 4-3):

The screenshot shows the WAN configuration interface for a Dynamic IP connection. The page has a green header with the word 'WAN'. Below the header, the 'WAN Connection Type' is set to 'Dynamic IP'. The IP Address, Subnet Mask, and Default Gateway are all set to 0.0.0.0. There are 'Renew' and 'Release' buttons, and a status indicator that says 'Obtaining network parameters...'. The MTU Size is set to 1500 bytes. There is a checkbox for 'Use These DNS Servers' which is currently unchecked. The Primary DNS and Secondary DNS fields are both set to 0.0.0.0. The Host Name is set to WR340G. There is also a checkbox for 'Get IP with Unicast DHCP' which is unchecked. A 'Save' button is at the bottom.

Figure 4-3 WAN – Dynamic IP

This page displays the WAN IP parameters assigned dynamically by your ISP, including IP address, Subnet Mask, Default Gateway, etc. Click the **Renew** button to renew the IP parameters from your ISP. Click the **Release** button to release the IP parameters.

- **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

If your ISP gives you one or two DNS addresses, select **Use These DNS Servers** and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from your ISP.

 **Note:**

If you get address and find error when you go to a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

- **Get IP with Unicast DHCP** - A few ISPs' DHCP servers do not support the broadcast applications. If you cannot get the IP Address normally, you can choose this option. (This is rarely required.)

- If you choose **Static IP**, you should have fixed IP parameters specified by your ISP. The Static IP settings page will appear, shown in Figure 4-4:

WAN

WAN Connection Type: Static IP

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0 (Optional)

MTU Size (in bytes): 1500 (The default is 1500. Do not change it unless necessary.)

Primary DNS: 0.0.0.0 (Optional)

Secondary DNS: 0.0.0.0 (Optional)

Save

Figure 4-4 WAN - Static IP

You should type the following parameters into the spaces provided:

- **IP Address** - Enter the IP address in dotted-decimal notation provided by your ISP.
 - **Subnet Mask** - Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.
 - **Default Gateway** - (Optional) Enter the gateway IP address in dotted-decimal notation provided by your ISP.
 - **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
 - **Primary DNS** - (Optional) Enter the DNS address in dotted-decimal notation provided by your ISP.
 - **Secondary DNS** - (Optional) Type another DNS address in dotted-decimal notation provided by your ISP if provided.
- If you choose **PPPoE**, you should enter the following parameters (Figure 4-5):

WAN

WAN Connection Type: PPPoE

PPPoE Connection:

User Name: username

Password: ●●●●●●●●●●

Secondary Connection: Disabled Dynamic IP Static IP (For Dual Access/Russia PPPoE)

Wan Connection Mode: Connect on Demand
 Max Idle Time: 15 minutes (0 means remaining active all the time.)

Connect Automatically

Time-based Connecting
 Period of Time: from 0 : 0 (HH:MM) to 23 : 59 (HH:MM)

Connect Manually
 Max Idle Time: 15 minutes (0 means remaining active all the time.)

Disconnected

Figure 4-5 WAN - PPPoE

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Secondary Connection** - It's available only for PPPoE Connection. If your ISP provides an extra Connection type such as Dynamic/Static IP to connect to a local area network, then you can check the radio button of Dynamic/Static IP to activate this secondary connection.
 - **Disabled** - The Secondary Connection is disabled by default, so there is PPPoE connection only. This is recommended.
 - **Dynamic IP** - Use dynamic IP address to connect to the local area network provided by ISP.
 - **Static IP** - Use static IP address to connect to the local area network provided by ISP.
- **Connect on Demand** - You can configure the router to disconnect your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.
- **Connect Automatically** - Connect automatically after the router is disconnected. To use this option, click the radio button.

- **Time-based Connecting** - You can configure the router to make it connect or disconnect based on time. Enter the start time in HH:MM format for connecting and end time in HH:MM format for disconnecting in the **Period of Time** fields.

 **Note:**

Only when you have configured the system time on System Tools -> Time page, will the Time-based Connecting function can take effect.

- **Connect Manually** - You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect from the Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number time in minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

Click the **Advanced Settings** button to set up the advanced option, the page shown in Figure 4-6 will then appear:

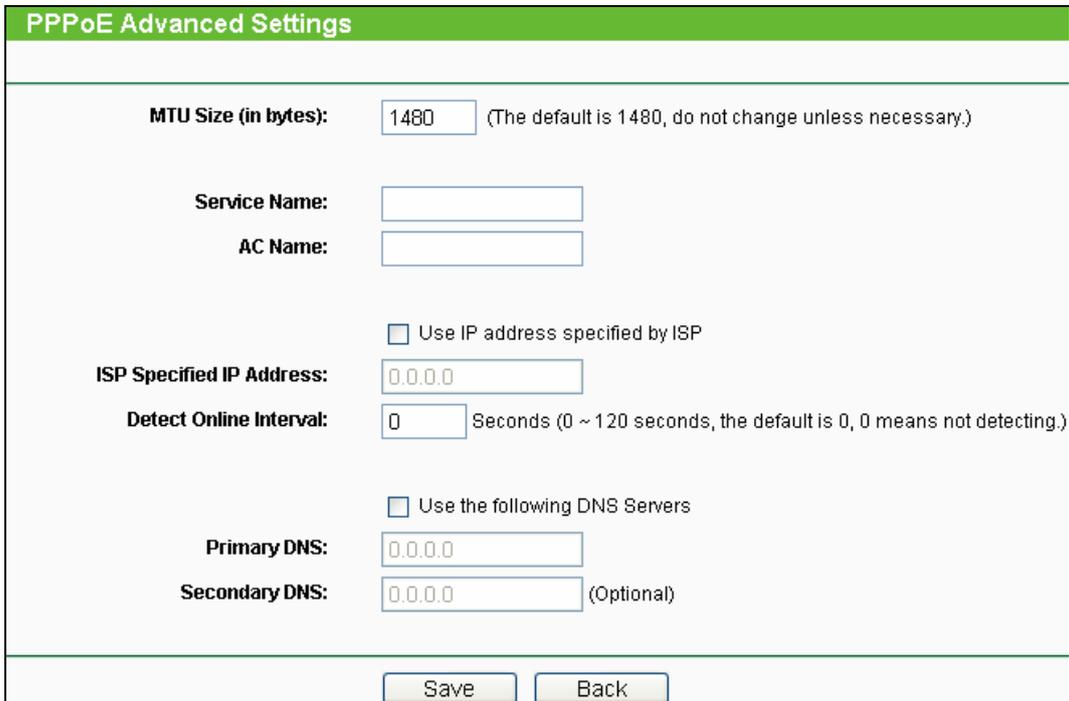


Figure 4-6 PPPoE Advanced Settings

- **Packet MTU** - The default MTU size is 1480 bytes, which value is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.
- **Service Name/AC Name** - The service name and AC (Access Concentrator) name, these should not be configured unless you are sure it is necessary for your ISP.

- **ISP Specified IP Address** - If you know that your ISP does not automatically transmit your IP address to the router during login, click “**Use the IP Address specified by ISP**” check box and enter the IP Address in dotted-decimal notation, which your ISP provided.
- **Detect Online Interval** - The default value is 0, you can input the value between 0 and 120. The router will detect Access Concentrator online at every interval between seconds. If the value is 0, it means, do not detect.
- **DNS IP address** - If you know that your ISP does not automatically transmit DNS addresses to the router during login, click “**Use the following DNS servers**” checkbox and enter the IP address in dotted-decimal notation of your ISP’s primary DNS server. If a secondary DNS server address is available, enter it as well.

Click the **Save** button to save your settings.

4. If you choose **L2TP/Russia L2TP**, you should enter the following parameters (Figure 4-7):

The screenshot shows the WAN configuration interface for L2TP/Russia L2TP. The page has a green header with the text 'WAN'. Below the header, the 'WAN Connection Type' is set to 'L2TP/Russia L2TP'. The 'User Name' field contains 'username' and the 'Password' field contains a series of dots. There are 'Connect' and 'Disconnect' buttons, with the status 'Disconnected!' displayed. Below these are radio buttons for 'Dynamic IP' (selected) and 'Static IP'. The 'Server IP Address/Name' field is empty. Below it are fields for 'IP Address', 'Subnet Mask', 'Default Gateway', and 'DNS', all containing '0.0.0.0'. Further down are 'Internet IP Address' and 'Internet DNS' fields, also containing '0.0.0.0'. The 'MTU Size (in bytes)' is set to '1460' with a note: '(The default is 1460. Do not change it unless necessary.)'. The 'Max Idle Time' is set to '15' minutes with a note: '(0 means remaining active all the time.)'. At the bottom, there are radio buttons for 'WAN Connection Mode': 'Connect on Demand' (selected), 'Connect Automatically', and 'Connect Manually'. A 'Save' button is located at the very bottom of the form.

Figure 4-7 L2TP/Russia L2TP Settings

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP** – Choose either as you are given by your ISP.

Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

- **Connect on Demand** - You can configure the router to disconnect from your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.

- **Connect Automatically** - Connect automatically after the router is disconnected. To use this option, click the radio button.
- **Connect Manually** - You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.

5. If you choose **PPTP/Russia PPTP**, you should enter the following parameters (Figure 4-8):

WAN

WAN Connection Type: PPTP/Russia PPTP

User Name: username

Password:

Disconnected!

Dynamic IP Static IP

Server IP Address/Name: _____

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

DNS: 0.0.0.0, 0.0.0.0

Internet IP Address: 0.0.0.0

Internet DNS: 0.0.0.0, 0.0.0.0

MTU Size (in bytes): 1420 (The default is 1420. Do not change it unless necessary.)

Max Idle Time: 15 minutes (0 means remaining active all the time.)

WAN Connection Mode:

Connect on Demand

Connect Automatically

Connect Manually

Figure 4-8 PPTP/Russia PPTP Settings

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP** – Choose either as you are given by your ISP and enter the ISP's IP address or the domain name.

If you choose static IP and enter the domain name, you should also enter the DNS assigned by your ISP. And click the **Save** button.

Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

- **Connect on Demand** - You can configure the router to disconnect from your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise,

enter the number of minutes you want to have elapsed before your Internet connection terminates.

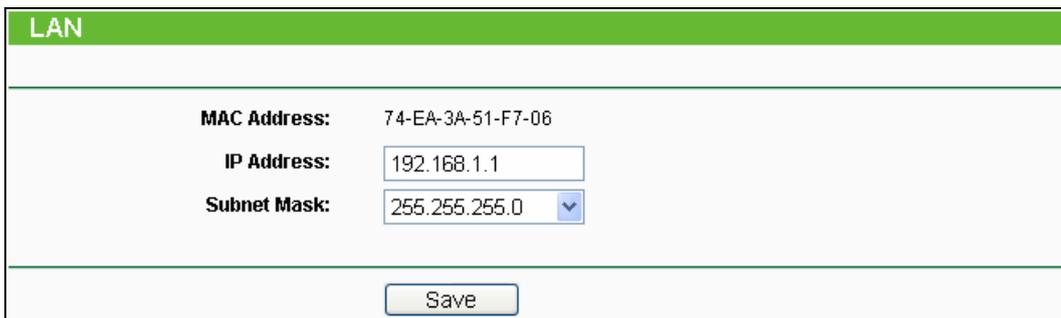
Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

- **Connect Automatically** - Connect automatically after the router is disconnected. To use this option, click the radio button.
- **Connect Manually** - You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

4.4.2 LAN

You can configure the IP parameters of LAN on this page.



The screenshot shows the LAN configuration interface. At the top, there is a green header with the text "LAN". Below the header, there are three rows of configuration fields:

- MAC Address:** 74-EA-3A-51-F7-06
- IP Address:** 192.168.1.1
- Subnet Mask:** 255.255.255.0 (with a dropdown arrow)

At the bottom of the form, there is a "Save" button.

Figure 4-9 LAN

- **MAC Address** - The physical address of the router, as seen from the LAN. The value can't be changed.
- **IP Address** - Enter the IP address of your router in dotted-decimal notation (factory default: 192.168.1.1).
- **Subnet Mask** - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

Note:

If you change the IP Address of LAN, you must use the new IP Address to login the router.

If the new LAN IP Address you set is not in the same subnet, the IP Address pool of the DHCP server will not take effect, until they are re-configured.

If the new LAN IP Address you set is not in the same subnet, the Virtual Server and DMZ Host will change accordingly at the same time.

4.4.3 MAC Clone

You can configure the MAC address of the WAN port on this page, Figure 4-10:

Figure 4-10 MAC Address Clone

Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable/DSL Modem or Ethernet during installation. Changes are rarely needed here.

- **WAN MAC Address** - This field displays the current MAC address of the WAN port, which is used for the WAN port. If your ISP requires that you register the MAC address, please enter the correct MAC address into this field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit).
- **Your PC's MAC Address** - This field displays the MAC address of the PC that is managing the router. If the MAC address is required, you can click the **Clone MAC Address** button and this MAC address will fill in the **WAN MAC Address** field.

Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value.

Click the **Save** button to save your settings.

 **Note:**

Only the PC on your LAN can use the MAC Address Clone feature.

If you click the **Save** button, the router will prompt you to reboot.

4.5 Wireless



Figure 4-11 Wireless menu

There are five submenus under the Wireless menu (shown in Figure 4-11): **Wireless Settings**, **Security Settings**, **MAC Filtering**, **Wireless Advanced** and **Wireless Statistics**. Click any of

them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.5.1 Wireless Settings

The basic settings for the wireless network are set on this page, Figure 4-12:



Figure 4-12 Wireless Settings

- **SSID** - Enter a value of up to 32 characters. The same name (SSID) must be assigned to all wireless devices in your network. The default SSID is TP-LINK_XXXXXX, but it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

The default region is United States. When you select your local region from the pull-down list, Click the **Save** button, then the Note Dialog appears. Click **OK**.

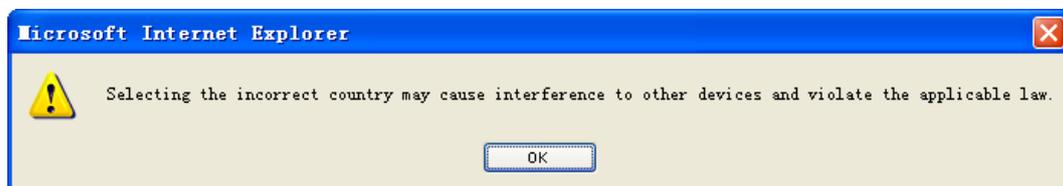


Figure 4-13 Note Dialog

Note:

Limited by local law regulations, version for North America does not have region selection option.

- **Channel** - This field determines which operating frequency will be used. The default channel is set to Auto. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

- **Mode** - If all of the wireless devices connected with this wireless router can connect in the same transmission mode(eg. 802.11b), you can choose "Only" mode(eg. 11b only). If you have some devices that use a different transmission mode, choose the appropriate "Mixed" mode.
- **Enable Wireless Router Radio** - The wireless radio of this Router can be enabled or disabled to allow wireless stations access. If enabled, wireless stations will be able to access the router. Otherwise, wireless stations will not be able to access.
- **Enable SSID Broadcast** - If you select the **Enable SSID Broadcast** checkbox, the Wireless Router SSID will broadcast its name (SSID) on the air.
- **Enable WDS** - You can select this to enable WDS, with this function, the Router can bridge two or more Wlans. If this checkbox is selected, you had better make sure the following settings are correct.

The screenshot shows a configuration window for enabling WDS. At the top, the checkbox 'Enable WDS' is checked. Below it are several input fields and a button:

- SSID(to be bridged):** An empty text input field.
- BSSID(to be bridged):** An empty text input field with the example '00-1D-0F-11-22-33' shown to its right.
- Survey**: A button to search for APs.
- Key type:** A dropdown menu currently set to 'None'.
- WEP Index:** A dropdown menu currently set to '1'.
- Auth type:** A dropdown menu currently set to 'open'.
- Password:** An empty text input field.

At the bottom of the window are two buttons: 'Save' and 'Help'.

Figure 4-14 Enable WDS

- **SSID(to be bridged)** - The SSID of the AP your Router is going to connect to as a client. You can also use the search function to select the SSID to join.
- **BSSID(to be bridged)** - The BSSID of the AP your Router is going to connect to as a client. You can also use the search function to select the BSSID to join.
- **Survey** - Click this button, you can search the AP which runs in the current channel.
- **Key type** - This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type
- **WEP Index** - This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the index of the WEP key.
- **Auth Type** - This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the authorization type of the Root AP.
- **Password** - If the AP your Router is going to connect needs password, you need to fill the password in this blank.

4.5.2 Security Settings

Options related to security can be set on this page.

The screenshot shows the 'Wireless Security' configuration page. It features a green header and a white background. The main content is organized into sections based on security protocols:

- Disable Security:** A radio button that is currently selected.
- WEP:** A radio button that is not selected. It includes:
 - Type:** A dropdown menu set to 'Automatic'.
 - WEP Key Format:** A dropdown menu set to 'Hexadecimal'.
 - Key Selected:** A section with four radio buttons labeled 'Key 1' through 'Key 4'. 'Key 1' is selected.
 - WEP Key:** Four text input fields corresponding to Key 1-4.
 - Key Type:** Four dropdown menus, each set to 'Disabled'.
- WPA/WPA2:** A radio button that is not selected. It includes:
 - Version:** A dropdown menu set to 'Automatic'.
 - Encryption:** A dropdown menu set to 'Automatic'.
 - Radius Server IP:** A text input field.
 - Radius Port:** A text input field with '1812' and a note '(1-65535, 0 stands for default port 1812)'. The field is highlighted in blue.
 - Radius Password:** A text input field.
 - Group Key Update Period:** A text input field with '86400' and a note '(in second, minimum is 30, 0 means no update)'. The field is highlighted in blue.
- WPA-PSK/WPA2-PSK:** A radio button that is not selected. It includes:
 - Version:** A dropdown menu set to 'Automatic'.
 - Encryption:** A dropdown menu set to 'Automatic'.
 - PSK Password:** A text input field.
 - Group Key Update Period:** A text input field with '86400' and a note '(in second, minimum is 30, 0 means no update)'. The field is highlighted in blue.

At the bottom of the page, there is a 'Reboot' checkbox and a 'Save' button.

Figure 4-15 Wireless Security

You can select one of the following security options:

- **Disable Security** - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Router without encryption. It is recommended strongly that you choose one of following options to enable security.
- **WEP** - Select WEP authentication type based on 802.11 authentications.
- **WPA /WPA2** - Select WPA/WPA2 authentication type based on Radius Server.
- **WPA-PSK/WPA2-PSK** - Select WPA/WPA2 authentication type based on pre-shared passphrase.

Each security option has its own settings as described below.

WEP

- **Type** - You can select one of the following types.
 - **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station request.
 - **Open System** - Select 802.11 Open System authentication.

- **Shared Key** - Select 802.11 Shared Key authentication.
- **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII Code Format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
- **Key Selected** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
- **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**) for encryption. "Disabled" means the WEP key entry is invalid.
 - For **64-bit** encryption - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.
 - For **128-bit** encryption - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.
 - For **152-bit** encryption - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.

WPA/WPA2

- **Version** - You can select one of following versions
 - **Automatic** - Select **WPA** or **WPA2** automatically based on the wireless station's capability and request.
 - **WPA** - Wi-Fi Protected Access.
 - **WPA2** - WPA version 2.
- **Encryption** - You can select **Automatic**, or **TKIP**, or **AES**.
- **Radius Server IP** - Enter the IP address of the Radius Server.
- **Radius Port** - Enter the port that radius service used.
- **Radius Password** - Enter the password for the Radius Server.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

WPA-PSK/WPA2-PSK

- **Version** - You can select one of following versions.
 - **Automatic** - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.
 - **WPA-PSK** - Pre-shared key of WPA.
 - **WPA2-PSK** - Pre-shared key of WPA2.
- **Encryption** - You can select either **Automatic**, or **TKIP** or **AES**.

- **PSK Password** - You can enter **ASCII** or **Hexadecimal** characters. For **Hexadecimal**, the length should be between 8 and 64 characters; for **ASCII**, the length should be between 8 and 63 characters.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

Be sure to click the **Save** button to save your settings on this page.

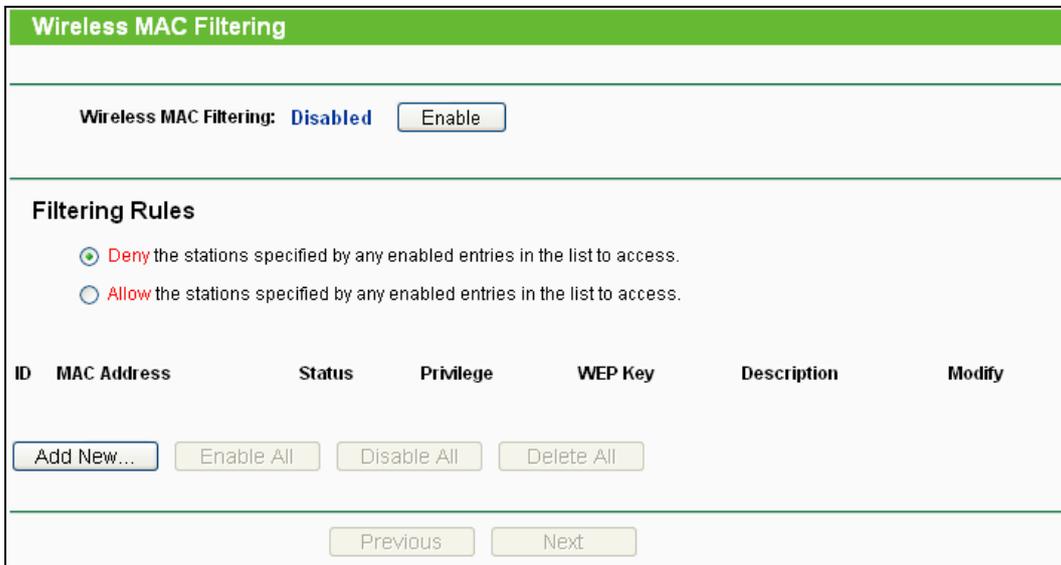
 **Note:**

The router will reboot automatically after you click save.

- **Reboot** - Select the radio button to reboot the router automatically after all the above settings.

4.5.3 MAC Filtering

The Wireless MAC Filtering for wireless networks is set on this page, Figure 4-16:



ID	MAC Address	Status	Privilege	WEP Key	Description	Modify
<div style="text-align: center;"> <input type="button" value="Add New..."/> <input type="button" value="Enable All"/> <input type="button" value="Disable All"/> <input type="button" value="Delete All"/> </div>						
<input type="button" value="Previous"/> <input type="button" value="Next"/>						

Figure 4-16 Wireless MAC address Filtering

The Wireless MAC Address Filtering feature allows you to control wireless stations accessing the router, which depend on the station's MAC addresses.

- **MAC Address** - The wireless station's MAC address that you want to access.
- **Status** - The status of this entry either **Enabled** or **Disabled**.
- **Privilege** - Select the privileges for this entry. You may select one of the following **Allow / Deny**.
- **Description** - A simple description of the wireless station.

First, you must decide whether the unspecified wireless stations can access the router or not. If you desire that the unspecified wireless stations can access the router, please select the radio button **Allow the stations not specified by any enabled entries in the list to access**,

otherwise, select the radio button **Deny the stations not specified by any enabled entries in the list to access**.

To Add a Wireless MAC Address filtering entry, click the **Add New...** button. The **Add or Modify Wireless MAC Address Filtering entry** page will appear, shown in Figure 4-17:



Figure 4-17 Add or Modify Wireless MAC Address Filtering entry

To add a MAC Address Filtering entry, follow these instructions:

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0A-EB-B0-00-0B.
2. Enter a simple description of the wireless station in the **Description** field. For example: Wireless station A.
3. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

To add another entries, repeat steps 1~4.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

Click the **Next** button to go to the next page and click the **Previous** button to return to the previous page.

For example: If you desire that the wireless station A with MAC address 00-0A-EB-00-07-BE be able to access the router. The wireless station B with MAC address 00-0A-EB-00-07-5F not be able to access the router, while all other wireless stations cannot access the router, you should configure the **Wireless MAC Address Filtering** list by following these steps:

1. Click the **Enable** button to enable this function.

2. Select the radio button: **Deny the stations not specified by any enabled entries in the list to access** for **Filtering Rules**.
3. Delete all or disable all entries if there are any entries already.
4. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-BE in the **MAC Address** field, enter wireless station A in the **Description** field, select **Allow** in the **Privilege** pull-down list and select **Enabled** in the **Status** pull-down list. Click the **Save** and the **Return** button.
5. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-5F in the **MAC Address** field, enter wireless station B in the **Description** field, select **Deny** in the **Privilege** pull-down list and select **Enabled** in the **Status** pull-down list. Click the **Save** and the **Return** button.

The filtering rules that configured should be similar to the following list:

ID	MAC Address	Status	Privilege	Description	Modify
1	00-0A-EB-00-07-BE	Enabled	allow	Wireless Station A	Modify Delete
2	00-0A-EB-00-07-5F	Enabled	deny	Wireless Station B	Modify Delete

Note:

If you select the radio button **Allow the stations not specified by any enabled entries in the list to access** for **Filtering Rules**, the wireless station B will still not be able to access the router, however, other wireless stations that are not in the list will be able to access the router.

If you enable the function and select the **Deny the stations not specified by any enabled entries in the list to access** for **Filtering Rules**, and there are not any enable entries in the list, thus, no wireless stations can access the router.

4.5.4 Wireless Advanced

Some advanced settings can be made on this page.

Wireless Advanced

Transmit Power: High ▼

Beacon Interval : 100 (40-1000)

RTS Threshold: 2346 (1-2346)

Fragmentation Threshold: 2346 (256-2346)

DTIM Interval: 1 (1-255)

Enable WMM

Enable AP Isolation

Save

Figure 4-18 Wireless Advanced

- **Transmit Power** - Here you can specify the transmit power of the Router. You can select **High**, **Middle** or **Low** as you like. **High** is the default setting and is recommended.
- **Beacon Interval** - The beacons are the packets sent by the Router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. You can specify a value between 40-1000 milliseconds. The default value is 100.

- **RTS Threshold** - Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the Router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold** - This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval** - This value determines the interval of the Delivery Traffic Indication Message (DTIM). You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable WMM** - WMM function can guarantee the packets with high- priority messages be transmitted preferentially. It is strongly recommended to enable this function.
- **Enable AP Isolation** - Isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

Be sure to click the **Save** button to save your settings on this page.

4.5.5 Wireless Statistics

This page shows **MAC Address**, **Current Status**, **Received Packets** and **Sent Packets** for each connected wireless station.

Wireless Statistics				
Current Connected Wireless Stations numbers: 1 <input type="button" value="Refresh"/>				
ID	MAC Address	Current Status	Received Packets	Sent Packets
1	00-0A-EB-00-23-11	AP-UP	0	755
<input type="button" value="Previous"/> <input type="button" value="Next"/>				

Figure 4-19 The router attached wireless stations

- **MAC Address** - The connected wireless station's MAC address
- **Current Status** - The connected wireless station's running status, one of STA-AUTH / STA-ASSOC / AP-UP / WPA / WPA-PSK /WPA2/WPA2-PSK/None
- **Received Packets** - Packets received by the station
- **Sent Packets** - Packets sent by the station

You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the **Refresh** button.

If the numbers of connected wireless stations go beyond one page, click the **Next** button to go to the next page and click the **Previous** button to return the previous page.

 **Note:**

This page will be refreshed automatically every 5 seconds.

4.6 DHCP

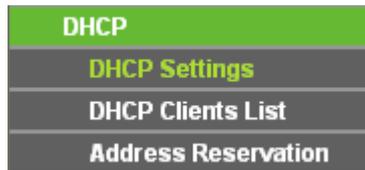


Figure 4-20 The DHCP menu

There are three submenus under the DHCP menu (shown in Figure 4-20): **DHCP Settings**, **DHCP Clients List** and **Address Reservation**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.6.1 DHCP Settings

The router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PC(s) that are connected to the router on the LAN. The DHCP Server can be configured on the page:

 A screenshot of the 'DHCP Settings' configuration page. The page has a green header with the title 'DHCP Settings'. Below the header, there are several configuration fields:

- DHCP Server:** Radio buttons for 'Disable' and 'Enable' (selected).
- Start IP Address:** Text input field containing '192.168.1.100'.
- End IP Address:** Text input field containing '192.168.1.199'.
- Address Lease Time:** Text input field containing '120', followed by the text 'minutes (1~2880 minutes, the default value is 120)'.
- Default Gateway:** Text input field containing '0.0.0.0' with '(optional)' to its right.
- Default Domain:** Text input field with '(optional)' to its right.
- Primary DNS:** Text input field containing '0.0.0.0' with '(optional)' to its right.
- Secondary DNS:** Text input field containing '0.0.0.0' with '(optional)' to its right.

 At the bottom of the form is a 'Save' button.

Figure 4-21 DHCP Settings

- **DHCP Server - Enable or Disable** the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must manually configure the computer.
- **Start IP Address** - This field specifies the first of the addresses in the IP address pool. 192.168.1.100 is the default start address.
- **End IP Address** - This field specifies the last of the addresses in the IP address pool. 192.168.1.199 is the default end address.
- **Address Lease Time** - The **Address Lease Time** is the amount of time in which a network user will be allowed connection to the router with their current dynamic IP Address. Enter the amount of time, in minutes. The user will be "leased" this dynamic IP Address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.
- **Default Gateway** - (Optional.) Suggest to input the IP address of the LAN port of the router, default value is 192.168.1.1

- **Default Domain** - (Optional.) Input the domain name of your network.
- **Primary DNS** - (Optional.) Input the DNS IP address provided by your ISP. Or consult your ISP.
- **Secondary DNS** - (Optional.) Input the IP address of another DNS server if your ISP provides two DNS servers.

 **Note:**

To use the DHCP server function of the router, you must configure all computers on the LAN as "Obtain an IP Address automatically" mode. This function will take effect until the router reboots.

4.6.2 DHCP Clients List

This page shows **Client Name**, **MAC Address**, **Assigned IP**, and **Lease Time** for each DHCP Client attached to the router:

DHCP Clients List				
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	lilo	00-0A-EB-13-09-1A	192.168.1.100	01:59:40

Figure 4-22 DHCP Clients List

- **Index** - The index of the DHCP Client
- **Client Name** - The name of the DHCP client
- **MAC Address** - The MAC address of the DHCP client
- **Assigned IP** - The IP address that the router has allocated to the DHCP client.
- **Lease Time** - The time of the DHCP client leased. Before the time is up, DHCP client will request to renew the lease automatically.

You cannot change any of the values on this page. To update this page and to show the current attached devices, click on the **Refresh** button.

4.6.3 Address Reservation

When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings. This page is used for address reservation.

Address Reservation				
ID	MAC Address	Reserved IP Address	Status	Modify
1	00-0A-EB-13-09-BB	192.168.1.100	Enabled	Modify Delete

Figure 4-23 Address Reservation

- **MAC Address** - The MAC address of the PC of which you want to reserve IP address.
- **Assigned IP Address** - The IP address of the router reserved.
- **Status** - The status of this entry either **Enabled** or **Disabled**.

To Reserve IP addresses:

1. Click the **Add New** button. (Pop-up Figure 4-23)
2. Enter the MAC address (The format for the MAC Address is XX-XX-XX-XX-XX-XX.) and IP address in dotted-decimal notation of the computer you wish to add.
3. Click the **Save** button when finished.

Add or Modify an Address Reservation Entry	
MAC Address:	<input type="text"/>
Reserved IP Address:	<input type="text"/>
Status:	Enabled <input type="button" value="v"/>

Figure 4-24 Add or Modify an Address Reservation Entry

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

Click the **Next** button to go to the next page and Click the **Previous** button to return the previous

Note:

The function won't take effect until the router reboots.

4.7 Forwarding

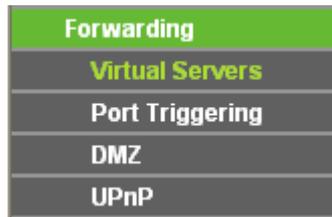


Figure 4-25 The Forwarding menu

There are four submenus under the Forwarding menu: **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.7.1 Virtual Servers

Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP Address because its IP Address may change when using the DHCP function. You can set up virtual servers on this page:

 A screenshot of the 'Virtual Servers' configuration page. At the top, there is a green header bar with the text 'Virtual Servers'. Below the header is a table with the following columns: ID, Service Ports, IP Address, Protocol, Status, and Modify. There is one row of data. Below the table, there are four buttons: 'Add New...', 'Enable All', 'Disable All', and 'Delete All'. At the bottom of the page, there are two buttons: 'Previous' and 'Next'.

ID	Service Ports	IP Address	Protocol	Status	Modify
1	21	192.168.1.101	ALL	Enabled	Modify Delete

Figure 4-26 Virtual Servers

- **Service Port** - The numbers of External Ports. You can type a service port or a range of service ports (the format is XXX – YYY, XXX is the start port, YYY is the end port).
- **IP Address** - The IP Address of the PC providing the service application.
- **Protocol** - The protocol used for this application, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- **Status** - The status of this entry either **Enabled** or **Disabled**.

To setup a virtual server entry:

1. Click the **Add New button**. (pop-up Figure 4-26)
2. Select the service you want to use from the Common Service Port list. If the **Common Service Port** list does not have the service that you want to use, type the number of the service port or service port range in the **Service Port** box.
3. Type the IP Address of the computer in the **Server IP Address** box.
4. Select the protocol used for this application, either **TCP** or **UDP**, or **All**.

5. Select the **Enable** checkbox to enable the virtual server.
6. Click the **Save** button.

The screenshot shows a web form titled "Add or Modify a Virtual Server Entry". The form contains the following fields and controls:

- Service Port:** A text input field with a hint "(000-XXX or XXX)".
- IP Address:** A text input field.
- Protocol:** A dropdown menu currently set to "ALL".
- Status:** A dropdown menu currently set to "Enabled".
- Common Service Port:** A dropdown menu currently set to "--Select One--".

At the bottom of the form, there are two buttons: "Save" and "Back".

Figure 4-27 Add or Modify a Virtual Server Entry

Note:

It is possible that you have a computer or server that has more than one type of available service. If so, select another service, and enter the same IP Address for that computer or server.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

Click the **Next** button to go to the next page and Click the **Previous** button to return the previous page.

Note:

If you set the virtual server of service port as 80, you must set the Web management port on Security → Remote Management page to be any value except 80 such as 8080. Or else there will be a conflict to disable the virtual server.

4.7.2 Port Triggering

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT router. Port Triggering is used for some of these applications that can work with an NAT router. You can set up Port Triggering on this page:

Port Triggering						
ID	Trigger Port	Trigger Protocol	Incoming Ports	Incoming Protocol	Status	Modify
1	554	ALL	6970-6999	ALL	Enabled	Modify Delete

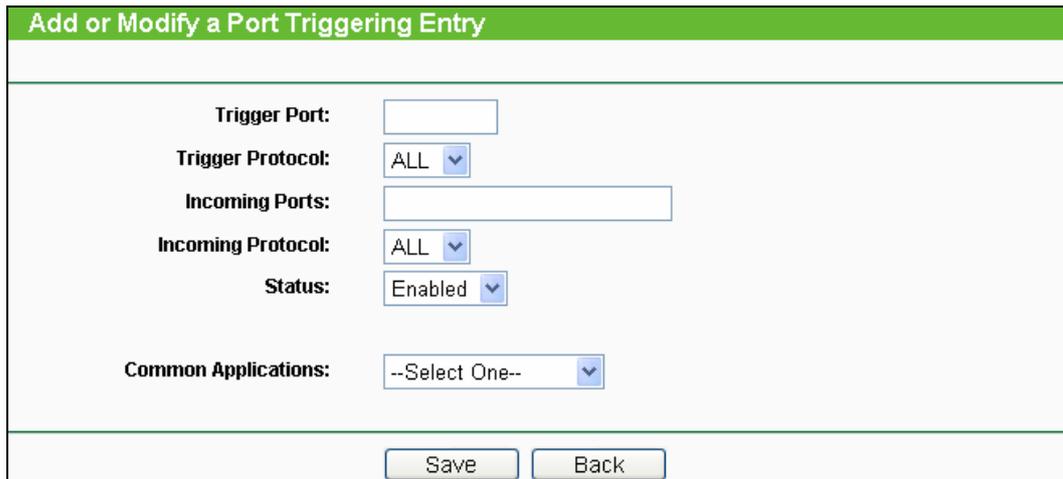
Figure 4-28 Port Triggering

Once configured, operation is as follows:

1. A local host makes an outgoing connection using a destination port number defined in the Trigger Port field.
 2. The router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.
 3. When necessary the external host will be able to connect to the local host using one of the ports defined in the **Incoming Ports** field.
- **Trigger Port** - The port for outgoing traffic. An outgoing connection using this port will "Trigger" this rule.
 - **Trigger Protocol** - The protocol used for Trigger Ports, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
 - **Incoming Ports** - The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of ports (or port section). Every group of ports must be set apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.
 - **Incoming Protocol** - The protocol used for Incoming Ports Range, either TCP or UDP, or ALL (all protocols supported by the router).
 - **Status** - The status of this entry either **Enabled** or **Disabled**.

To add a new rule, enter the following data on the **Port Triggering** screen.

1. Click the **Add New button**. (pop-up Figure 4-28)
2. Enter a port number used by the application when it generates an outgoing request.
3. Select the protocol used for **Trigger Port** from the pull-down list, either **TCP**, **UDP**, or **All**.
4. Enter the range of port numbers used by the remote system when it responds to the PC's request.
5. Select the protocol used for **Incoming Ports Range** from the pull-down list, either **TCP** or **UDP**, or **All**.
6. Select the **Enable** checkbox to enable.
7. Click the **Save** button to save the new rule.



Add or Modify a Port Triggering Entry

Trigger Port:

Trigger Protocol: ALL ▾

Incoming Ports:

Incoming Protocol: ALL ▾

Status: Enabled ▾

Common Applications: --Select One-- ▾

Save Back

Figure 4-29 Add or Modify a Triggering Entry

There are many popular applications in the **Popular Application** list. You can select it, and the application will fill in the **Trigger Port**, **incoming Ports Range** boxes and select the **Enable** checkbox. It has the same effect as adding a new rule.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

 **Note:**

When the trigger connection is released, the according opening ports will be closed.

Each rule allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.

Incoming Port Range cannot overlap each other.

4.7.3 DMZ

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may change when using the DHCP function. You can set up DMZ host on this page shown in figure 5-29:

Figure 4-30 DMZ

To assign a computer or server to be a DMZ server:

1. Click the **Enable** radio button
2. Enter the local host IP Address in the **DMZ Host IP Address** field

 **Note:**

After you set the DMZ host, the firewall related to the host will not work.

4.7.4 UPnP

The Universal Plug and Play (UPnP) feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN. You can configure UPnP on this page:

Figure 4-31 UPnP Settings

- **Current UPnP Status** - UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button. This feature is disabled by default.
- **Current UPnP Settings List** - This table displays the current UPnP information.
 - **App Description** – The description provided by the application in the UPnP request
 - **External Port** - External port, which the router opened for the application.
 - **Protocol** – Shows which type of protocol is opened.
 - **Internal Port** - Internal port, which the router opened for local host.
 - **IP Address** - The UPnP device that is currently accessing the router.
 - **Status** - Either Enabled or Disabled, “Enabled” means that port is still active. Otherwise, the port is inactive.

Click **Refresh** to update the Current UPnP Settings List.

4.8 Security

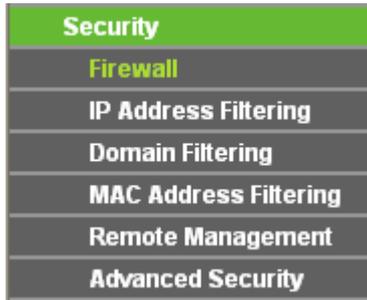


Figure 4-32 The Security menu

There are six submenus under the Security menu: **Firewall**, **IP Address Filtering**, **Domain Filtering**, **MAC Address Filtering**, **Remote Management** and **Advanced Security**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.8.1 Firewall

Using the Firewall page, you can turn the general firewall switch on or off. The default setting for the switch is off. If the general firewall switch is off, even if IP Address Filtering, DNS Filtering and MAC Filtering are enabled, their settings are ineffective.

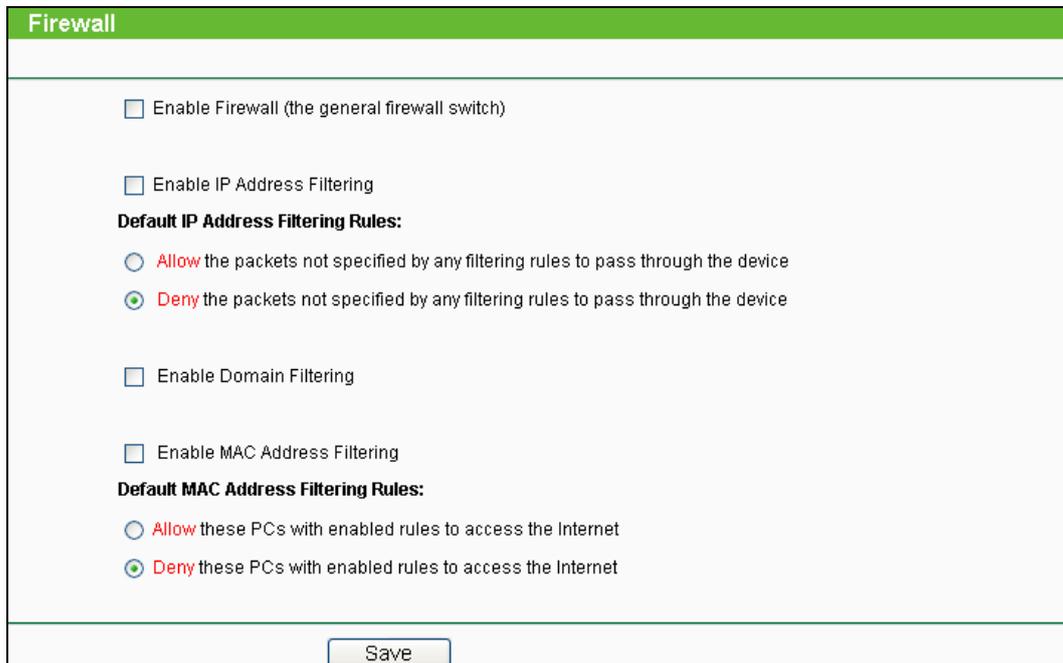
The Firewall settings page has a green header. It contains several checkboxes: "Enable Firewall (the general firewall switch)", "Enable IP Address Filtering", "Enable Domain Filtering", and "Enable MAC Address Filtering". Below "Enable IP Address Filtering" is a section titled "Default IP Address Filtering Rules:" with two radio button options: "Allow the packets not specified by any filtering rules to pass through the device" and "Deny the packets not specified by any filtering rules to pass through the device". Below "Enable MAC Address Filtering" is a section titled "Default MAC Address Filtering Rules:" with two radio button options: "Allow these PCs with enabled rules to access the Internet" and "Deny these PCs with enabled rules to access the Internet". A "Save" button is at the bottom.

Figure 4-33 Firewall Settings

- **Enable Firewall** - the general firewall switch is on or off.
- **Enable IP Address Filtering** - set IP Address Filtering is enabled or disabled. There are two default filtering rules of IP Address Filtering, either Allow or Deny passing through the router.
- **Enable Domain Filtering** - set Domain Filtering is enabled or disabled.
- **Enable MAC Filtering** - set MAC Address Filtering is enabled or disabled. You can select the default filtering rules of MAC Address Filtering, either Allow or Deny accessing the router.

4.8.2 IP Address Filtering

The IP address Filtering feature allows you to control Internet Access by specific users on your LAN based on their IP addresses. The IP address filtering is set on this page:

Figure 4-34 IP address Filtering

To disable the IP Address Filtering feature, keep the default setting, **Disabled**. To set up an IP Address Filtering entry, click **Enable** Firewall and **Enable** IP Address Filtering on the Firewall page, and click the **Add New...** button. The page "**Add or Modify an IP Address Filtering entry**" will appear shown in Figure 4-35:

Figure 4-35 Add or Modify an IP Address Filtering Entry

To create or modify an IP Address Filtering entry, please follow these instructions:

1. **Effective Time** - Enter a range of time in HHMM format, which point to the range time for the entry to take effect. For example, 0803 - 1705, the entry will take effect from 08:03 to 17:05.
2. **LAN IP Address** - Enter a LAN IP Address or a range of LAN IP addresses in the field, in dotted-decimal notation format. For example, 192.168.1.20 - 192.168.1.30. Keep the field open, which means all LAN IP Addresses have been put into the field.
3. **LAN Port** - Enter a LAN Port or a range of LAN ports in the field. For example, 1030 - 2000. Keep the field open, which means all LAN ports have been put into the field.
4. **WAN IP Address** - Enter a WAN IP Address or a range of WAN IP Addresses in the field, in dotted-decimal notation format. For example, 61.145.238.6 - 61.145.238.47. Keep the field open, which means all WAN IP Addresses have been put into the field.

5. **WAN Port** - Enter a WAN Port or a range of WAN Ports in the field. For example, 25 – 110. Keep the field open, which means all WAN Ports have been put into the field.
6. **Protocol** - Select which protocol is to be used, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
7. **Action** - Select either **Allow** or **Deny** through the router.
8. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
9. Click the **Save** button to save this entry.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

You can change the entry's order as desired. Fore entries are before hind entries. Enter the ID number in the first box you want to move and another ID number in second box you want to move to, and then click the **Move** button to change the entry's order.

Click the **Next** button to the next page and click the **Previous** button to return to the previous page.

For example: If you desire to block E-mail received and sent by the IP Address 192.168.1.7 on your local network, and to make the PC with IP Address 192.168.1.8 unable to visit the website of IP Address 202.96.134.12, while other PC(s) have no limit you should specify the following IP address filtering list:

ID	Effective time	LAN IP Address	LAN Port	WAN IP Address	WAN Port	Protocol	Action	Status	Modify
1	0000-2400	192.168.1.7	25	-	-	ALL	Deny	Enabled	Modify Delete
2	0000-2400	192.168.1.7	110	-	-	ALL	Deny	Enabled	Modify Delete
3	0000-2400	192.168.1.8	-	202.96.134.12	-	ALL	Deny	Enabled	Modify Delete

4.8.3 Domain Filtering

The Domain Filtering page allows you to control access to certain websites on the Internet by specifying their domains or key words.

ID	Effective time	Domain Name	Status	Modify
<input type="button" value="Add New..."/> <input type="button" value="Enable All"/> <input type="button" value="Disable All"/> <input type="button" value="Delete All"/>				
<input type="button" value="Previous"/> <input type="button" value="Next"/>				

Figure 4-36 Domain Filtering

Before adding a Domain Filtering entry, you must ensure that **Enable** Firewall and **Enable** Domain Filtering have been selected on the Firewall page. To Add a Domain filtering entry, click the **Add New...** button. The page "**Add or Modify a Domain Filtering entry** " will appear, shown in Figure 4-37:

Figure 4-37 Add or Modify a Domain Filtering entry

To add or modify a Domain Filtering entry, follow these instructions:

1. **Effective Time** - Enter a range of time in HHMM format specifying the time for the entry to take effect. For example, if you enter: 0803 - 1705, than the entry will take effect from 08:03 to 17:05.
2. **Domain Name** - Type the domain or key word as desired in the field. A blank in the domain field means all websites on the Internet. For example: www.xxyy.com.cn, .net.
3. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enabled All** button to make all entries enabled.

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

Click the **Next** button to go to the next page and the **Previous** button to return to the previous page.

For example: if you want to block the PC(s) on your LAN to access websites www.xxyy.com.cn, www.aabbcc.com and websites with .net in the end on the Internet while no limit for other websites, you should specify the following Domain filtering list:

ID	Effective time	Domain Name	Status	Modify
1	0000-2400	www.xxyy.com	Enabled	Modify Delete
2	0800-2000	www.aabbcc.com	Enabled	Modify Delete
3	0000-2400	.net	Enabled	Modify Delete

4.8.4 MAC Address Filtering

Like the IP Address Filtering page, the MAC Address Filtering page allows you to control access to the Internet by users on your local network based on their MAC Address.

Figure 4-38 MAC address Filtering

Before setting up MAC Filtering entries, you must ensure that **Enable Firewall** and **Enable MAC Filtering** have been selected on the Firewall page. To Add a MAC Address filtering entry, clicking the **Add New...** button. The page "**Add or Modify a MAC Address Filtering entry**" will appear, shown in Figure 4-39:

Figure 4-39 Add or Modify a MAC Address Filtering entry

To add or modify a MAC Address Filtering entry, follow these instructions:

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0E-AE-B0-00-0B.
2. Type the description of the PC in the **Description** field. Fox example: John's PC.
3. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

To add additional entries, repeat steps 1-4.

When finished, click the **Return** button to return to the **MAC Address Filtering** page.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.

2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled.

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

Click the **Next** button to go to the next page and click the **Previous** button to return to the previous page.

Fox example: If you want to block the PC with MAC addresses 00-0A-EB-00-07-BE and 00-0A-EB-00-07-5F to access the Internet, first, enable the **Firewall** and **MAC Address Filtering** on the **Firewall** page, then, you should specify the Default MAC Address Filtering Rule "**Deny these PC(s) with effective rules to access the Internet**" on the Firewall page and the following MAC address filtering list on this page:

ID	MAC Address	Description	Status	Modify
1	00-0A-EB-00-07-BE	John's computer	Enabled	Modify Delete
2	00-0A-EB-00-07-5F	Alice's computer	Enabled	Modify Delete

4.8.5 Remote Management

You can configure the Remote Management function on this page. This feature allows you to manage your Router from a remote location, via the Internet.

Remote Management	
Web Management Port:	<input type="text" value="80"/>
Remote Management IP Address:	<input type="text" value="0.0.0.0"/>
<input type="button" value="Save"/>	

Figure 4-40 Remote Management

- **Web Management Port** - Web browser access normally uses the standard HTTP service port 80. This router's default remote management Web port number is 80. For greater security, you can change the remote management Web interface to a custom port by entering that number in this box provided. Choose a number between 1024 and 65534, but do not use the number of any common service port.
- **Remote Management IP Address** - This is the current address you will use when accessing your router from the Internet. The default IP Address is 0.0.0.0. It means this function is disabled. To enable this function, change the default IP Address to another IP Address as desired.

To access the router, you will type your router's WAN IP Address into your browser's Address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For

example, if your Router's WAN address is 202.96.12.8 and you use port number 8080, enter in your browser: <http://202.96.12.8:8080>. You will be asked for the router's password. After successfully entering the password, you will be able to access the router's Web-based utility.

 **Note:**

Be sure to change the router's default password to a very secure password.

4.8.6 Advanced Security

Using Advanced Security page, you can protect the router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood from LAN.

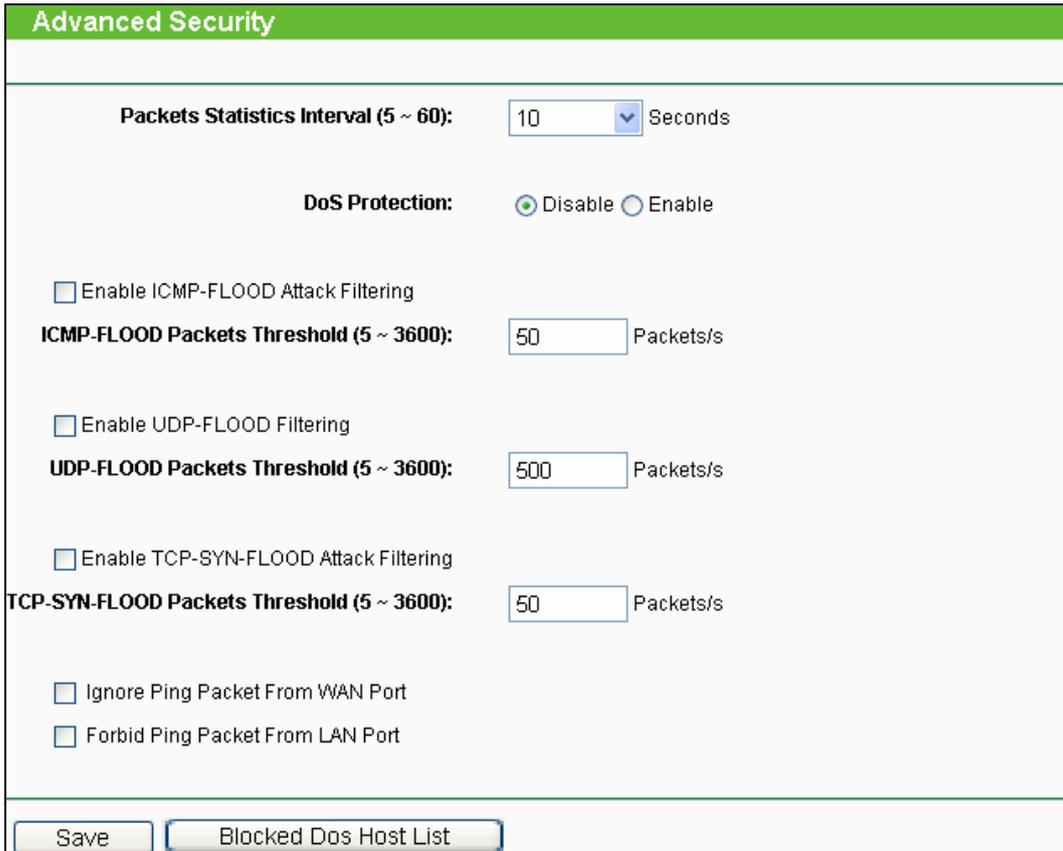


Figure 4-41 Advanced Security settings

- **Packets Statistic interval (5 ~ 60)** - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The **Packets Statistic interval** value indicates the time section of the packets statistic. The result of the statistic used for analysis by **SYN Flood**, **UDP Flood** and **ICMP-Flood**.
- **DoS protection - Enable** or **Disable** the DoS protection function. Only when it is enabled, will the flood filters be effective.
- **Enable ICMP-FLOOD Attack Filtering - Enable** or **Disable** the **ICMP-FLOOD** Attack Filtering.
- **ICMP-FLOOD Packets threshold: (5 ~ 3600)** - The default value is 50. Enter a value between 5 ~ 3600 packets. When the current **ICMP-FLOOD** Packets numbers is beyond the set value, the router will start up the blocking function immediately.
- **Enable UDP-FLOOD Filtering - Enable** or **Disable** the **UDP-FLOOD** Filtering.

- **UDP-FLOOD Packets threshold: (5 ~ 3600)** - The default value is 50. Enter a value between 5 ~ 3600 packets. When the current **UDP-FLOOD** Packets numbers is beyond the set value, the router will start up the blocking function immediately.
- **Enable TCP-SYN-FLOOD Attack Filtering** - **Enable** or **Disable** the **TCP-SYN- FLOOD** Attack Filtering.
- **TCP-SYN-FLOOD Packets threshold: (5 ~ 3600)** - The default value is 50. Enter a value between 5 ~ 3600 packets. When the current **TCP-SYN-FLOOD** Packets numbers is beyond the set value, the router will start up the blocking function immediately.
- **Ignore Ping Packet from WAN Port** - **Enable** or **Disable** ignore ping packet from WAN port. The default is disabled. If enabled, the ping packet from the Internet cannot access the router.
- **Forbid Ping Packet from LAN Port** - **Enable** or **Disable** forbidding Ping Packet to access the router from the LAN port. The default value is disabled. If enabled, the ping packet from the LAN port cannot access the router. (Defends against some viruses)

Click the **Save** button to save the settings.

Click the **Blocked DoS Host Table** button to display the DoS host table by blocking. The page will appear:

Blocked DoS Host List			
ID	Host IP Address	Host MAC Address	Modify
1	192.168.1.103	00-13-AA-6D-77	Delete

Figure 4-42 Thwarted DoS Host Table

This page shows **Host IP Address** and **Host MAC Address** for each host blocked by the router.

- **Host IP Address-** The IP address that blocked by DoS are displayed here.
- **Host MAC Address** - The MAC address that blocked by DoS are displayed here.

To update this page and to show the current blocked host, click on the **Refresh** button.

Click the **Clear All** button to clear all displayed entries. After the table is empty the blocked host will regain the capability to access Internet.

Click the **Return** button to return to the **Advanced Security** page.

4.9 Static Routing

A static route is a pre-determined path that network information must travel to reach a specific host or network. To add or delete a route, work in the area under the Static Routing page.

Static Routing					
ID	Destination IP Address	Subnet Mask	Default Gateway	Status	Modify
1	202.108.37.42	255.255.255.255	202.108.36.1	Enabled	Modify Delete

Figure 4-43 Static Routing

To add static routing entries:

1. Click the **Add New** button.
2. Enter the following data:
 - **Destination IP Address** - The **Destination IP Address** is the address of the network or host that you want to assign to a static route.
 - **Subnet Mask** - The **Subnet Mask** determines which portion of an IP Address is the network portion, and which portion is the host portion.
 - **Gateway** - This is the IP Address of the gateway device that allows for contact between the router and the network or host.
3. Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save it.

Add or Modify a Static Route Entry	
Destination IP Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default Gateway:	<input type="text"/>
Status:	Enabled <input type="button" value="v"/>

Figure 4-44 Add or Modify a Static Route Entry

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled.

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

4.10 IP QoS

You can configure the IP QoS function on this page.

ID	IP Range	Mode	Bandwidth	Description	Enable	Clear
1	192.168.1. - 192.168.1.	Minimum Bandwidth Guarantee			<input type="checkbox"/>	Clear
2	192.168.1. - 192.168.1.	Minimum Bandwidth Guarantee			<input type="checkbox"/>	Clear
3	192.168.1. - 192.168.1.	Minimum Bandwidth Guarantee			<input type="checkbox"/>	Clear
4	192.168.1. - 192.168.1.	Minimum Bandwidth Guarantee			<input type="checkbox"/>	Clear
5	192.168.1. - 192.168.1.	Minimum Bandwidth Guarantee			<input type="checkbox"/>	Clear
6	192.168.1. - 192.168.1.	Minimum Bandwidth Guarantee			<input type="checkbox"/>	Clear
7	192.168.1. - 192.168.1.	Minimum Bandwidth Guarantee			<input type="checkbox"/>	Clear
8	192.168.1. - 192.168.1.	Minimum Bandwidth Guarantee			<input type="checkbox"/>	Clear

Figure 4-45 IP QoS

- **Enable IP QoS** - Enable or disable the function of IP QoS.
- **Choose BandWidth Type** - Select the network connection type from the drop-down list.
- **Bandwidth Apply** - The bandwidth you get. If you are not clear about that, please contact with your ISP for help.
- **IP Range** - IP range of this entry.
- **Mode** - There are two types of mode: Minimum Bandwidth Guarantee and Maximum Bandwidth Limit.
- **Bandwidth** – The bandwidth you supply to this entry.
- **Description** – The description for this entry.

Click **Enable** to enable this entry.

Click the **Clear** button to clear a single entry.

Click the **Clear All** button to clear all entries.

Click the **Save** button to save all configurations.

Note:

1. The conversion relation of bandwidth: 1Mbps = 1000Kbps.
2. Please choose the Network Connection Type and set the bandwidth according to your Network. If you are not clear about that, please contact with your ISP for help.

3. If no IP QoS item is enabled, the Bandwidth Apply won't be effective.
4. IP address range for different entries could not have intersection with each other.
5. After the configurations, click the **Save** button for the change to take effect.

4.11 IP & MAC Binding Setting

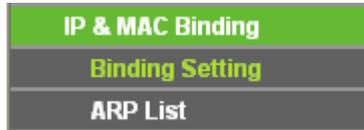


Figure 4-46 the IP & MAC Binding menu

There are two submenus under the IP & MAC Binding menu: **Binding Setting** and **ARP List**. Click any of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

4.11.1 Binding Setting

This page displays the IP & MAC Binding Setting table; you can operate it in accord with your desire..

Binding Settings				
		ARP Binding: <input checked="" type="radio"/> Disable <input type="radio"/> Enable		<input type="button" value="Save"/>
ID	MAC Address	IP Address	Bind	Modify
1	00-E0-4C-00-07-BE	192.168.1.4	<input checked="" type="checkbox"/>	Modify Delete
<input type="button" value="Add New..."/> <input type="button" value="Enable All"/> <input type="button" value="Delete All"/> <input type="button" value="Find"/>				
<input type="button" value="Previous"/> <input type="button" value="Next"/> Page 1 <input type="button" value="v"/>				

Figure 4-47 IP & MAC Binding Setting

- **MAC Address** - The MAC address of the controlled computer in the LAN.
- **IP Address** - The assigned IP address of the controlled computer in the LAN.
- **Bind** - Whether or not enable the arp binding.
- **Modify** - Edit or delete item.

When you want to add or modify an IP & MAC Binding entry, you can click the **Add New** button or **Modify** button, and then you will go to the next page. This page is used for adding or modifying an IP & MAC Binding entry.

Figure 4-48 IP & MAC Binding Setting (Add & Modify)

To add IP & MAC Binding entries:

1. Click the **Add New..** button.
2. Enter the MAC Address and IP Address.
3. Select the Bind checkbox.
4. Click the **Save** button to save it.

To modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Modify** or **Delete** as desired on the **Modify** column.

To find an existing entry:

1. Click the **Find** button (shown in Figure 4-47).
2. Enter the MAC Address or IP Address.
3. Enter the **Find** button in the next page (shown in Figure 4-49).

Figure 4-49 Find IP & MAC Binding Entry

Click the **Enable All** button to make all entries enabled.

Click the **Delete All** button to delete all entries.

4.11.2 ARP List

To manage the computer, you could observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could configure the items on

the ARP list also. This page displays the ARP List; it shows all the existing IP & MAC Binding entries.

ARP List				
ID	MAC Address	IP Address	Status	Configure
1	00-0A-EB-13-09-1A	192.168.1.77	Unbound	Load Delete
1	00-0A-EB-13-09-0B	192.168.1.2	Bound	Load Delete

Figure 4-50 ARP List

- **MAC Address** - The MAC address of the controlled computer in the LAN.
 - **IP Address** - The assigned IP address of the controlled computer in the LAN.
 - **Status** - Enabled or Disabled of the MAC address and IP address binding.
 - **Configure** - Load or delete item.
 - **Load** - Load the item to the IP & MAC Binding list.
 - **Delete** - Delete the item.
1. Click the **Bind All** button to bind all the current items, available after enable.
 2. Click the **Load All** button to load all items to the IP & MAC Binding list.
 3. Click the **Refresh** button to refresh all items.

 **Note:**

An item could not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before. Error warning will prompt as well. Likewise, "Load All" only loads the items without interference to the IP & MAC Binding list

4.12 Dynamic DNS

The router offers a Dynamic Domain Name System (**DDNS**) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP Address. It is useful when you are hosting your own website, FTP server, or other server behind the router. Before using this feature, you need to sign up for DDNS service providers such as www.dyndns.org, www.oray.net or www.comexe.cn. The Dynamic DNS client service provider will give you a password or key.

To set up for DDNS, follow these instructions:

4.12.1 Dyndns.org DDNS

If your selected dynamic DNS Service Provider is www.dyndns.org, the page will appear as shown in Figure 4-51:

DDNS

Service Provider: Dyndns (www.dyndns.org) [Go to register...](#)

User Name:

Password:

Domain Name:

Enable DDNS

Connection Status: DDNS not launching!

Figure 4-51 Dyndns.org DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **domain names** your dynamic DNS service provider gave.
 2. Type the **User Name** for your DDNS account.
 3. Type the **Password** for your DDNS account.
 4. Click the **Login** button to login to the DDNS service.
- **Connection Status** -The status of the DDNS service connection is displayed here. Click **Logout** to logout of the DDNS service.

4.12.2 Oray.net DDNS

If your selected dynamic DNS **Service Provider** is www.oray.net, the page will appear as shown in Figure 4-52:

DDNS

Service Provider: PeanutHull (www.oray.net) [Go to register...](#)

User Name:

Password:

Enable DDNS

Connection Status: DDNS not launching!

Service Type: ---

Domain Name: ---

Figure 4-52 Oray.net DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **User Name** for your DDNS account.
2. Type the **Password** for your DDNS account.
3. Click the **Login** button to login the DDNS service.
 - **Connection Status** - The status of the DDNS service connection is displayed here.
 - **Domain Name** - The domain names are displayed here.

Click **Logout** to logout the DDNS service.

4.12.3 Comexe.cn DDNS

If your selected dynamic DNS **Service Provider** is www.comexe.cn, the page will appear as shown in Figure 4-53:

The screenshot shows the DDNS configuration interface. At the top, a green bar contains the text 'DDNS'. Below this, the 'Service Provider' is set to 'Comexe (www.comexe.cn)' with a dropdown arrow and a 'Go to register...' link. There are five 'Domain Name' input fields. Below these are 'User Name' and 'Password' input fields. A checkbox for 'Enable DDNS' is present. The 'Connection Status' is 'DDNS not launching!'. There are 'Login' and 'Logout' buttons, and a 'Save' button at the bottom.

Figure 4-53 Comexe.cn DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **domain names** your dynamic DNS service provider gave.
 2. Type the **User Name** for your DDNS account.
 3. Type the **Password** for your DDNS account.
 4. Click the **Login** button to login to the DDNS service.
- **Connection Status** -The status of the DDNS service connection is displayed here.

Click **Logout** to logout of the DDNS service.

4.13 System Tools



Figure 4-54 The System Tools menu

There are nine submenus under the System Tools menu: **Time**, **Diagnostic**, **Firmware**, **Factory Defaults**, **Backup and Restore**, **Reboot**, **Password**, **Log** and **Statistics**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.13.1 Time

You can set time manually or get GMT from the Internet for the router on this page:

Figure 4-55 Time settings

- **Time Zone** - Select your local time zone from this pull-down list.
- **Date** - Enter your local date in MM/DD/YY into the right blanks.
- **Time** - Enter your local time in HH/MM/SS into the right blanks.

To set time manually, follow the steps below:

1. Select your local time zone.
2. Enter the **Date** in Month/Day/Year format.

3. Enter the **Time** in Hour/Minute/Second format.
4. Click **Save**.

For automatic time synchronization:

1. Enter the address of the **NTP Server Prior**.
2. Click the **Get GMT** button to get GMT time from Internet if you have connected to Internet.

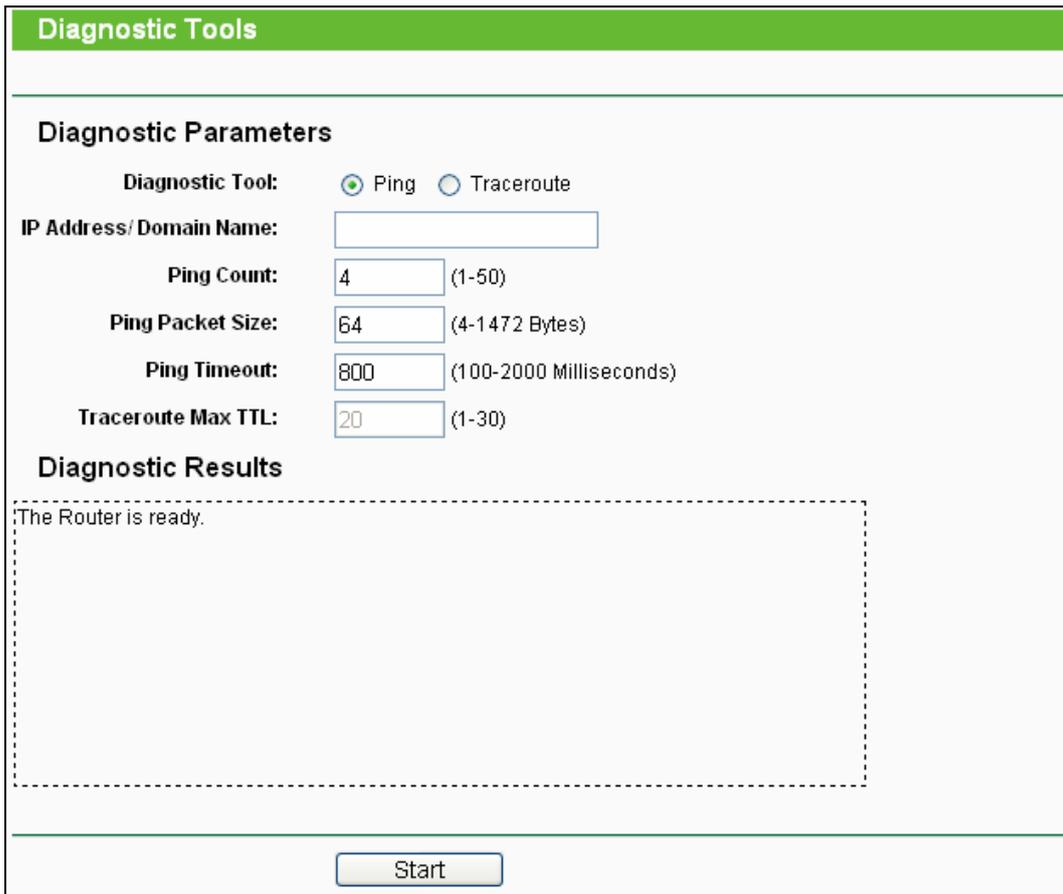
 **Note:**

This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, if not, the time limited on these functions will not take effect.

- The time will be lost if the router is turned off.
- The router will obtain GMT automatically from Internet if it has already connected to Internet.

4.13.2 Diagnostic

Choose menu "**System Tools** → **Diagnostic**", you can transact Ping or Traceroute function to check connectivity of your network in the following screen.



Diagnostic Tools

Diagnostic Parameters

Diagnostic Tool: Ping Traceroute

IP Address/ Domain Name:

Ping Count: (1-50)

Ping Packet Size: (4-1472 Bytes)

Ping Timeout: (100-2000 Milliseconds)

Traceroute Max TTL: (1-30)

Diagnostic Results

The Router is ready.

Figure 4-56 Diagnostic Tools

- **Diagnostic Tool** - Check the radio button to select one diagnostic tool.
 - **Ping** - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.

- **Traceroute** - This diagnostic tool tests the performance of a connection.

 **Note:**

You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- **IP Address/Domain Name** - Type the destination IP address (such as 202.108.22.5) or Domain name (such as www.baidu.com).
- **Pings Count** - The number of Ping packets for a Ping connection.
- **Ping Packet Size** - The size of Ping packet.
- **Ping Timeout** - Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.
- **Traceroute Max TTL** - The max number of hops for a Traceroute connection.

Click **Start** to check the connectivity of the Internet.

The **Diagnostic Results** page displays the result of diagnosis.

If the result is similar to the following screen, the connectivity of the Internet is fine.

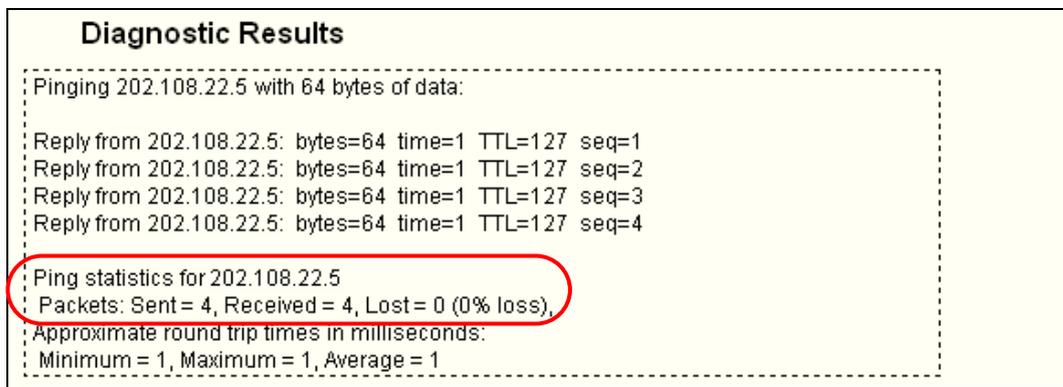


Figure 4-57 Diagnostic Results

 **Note:**

Only one user can use this tool at one time. "Ping Count", "Ping Packet Size" and "Ping Timeout" are Ping Parameters. "Traceroute Max TTL" is Traceroute Parameter.

4.13.3 Firmware

The page allows you to upgrade the latest version firmware to keep your router up-to-date.

Figure 4-58 Firmware Upgrade

New firmware is posted at <http://www.tp-link.com> and can be downloaded for free. If the router is not experiencing difficulties, there is no need to upgrade firmware, unless the new firmware supports a new feature you need.

Note:

When you upgrade the router's firmware, you will lose current configuration settings, so make sure you backup the router's settings before you upgrade its firmware.

To upgrade the router's firmware, follow these instructions:

1. Download the latest firmware upgrade file from the TP-LINK website <http://www.tp-link.com>.
 2. Enter or select the path name where you save the downloaded file on the computer into the **File** blank.
 3. Click the **Upgrade** button.
- **Firmware Version** - Displays the current firmware version.
 - **Hardware Version** - Displays the current hardware version. The hardware version of the upgrade file must accord with the current hardware version.

Note:

The firmware version must correspond to the hardware. The upgrade process takes a few minutes and the Router will restart automatically when the upgrade is completed. It is important to keep power on during the entire process. Loss of power during the upgrade could damage the Router.

4.13.4 Factory Defaults

This page allows you to restore the factory default settings for the router.

Figure 4-59 Restore Factory Default

Click the **Restore** button to reset all configuration settings to their default values.

- The default User Name: admin
- The default Password: admin

- The default access: tplinklogin.net

 **Note:**

Any settings you have saved will be lost when the default settings are restored.

4.13.5 Backup & Restore

This page allows you to save current configuration of router as backup or restore the configuration file you saved before.



Figure 4-60 Backup & Restore Configuration

- Click the **Backup** button to save all configuration settings as a backup file in your local computer.
- To restore the router's configuration, follow these instructions:
 - 1 Click the **Browse** button to select the backup file which you want to restore.
 - 2 Click the **Restore** button.

 **Note:**

The current configuration will be covered with the uploading configuration file. The restoration process lasts for 20 seconds and the router will restart automatically. Keep the router on during the restoring process to prevent any damage.

4.13.6 Reboot

This page allows you to reboot the router.

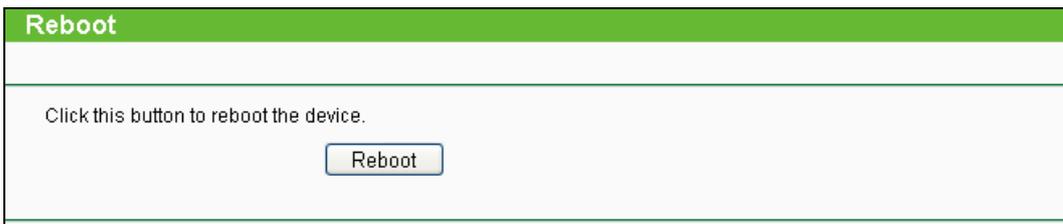


Figure 4-61 Reboot the router

Click the **Reboot** button to reboot the router.

Some settings of the router will take effect only after rebooting, which include:

- Change LAN IP Address. (System will reboot automatically)
- MAC Clone (system will reboot automatically)
- DHCP service function.
- Static address assignment of DHCP server.
- Web Service Port of the router.

- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router's settings to factory default (system will reboot automatically).

4.13.7 Password

This page allows you to change the factory default user name and password of the router.

Password	
Old User Name:	<input type="text" value="admin"/>
Old Password:	<input type="text"/>
New User Name:	<input type="text"/>
New Password:	<input type="text"/>
Confirm New Password:	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Clear All"/>	

Figure 4-62 Password

It is recommended strongly that you change the factory default user name and password of the router. All users who try to access the router's Web-based utility or Quick Setup will be prompted

Note:

The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.

Click the **Save** button when finished.

Click the **Clear All** button to clear all.

4.13.8 Syslog

This page allows you to query the logs of the router.

System Log	
Index	Log Content
1	0520:System: Logs were cleared.
Time = 2006-01-01 8:08:39 520s	
H-Ver = WR340G 4.0 00000000 : S-Ver = 4.17.9 Build 110329 Rel.45392n	
L = 192.168.1.1 : M = 255.255.255.0	
W1 = DHCP : W = 0.0.0.0 : M = 0.0.0.0 : G = 0.0.0.0	
Free=5028, Busy=2, Bind=0, Inv=0/2, Bc=0/4, Dns=82, cl=384, fc=0/0, sq=0/0	
<input type="button" value="Refresh"/> <input type="button" value="Clear All"/>	

Figure 4-63 System Log

The router can keep logs of all traffic. You can query the logs to find what happened to the router.

Click the **Refresh** button to refresh the logs.

Click the **Clear All** button to clear all the logs.

4.13.9 Statistics

The Statistics page displays the network traffic of each PC in LAN, including total traffic and traffic of the last **Packets Statistic interval** seconds.

Figure 4-64 Statistics

- **Current Statistics Status** - Enable or Disable. The default value is disabled. To enable, click the **Enable** button. If disabled, the function of DoS protection in Security settings will be ineffective.
- **Packets Statistics Interval** - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval indicates the time section of the packets statistic.
- **Sorted Rules** - Here displays sort as desired.

Statistics Table:

IP Address		The IP Address displayed with statistics
Total	Packets	The total amount of packets received and transmitted by the router.
	Bytes	The total amount of bytes received and transmitted by the router.
Current	Packets	The total amount of packets received and transmitted in the last Packets Statistic interval seconds.
	Bytes	The total amount of bytes received and transmitted in the last Packets Statistic interval seconds.
	ICMP Tx	The total amount of the ICMP packets transmitted to WAN in the last Packets Statistic interval seconds.
	UDP Tx	The total amount of the UDP packets transmitted to WAN in the last Packets Statistic interval seconds.
	TCP SYN Tx	The total amount of the TCP SYN packets transmitted to WAN in the last Packets Statistic interval seconds.

Click the **Save** button to save the **Packets Statistic interval** value.

Click the **Auto-refresh** checkbox to refresh automatically.

Click the **Refresh** button to refresh immediately.

Appendix A: FAQ

1. How do I configure the router to access Internet by ADSL users?

- 1) First, configure the ADSL Modem configured in RFC1483 bridge model.
- 2) Connect the Ethernet cable from your ADSL Modem to the WAN port on the router. The telephone cord plugs into the Line port of the ADSL Modem.
- 3) Login to the router, click the "Network" menu on the left of your browser, and click "WAN" submenu. On the WAN page, select "PPPoE" for WAN Connection Type. Type user name in the "User Name" field and password in the "Password" field, finish by clicking "Connect".

The screenshot shows the WAN Connection Type configuration page. The "WAN Connection Type" is set to "PPPoE". Under "PPPoE Connection", the "User Name" is "username" and the "Password" is masked with dots. The "Secondary Connection" is set to "Disabled". The "Wan Connection Mode" is set to "Connect on Demand" with a "Max Idle Time" of 15 minutes. The "Period of Time" is set from 0:00 to 23:59. The "Connect" button is highlighted, and the status is "Disconnected".

PPPoE Connection Type

- 4) If your ADSL lease is in "pay-according-time" mode, select "Connect on Demand" or "Connect Manually" for Internet connection mode. Type an appropriate number for "Max Idle Time" to avoid wasting paid time. Otherwise, you can select "Connect Automatically" for Internet connection mode.

The screenshot shows the WAN Connection Mode configuration page. The "WAN Connection Mode" is set to "Connect on Demand" with a "Max Idle Time" of 15 minutes. The "Period of Time" is set from 0:00 to 23:59. The "Connect" button is highlighted, and the status is "Disconnected".

PPPoE Connection Mode

Note:

Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.

If you are a Cable user, please configure the router following the above steps.

2. How do I configure the router to access Internet by Ethernet users?

- 1) Login to the router, click the "Network" menu on the left of your browser, and click "WAN" submenu. On the WAN page, select "Dynamic IP" for "WAN Connection Type", finish by clicking "Save".
- 2) Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable/DSL Modem during installation. If your ISP requires MAC register, login to the router and click the "Network" menu link on the left of your browser, and then click "MAC Clone" submenu link. On the "MAC Clone" page, if your PC's MAC address is proper MAC address, click the "Clone MAC Address" button and your PC's MAC address will fill in the "WAN MAC Address" field. Or else, type the MAC Address into the "WAN MAC Address" field. The format for the MAC Address is XX-XX-XX-XX-XX-XX. Then click the "Save" button. It will take effect after rebooting.

MAC Clone	
WAN MAC Address:	74-EA-3A-51-F7-07 <input type="button" value="Restore Factory MAC"/>
Your PC's MAC Address:	00-19-66-80-54-2B <input type="button" value="Clone MAC Address To"/>
<input type="button" value="Save"/>	

MAC Clone

3. I want to use Netmeeting, what do I need to do?

- 1) If you start Netmeeting as a sponsor, you don't need to do anything with the router.
- 2) If you start as a response, you need to configure Virtual Server or DMZ Host.
- 3) How to configure Virtual Server: Login to the router, click the "Forwarding" menu on the left of your browser, and click "Virtual Servers" submenu. On the "Virtual Server" page, click **Add New**, then on the "Add or Modify a Virtual Server" page, enter "1720" into the blank behind the "Service Port", and your IP address behind the IP Address, assuming 192.168.1.169 for an example, remember to "Enable" and "Save".

Virtual Servers					
ID	Service Ports	IP Address	Protocol	Status	Modify
1	1720	192.168.1.169	ALL	Enabled	Modify Delete
<input type="button" value="Add New..."/> <input type="button" value="Enable All"/> <input type="button" value="Disable All"/> <input type="button" value="Delete All"/>					
<input type="button" value="Previous"/> <input type="button" value="Next"/>					

Virtual Servers

Note:

Your opposite side should call your WAN IP, which is displayed on the "Status" page.

- 4) How to enable DMZ Host: Login to the router, click the "Forwarding" menu on the left of your browser, and click "DMZ" submenu. On the "DMZ" page, click "Enable" radio and type your IP address into the "DMZ Host IP Address" field, using 192.168.1.169 as an example, remember to click the "Save" button.

DMZ

4. I want to build a WEB Server on the LAN, what should I do?

Because the WEB Server port 80 will interfere with the WEB management port 80 on the router, you must change the WEB management port number to avoid interference.

To change the WEB management port number: Login to the router, click the "Security" menu on the left of your browser, and click "Remote Management" submenu. On the "Remote Management" page, type a port number except 80, such as 8080, into the "Web Management Port" field. Click "Save" and reboot the router.

Remote Management

Note:

If the above configuration takes effect, to configure to the router by typing <http://192.168.1.1:8080> in the address field of the web browser.

Login to the router, click the "Forwarding" menu on the left of your browser, and click the "Virtual Servers" submenu. On the "Virtual Server" page, enter "80" into the blank below the "Service Port", and your IP address below the IP Address, assuming 192.168.1.188 for an example, remember to "Enabled" and "Save".

Add or Modify a Virtual Server Entry

Service Port: (XX-XX or XX)

IP Address:

Protocol: ▼

Status: ▼

Common Service Port: ▼

Virtual Server

Appendix B: Configuring the PC

In this section, we'll introduce how to install and configure the TCP/IP correctly in Windows XP. First make sure your Ethernet Adapter is working, refer to the adapter's manual if necessary.

1. Configure TCP/IP component

- 1) On the Windows taskbar, click the **Start** button, and then click **Control Panel**.
- 2) Click the **Network and Internet Connections** icon, and then click on the **Network Connections** tab in the appearing window.
- 3) Right click the icon that showed below, select **Properties** on the prompt page.

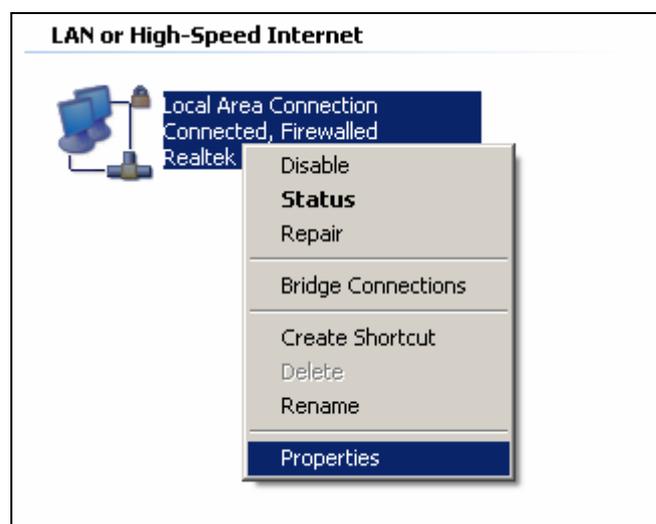


Figure 0-1

- 4) In the prompt page that showed below, double click on the **Internet Protocol (TCP/IP)**.

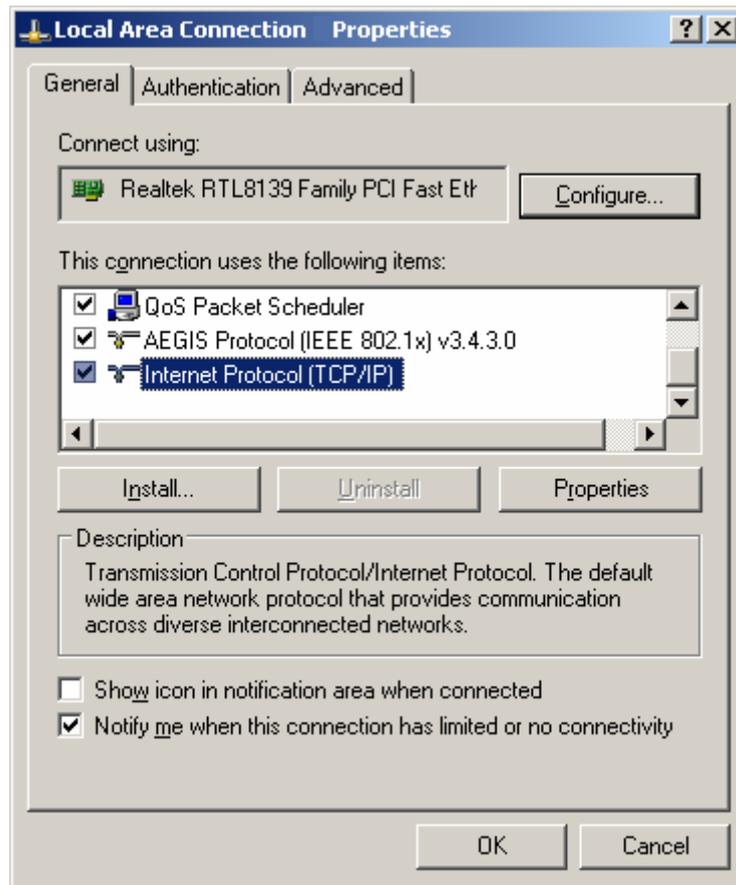


Figure 0-2

- 5) The following **TCP/IP Properties** window will display and the **IP Address** tab is open on this window by default.
- 6) Select **Obtain an IP address automatically**, Choose **Obtain DNS server automatically**, as shown in the Figure below:

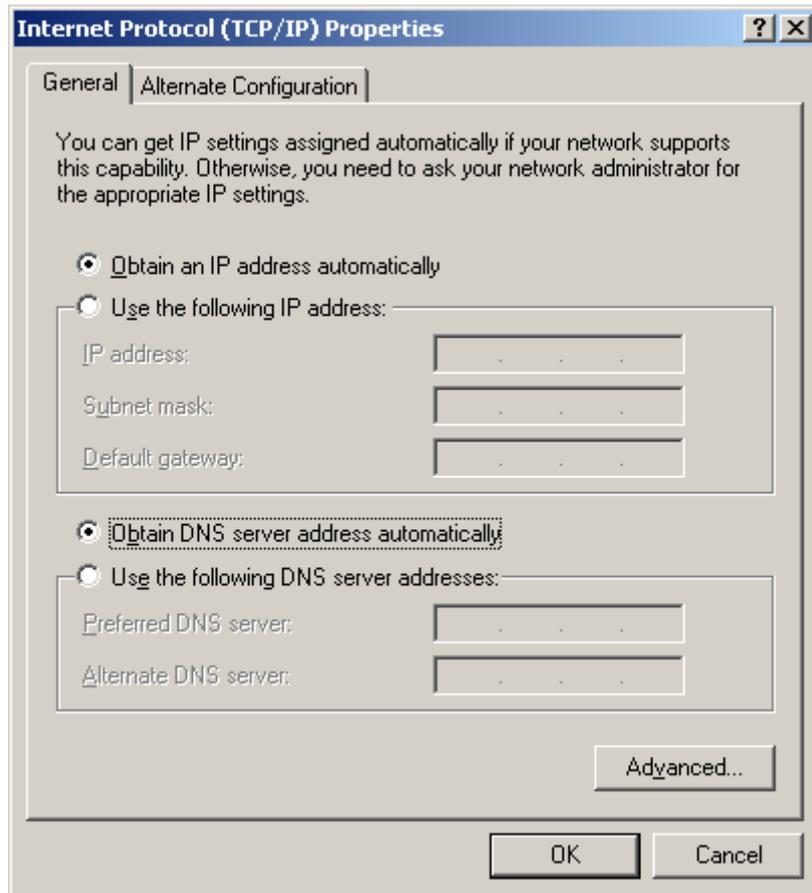


Figure 0-3

 **Note:**

For Windows 98 OS or before, the PC and Router may need to be restarted.

Appendix C: Specifications

General	
Standards and Protocols	IEEE 802.3, IEEE 802.3u, IEEE 802.11b and IEEE 802.11g TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Safety & Emission	FCC、CE
LEDs	Power, SYS, WLAN, WAN, 1-4
Ports	One 10/100M Auto-Negotiation WAN RJ45 port, Four 10/100M Auto-Negotiation LAN RJ45 ports supporting Auto MDI/MDIX
Wireless	
Modulation	IEEE 802.11b: DQPSK, DBPSK, DSSS, and CCK IEEE 802.11g: BPSK, QPSK, 16QAM, 64QAM, OFDM
Frequency*	2400 ~ 2483.5MHz
Wireless Data Rates	IEEE 802.11b: 1, 2, 5.5, and 11Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps
Media Access Protocol	CSMA/CA with ACK
Security	WEP/WPA/WPA2
Physical and Environment	
Working Temperature	0°C~40°C (32°F~104°F)
Storage Temperature	-40°C~70°C (-40°F~158°F)
Working Humidity	10% ~ 90% RH, Non-condensin
Storage Humidity	5% ~ 90% RH, Non-condensing

* Only 2.412GHz~2.462GHz is allowed to be used in USA, which means only channel 1~11 is available for American users to choose.

Appendix D: Glossary

Access Point - A device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

Ad-hoc Network - An ad-hoc network is a group of computers, each with a wireless adapter, connected as an independent IEEE 802.11 wireless LAN. Ad-hoc wireless computers operate on a peer-to-peer basis, communicating directly with each other without the use of an access point. Ad-hoc mode is also referred to as an Independent Basic Service Set (IBSS) or as peer-to-peer mode, and is useful at a departmental scale or SOHO operation.

AES (Advanced Encryption Standard) - A security method that uses symmetric 128-bit block data encryption.

ATM (Asynchronous Transfer Mode) - ATM is a cell based transfer mode that requires variable length user information to be segmented and reassembled to/from short, fixed length cells. It uses two different methods for carrying connectionless network interconnect traffic, routed and bridged Protocol Data Units (PDUs), over an ATM network.

Bridging - A device that connects different networks.

Browser - An application program that provides a way to look at and interact with all the information on the World Wide Web.

DDNS (Dynamic Domain Name System) - Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP - A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

DMZ (Demilitarized Zone) - Removes the Router's firewall protection from one PC, allowing it to be "seen" from the Internet.

DNS (Domain Name Server) - The IP address of your ISP's server, which translates the names of websites into IP addresses.