

---

# TP-LINK®

## User Guide

TL-WR542G

54Mbps Wireless Router



## COPYRIGHT &amp; TRADEMARKS

Specifications are subject to change without notice. **TP-LINK**<sup>®</sup> is the 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 © 2005 TP-LINK Technologies Co., Ltd. All rights reserved.

Package contents.....	4
Chapter 1: About this Guide .....	5
1.1 PURPOSES .....	5
1.2 CONVENTIONS .....	5
1.3 OVERVIEW OF THIS USER GUIDE .....	5
Chapter 2: Introduction.....	6
2.1 OVERVIEW OF THE ROUTER.....	6
2.2 FEATURES .....	6
2.3 PANEL LAYOUT .....	7
2.3.1 <i>The Front Panel</i> .....	7
2.3.2 <i>The Rear Panel</i> .....	8
Chapter 3: Connecting the Router .....	9
3.1 SYSTEM REQUIREMENTS .....	9
3.2 INSTALLATION ENVIRONMENT REQUIREMENTS .....	9
3.3 CONNECTING THE ROUTER .....	9
Chapter 4: Quick Installation Guide.....	11
4.1 TCP/IP CONFIGURATION.....	11
4.2 QUICK INSTALLATION GUIDE.....	12
Chapter 5: Configuring the Router .....	16
5.1 LOGIN.....	16
5.2 STATUS.....	16
5.3 SETUP WIZARD .....	17
5.4 NETWORK.....	17
5.4.1 <i>LAN</i> .....	18
5.4.2 <i>WAN</i> .....	18
5.4.3 <i>MAC Clone</i> .....	23
5.5 WIRELESS .....	24
5.5.1 <i>Wireless Settings</i> .....	25
5.5.2 <i>MAC Filtering</i> .....	27
5.5.3 <i>Wireless Statistics</i> .....	30
5.6 DHCP .....	30
5.6.1 <i>DHCP Settings</i> .....	31
5.6.2 <i>DHCP Clients List</i> .....	32
5.6.3 <i>Address Reservation</i> .....	32
5.7 FORWARDING .....	34
5.7.1 <i>Virtual Servers</i> .....	34
5.7.2 <i>Port Triggering</i> .....	36
5.7.3 <i>DMZ</i> .....	37
5.7.4 <i>UPnP</i> .....	38
5.8 SECURITY .....	39

---

5.8.1 Firewall.....	39
5.8.2 IP Address Filtering.....	40
5.8.3 Domain Filtering.....	42
5.8.4 MAC Filtering.....	44
5.8.5 Remote Management.....	45
5.8.6 Advanced Security.....	46
5.9 STATIC ROUTING.....	48
5.10 DDNS.....	49
5.10.1 Oray.net DDNS.....	50
5.10.2 Comexe.cn DDNS.....	50
5.11 SYSTEM TOOLS.....	51
5.11.1 Time.....	52
5.11.2 Firmware.....	52
5.11.3 Factory Defaults.....	53
5.11.4 Reboot.....	54
5.11.5 Password.....	54
5.11.6 Logs.....	55
5.11.7 Statistics.....	55
Appendix A: FAQ.....	57
Appendix B: Configuring the PCs.....	60
Appendix C: Specifications.....	65
Appendix D: Glossary.....	66
Appendix E: Contact Information.....	68

## Package contents

The following contents should be found in your box:

- One TL-WR542G 54Mbps Wireless Router
- One AC power Adapter for TL-WR542G 54Mbps Wireless Router
- One Resource CD for TL-WR542G 54Mbps Wireless Router, including:
  - ◆ This Guide
  - ◆ Other helpful Information
- Wall-mounting screws

Note: If any of the above contents is damaged or missing, please contact the retailer you purchased the TL-WR542G 54Mbps Wireless Router for assistance.

## Chapter 1: About this Guide

Thank you for choosing the TL-WR542G 54Mbps Wireless Router. The Router provides dedicated solution for Small Office/Home Office (SOHO) network. 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.

It adopts **2x to 3x eXtended Range™ WLAN transmission technology** so that transmission distance is 2-3 times of traditional 11g/b solutions, up to 855.36m tested in China. Transmission range is extended to 4-9 times.

It is easy, web-based setup for installation and management. Even though you may not be familiar with the Router, you may easily finish the configuration with the help of this guide. Before installing the Router, please look through this guide get to know all the router functions.

### 1.1 Purposes

This Guide tells you how to use the TL-WR542G 54Mbps Wireless Router.

### 1.2 Conventions

The Router mentioned in this Guide stands for TL-WR542G 54Mbps Wireless Router.

### 1.3 Overview of this User Guide

Chapter 1: About this Guide

Chapter 2: Introduction

Chapter 3: Connecting the Router

Chapter 4: Quick Installation Guide

Chapter 5: Configuring the Router

Appendix A: FAQ

Appendix B: Configuring the PCs

Appendix C: Specifications

Appendix D: Glossary

Appendix E: Contact Information

## Chapter 2: Introduction

### 2.1 Overview of the Router

The TL-WR542G 54Mbps Wireless Router integrates firewall, NAT-router and Wireless AP. Its design is dedicated to Small Office/Home Office (SOHO) Wireless network solution. The TL-WR542G 54Mbps Wireless Router will allow you to connect your network wirelessly better than ever, sharing Internet Access, files and fun, easily and securely.

In the most attentive wireless security, the TL-WR542G 54Mbps Wireless Router provides multiple protection measures. It can be set to turn off wireless network name (SSID) broadcast so that only station that have the SSID can be connected. The Router provides wireless LAN 64/128/152-bit WEP encryption security, and WPA and WPA-PSK authentication and TKIP/AES encryption security. It also supports VPN pass-through for sensitive data secure transmission.

The TL-WR542G 54Mbps Wireless Router complies with the IEEE802.11g/b standards so that data rate is up to 54Mbps. It adopts **2x to 3x eXtended Range™ WLAN transmission technology** so that transmission distance is 2-3 times of traditional 11g/b solutions, up to 855.36m tested in China. Transmission range is extended to 4-9 times. It is compatible with all IEEE802.11g and IEEE802.11b products.

The TL-WR542G 54Mbps Wireless Router provides flexible access control so that parents or network administrators can establish restricted access policies for children or staff. It is built-in NAT and DHCP server supporting static IP address distributing. It also supports Virtual Server and DMZ host for Port Triggering need, and Remote management and log so that network administrators can manage and monitor the network on real time.

The TL-WR542G 54Mbps Wireless Router is easy-to-manage. Quick Setup Wizard is supported and friendly help messages are provided for every step. So you can configure it quickly and share Internet access, files and fun.

### 2.2 Features

- Complies with IEEE802.11g, IEEE802.11b, IEEE802.3, IEEE802.3u standards
- Built in 4-port 10/100Mbps Switch
- Ethernet connection to a WAN device, such as a cable modem or DSL modem
- Adopts **2x to 3x eXtended Range™** WLAN transmission technology
- Shares data and Internet access for the network, connecting Internet through PPPoE on demand and disconnecting when idle
- Supports 54/48/36/24/18/12/9/6/11/5.5/3/2/1/0.5/0.25Mbps wireless LAN data transfer rates
- Provides 64/128/152-bit WEP encryption security

- Provides WPA and WPA-PSK authentication and TKIP/AES encryption security
- Provides wireless LAN ACL (Access Control List) filtering
- Built-in NAT and DHCP server supporting static IP address distributing
- Supports Virtual Server, Port Triggering, and DMZ host
- Built-in firewall supporting IP address filtering, Domain Name filtering, and MAC address filtering
- Supports connecting/disconnecting 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 staffs
- Supports TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
- Supports UPnP, Dynamic DNS, Static Routing, VPN pass-through
- Supports Traffic Stat.
- Supports ICMP-FLOOD, UDP-FLOOD, TCP-SYN-FLOOD filter
- Ignores Ping packets from WAN or LAN ports
- Supports firmware upgrade
- Supports Remote and Web management

## 2.3 Panel Layout

### 2.3.1 The Front Panel

The front panel of the TL-WR542G consists of several LED indicators, which is designed to indicate connections. Viewed from left to right. Table 2-1 describes the LEDs on the front panel of the Router.

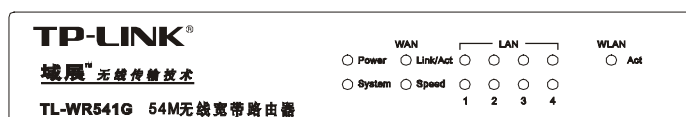


Figure 2-1: Front Panel sketch

Name	Action	Description
Power	Not lit	No Power
	Lit up	Power on
System	Lit up	The Router is Initializing
	Flashing	The Router works properly
	Not lit	The Router has a hardware error
Link/Act	Not lit	There is no device linked to the corresponding port
	Lit up	There is a device linked to the corresponding port but no activity
	Flashing	There is an active device linked to the corresponding port when activity
Speed	Not lit	The linked device is 10Mbps
	Lit up	The linked device is 100Mbps
WLAN	Not lit	The Wireless Radio function is disabled
	Flashing	The Wireless Radio function is enabled

Table 2-1 The LEDs description



### 2.3.2 The Rear Panel

The Rear panel contains the following features. (Viewed from left to right:)

- Wireless antenna
- Factory Default Reset button

There are two ways to reset the Router's factory defaults:

1. Use the **Factory Defaults** function on **System Tools** -> **Factory Defaults** page in the Router's Web-based Utility.
2. Use the Factory Default Reset button: First, turn off the Router's power. Second, press and hold the default reset button then turn on the Router's power, until the system LED light up (about 3 seconds). Last, release the reset button and wait for the router to reboot.

Note: Ensure the Router is powered on before it restarts completely

- WAN RJ45 port for connecting the Router to a cable or DSL modem
- Four LAN 10/100Mbps RJ45 ports for connecting the Router to the local PCs
- AC power socket: only use the Power adapter supplied with the TL-WR542G 54Mbps Wireless Router, use of a different adapter may result in product damage.

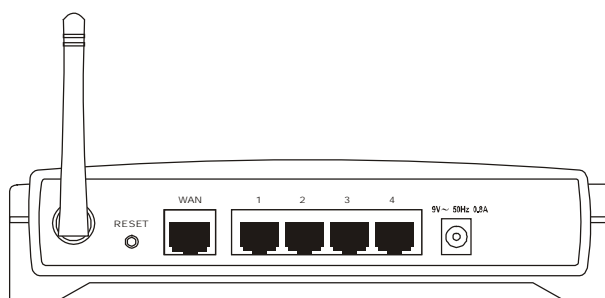


Figure 2-2: Rear Panel sketch

## Chapter 3: Connecting the Router

### 3.1 System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable modem that has RJ45 connector (you do not need it if you connect the Router to Ethernet)
- Each PC on the LAN needs working Ethernet NIC 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

### 3.2 Installation Environment Requirements

- Not in direct sunlight or near a heater or heating vent
- Not cluttered or crowded. There should be at least 2 inches (5 cm) of clear space on all sides of the switch
- Well ventilated (especially if it is in a closet)
- Operating temperature: 0°C~40°C (32°F~104°F)
- Operating Humidity: 10%~90%RH, Non-condensing

### 3.3 Connecting the Router

Before you install the Router, you should have connected your PC to the Internet through your broadband service successfully. If there is any problem, please contact 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) Power off your PCs, Cable or DSL modem and the Router.
- 2) Locate an optimum location for the Router. The best place is usually near the center of the area in which your PCs will wirelessly connect. The place must accord with the [Installation Environment Requirements](#).
- 3) Adjust the direction of the antenna. Normally, upright is a good direction.
- 4) Connect the PCs and each Switch/Hub on your LAN to the LAN Ports on the Router, shown in figure 3-1.
- 5) Connect the DSL/Cable Modem to the WAN port on the Router, shown in figure 3-1.
- 6) 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.
- 7) Power on Your PCs and Cable or DSL modem.

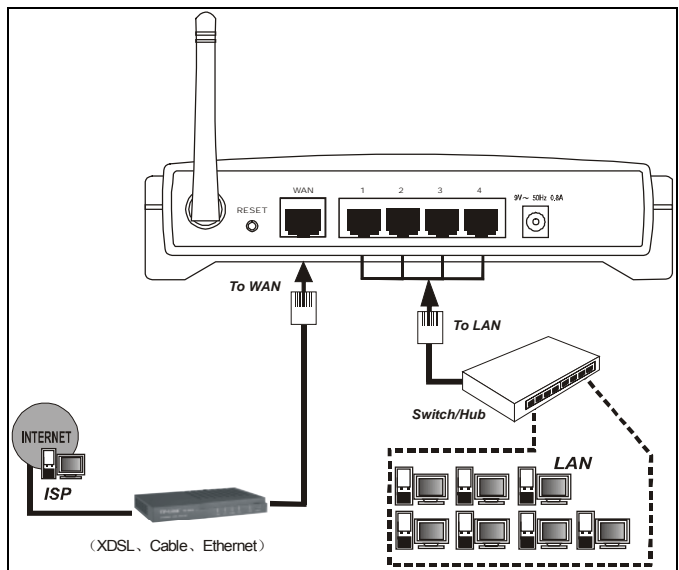


Figure 3-1: Physical Installation of the TL-WR542G 54Mbps Wireless Router

## Chapter 4: Quick Installation Guide

After connecting the TL-WR542G Router into your network, you should configure it. This chapter describes how to configure the basic functions of your TL-WR542G Wireless Router. These procedures only take you few minutes. You can access Internet via the Router immediately after successfully configured.

### 4.1 TCP/IP configuration

Default IP address of the TL-WR542G 54Mbps Wireless Router is 192.168.1.1, and default Subnet Mask is 255.255.255.0. These values can be seen from the LAN. They can be changed as you desire, but in this User Guide, we use the default values for description.

Connect the local PCs to the LAN ports on the Router. And then, there are two means to configure the IP address for your PCs.

- Configure the IP address manually
  - 1) Set up the TCP/IP Protocol for your PCs. If you need instructions on how to do this, please refer to [Appendix B: "Configuring the PCs."](#)
  - 2) Configure the network parameters. IP address is 192.168.1.xxx ("xxx" is from 2 to 254), Subnet Mask is 255.255.255.0, and Gateway is 192.168.1.1 (The Router's default IP address)
- Obtain an IP address automatically
  - 1) Set up the TCP/IP Protocol in "**Obtain an IP address automatically**" mode for your PCs. If you need instructions on how to do this, please refer to [Appendix B: "Configuring the PCs."](#)
  - 2) Power off the Router and PCs. Then power on the Router first, and then restart the PCs. The built-in DHCP server will assign IP addresses for the PCs.

Now, you can run the Ping command in the **command prompt** mode to verify the network connection between your PCs and the Router. The following example is in Windows 2000 OS.

Open a command prompt, and type *ping 192.168.1.1*, then press **Enter** key.

If the result displayed similar to that shown in Figure 4-1:

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<10ms TTL=64
Reply from 192.168.1.1: bytes=32 time<10ms TTL=64
Reply from 192.168.1.1: bytes=32 time<10ms TTL=64
Reply from 192.168.1.1: bytes=32 time<10ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 4-1: Successful result of Ping command

Congratulations! The connection between your PC and the Router has been established. If the result displayed similar to that shown in Figure 4-2:

```
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 4-2: Failed result of Ping command

It means that your PC has not connected to the Router. Please check it following these steps:

- 1) Is the connection between your PC and the Router correct?  
Note: The Link/Act LEDs of LAN port on the Router and LEDs on your PC's adapter should be lit.
- 2) Is the TCP/IP configuration for your PC proper?  
Note: If the Router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254, Gateway must be 192.168.1.1

## 4.2 Quick Installation Guide

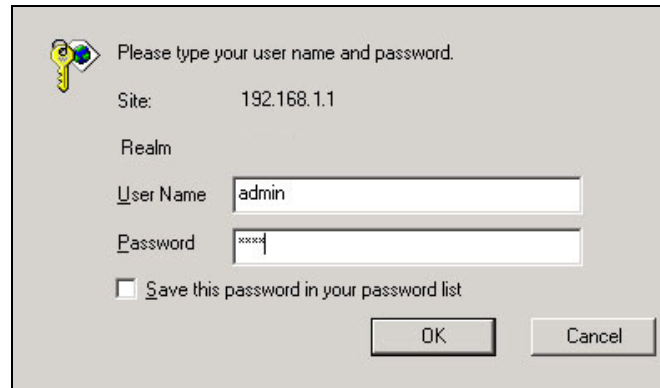
With Web-based (Internet Explorer or Netscape® Navigator) utility, the TL-WR542G 54Mbps Wireless Router is easy to configure and manage. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with web browser.

Connect to the Router by typing *http://192.168.1.1* in the address field of web browser.



Figure 4-3: Login to the Router

After a moment, a login window will appear similar to that shown in Figure 4-4. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press **Enter** key.



Please type your user name and password.

Site: 192.168.1.1

Realm

User Name: admin

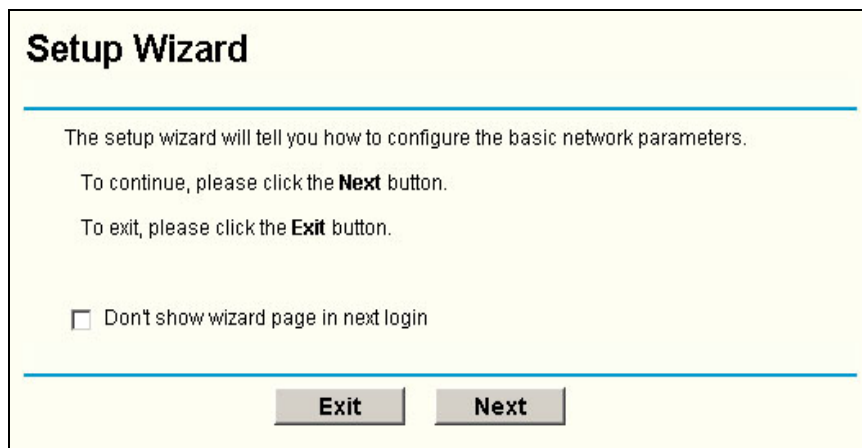
Password: xxxxx

Save this password in your password list

OK Cancel

Figure 4-4: Login Windows

If the User Name and Password are correct, the Setup Wizard page will appear, shown in figure 4-5. If not, please click the **Setup Wizard** link on the left of the main menu.



### Setup Wizard

The setup wizard will tell you how to configure the basic network parameters.

To continue, please click the **Next** button.

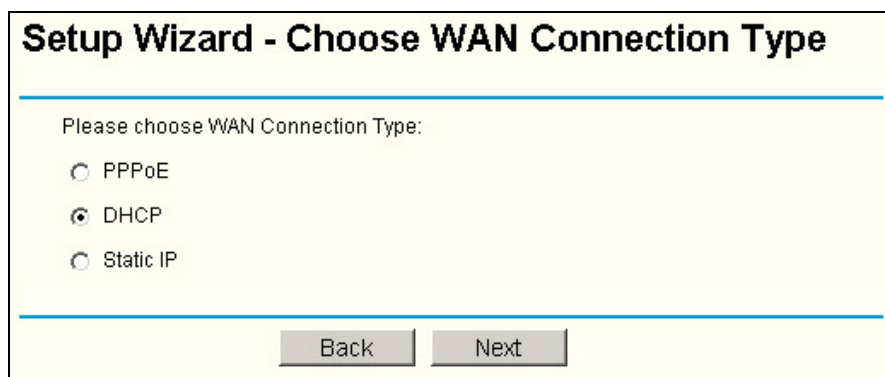
To exit, please click the **Exit** button.

Don't show wizard page in next login

Exit Next

Figure 4-5: Setup Wizard

Click **Next** button, the **Choose WAN Connection Type** page will appear, shown in figure 4-6.



### Setup Wizard - Choose WAN Connection Type

Please choose WAN Connection Type:

PPPoE

DHCP

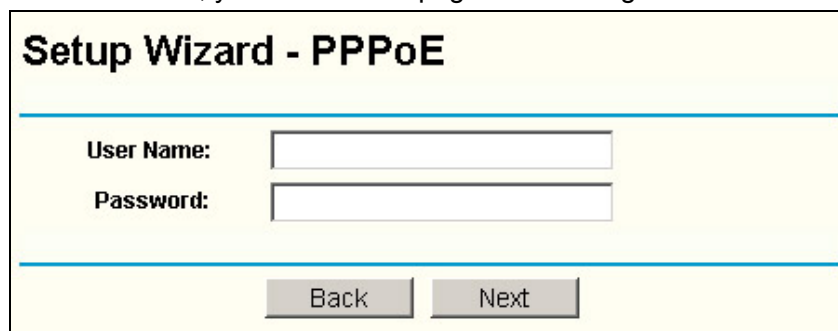
Static IP

Back Next

Figure 4-6: Choose WAN Connection Type

The TL-WR542G 54Mbps Wireless Router supports three popular ways to connect to Internet. Please select the exact one according to your ISP. And then click **Next** button to enter the necessary network parameters.

- 1) If you choose "PPPoE", you will see this page shown in figure 4-7:



**Setup Wizard - PPPoE**

User Name:

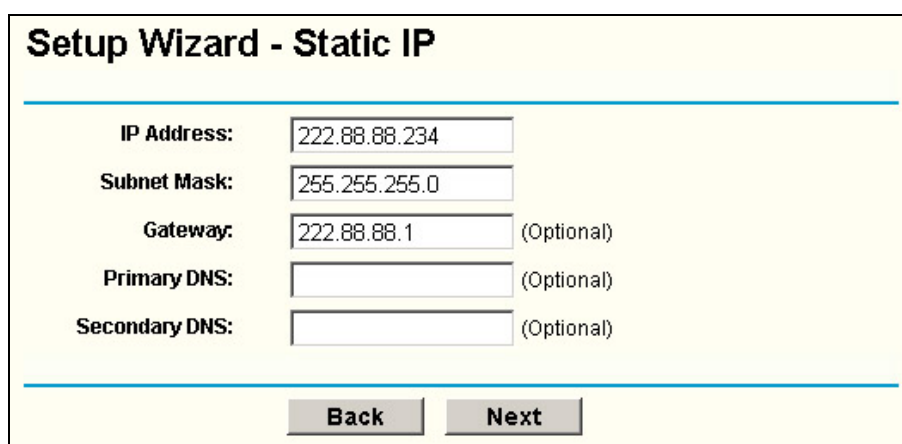
Password:

Back Next

Figure 4-7: Setup Wizard - PPPoE

**User Name and 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 you choose "DHCP", the Router will automatically get IP parameter from your ISP without entering any parameter.
- 3) If you Choose "**Static IP**", the Static IP settings page will appear that shown in figure 4-8:



**Setup Wizard - Static IP**

IP Address:

Subnet Mask:

Gateway:  (Optional)

Primary DNS:  (Optional)

Secondary DNS:  (Optional)

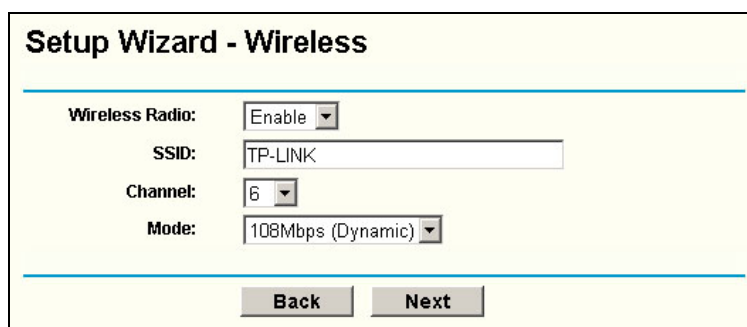
Back Next

Figure 4-8: Setup Wizard - Static IP

Note: The IP parameters should have been provided by your ISP.

- **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 WAN IP address, usually is 255.255.255.0
- **Default Gateway** - Enter the gateway into the box if required.
- **Primary DNS** - Enter the DNS Server IP address into the boxes if required.
- **Secondary DNS** - If your ISP provides another DNS server, enter it into this field.

After you complete the above, click **Next** button, the Wireless settings page will appear, shown in figure 4-9.



**Setup Wizard - Wireless**

Wireless Radio:

SSID:

Channel:

Mode:

Figure 4-9: Setup Wizard - Wireless settings

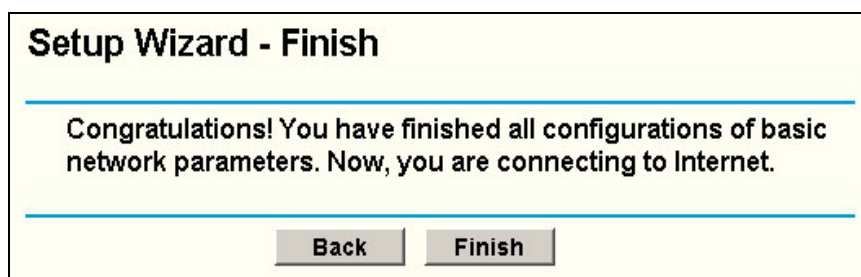
In the page, you can configure the follow wireless parameter:

- **Wireless Radio** - indicates whether the Access Point feature of the Router is enabled or not. If disabled, the WLAN LED on the front panel will not be lit and wireless stations will not be able to access the Router. If enabled, the WLAN LED will be lit up and wireless stations will be able to access the Router.
- **SSID** - Enter a value of up to 32 characters. The same SSID must be assigned to all wireless devices in your network. The default SSID is TP-LINK. This value is case-sensitive. For example, *TP-LINK* is NOT the same as *TP-Link*.
- **Channel** - the current channel in use. This field determines which operating frequency will be used.
- **Mode** - Indicates the current mode (**54Mbps (802.11g)**, **11Mbps (802.11b)**). If you select **54Mbps (802.11g)**, it is compatible with **11Mbps (802.11b)**.

These settings are only for basic wireless parameters, for advanced settings, please refer to [section 5.5: "Wireless."](#)

Note: The change of wireless settings won't take effect until the Router reboots! You can reboot it manually. If you need instructions on how to do this, please refer to [section 5.11.3: "rebooting the Router"](#)

Click Next button, you will see the Finish page:



**Setup Wizard - Finish**

**Congratulations! You have finished all configurations of basic network parameters. Now, you are connecting to Internet.**

Figure 4-10: Setup Wizard - Finish

After finishing all configurations of basic network parameters, please click **Finish** button to exit this **Setup Wizard**.



## Chapter 5: Configuring the Router

This chapter describes each web page's key functions.

### 5.1 login

After your successful login, you can configure and manage the Router. There are ten main menus on the left of the web-based utility. Submenus will be available after you click one of the main menus. The ten main menus are: **Status, Setup Wizard, Network, Wireless, DHCP, Forwarding, Security, Static Routing, DDNS and System Tools**. 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.

There are the detailed explanations for each web page's key functions below.

### 5.2 Status

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

#### 1) LAN

This field displays the current settings or information for LAN, including **MAC address, IP address and Subnet Mask**.

#### 2) Wireless

This field displays basic information or status for wireless function, including **Wireless Radio, SSID, Channel, Mode, Wireless MAC address and IP address**.

#### 3) 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 for WAN connection type, the **Disconnect** button will be shown here while you are accessing the Internet. You also can cut the connection by clicking the button. If you have not connected to the Internet, a **Connect** button will be shown, you can then establish the connection by clicking the button.

#### 4) Traffic Statistics

This field displays the Router's traffic statistics.

#### 5) System Active Time

The time of the Router running from it's powered on or reset.

### Router Status

---

**LAN**

**MAC Address:** 00-0A-EB-C9-98-76

**IP Address:** 192.168.1.1

**Subnet Mask:** 255.255.255.0

---

**Wireless**

**Wireless Radio:** Enabled

**SSID:** TP-LINK

**Channel:** 6

**Mode:** 108Mbps (Dynamic)

**MAC Address:** 00-0A-EB-C9-98-76

**IP Address:** 192.168.1.1

---

**WAN**

**MAC Address:** 00-0A-EB-C9-98-77

**IP Address:** 0.0.0.0 PPPoE

**Subnet Mask:** 0.0.0.0

**Default Gateway:** 0.0.0.0

**DNS Server:**

**Online Time:** 0 day 00:00:00

---

**Traffic Statistics**

	Received	Send
<b>Bytes:</b>	0	1368
<b>Packets:</b>	0	22

---

**System Active Time:** 0 day 00:02:08

Figure 5-1: Router status

### 5.3 Setup Wizard

Please refer to [Section 4.2: "Quick Installation Guide."](#)

### 5.4 Network

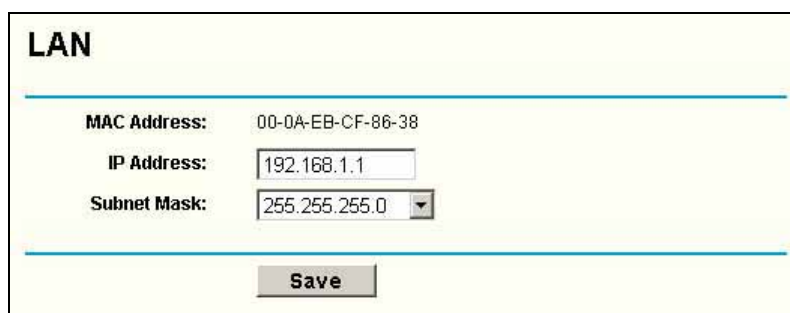


Figure 5-2: the Network menu

There are three submenus under the Network menu (shown in figure 5-2): **LAN**, **WAN** and **MAC Clone**. Click any of them, and you can configure the corresponding function. The detailed explanations for every submenu are provided below.

#### 5.4.1 LAN

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



The screenshot shows a web interface for configuring LAN settings. The title is "LAN". Below the title, there are three rows of configuration options:

- MAC Address:** 00-0A-EB-CF-86-38
- IP Address:** 192.168.1.1
- Subnet Mask:** 255.255.255.0

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

Figure 5-3: 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:

- a. If you change the IP Address of LAN, you must use the new IP Address to login the Router.
- b. If the new LAN IP Address you set is not in the same subnet, the IP Address pool in the DHCP sever will not take effect, until they are re-configured.
- c. 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.

#### 5.4.2 WAN

You can configure the WAN port parameters on this page.

First, please choose the WAN Connection Type (DHCP/Static IP/PPPoE/802.1x + DHCP/802.1x + Static IP) to the Internet. The default type is **DHCP**. If you aren't given any login parameters (fixed IP Address, logging ID, etc), please select **DHCP**. 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 PPPoE. If you are not sure which connection type you use currently, please contact your ISP to obtain the correct information.

1. If you choose **DHCP**, the Router will automatically get IP parameters from your ISP. You can see the page as follows (figure 5-4):

The screenshot shows the WAN configuration interface for a TL-WR542G router. The title is "WAN". The "WAN Connection Type" is set to "DHCP". The IP Address, Subnet Mask, and Default Gateway are all set to "0.0.0.0". There are "Renew" and "Release" buttons below the IP fields. The "MTU Size (in bytes)" is set to "1500" with a note: "(The default is 1500, don't change it if not necessary.)". There is a checkbox for "Use These DNS Servers" which is unchecked. Below it, "Primary DNS" and "Secondary DNS" are both set to "0.0.0.0" with a note "(optional)". There is another checkbox for "Get IP with Unicast DHCP (It is not needed usually.)" which is unchecked. A "Save" button is at the bottom.

Figure 5-4 WAN - DHCP

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

**Note:** If you get 'Address not found' errors 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 can't get the IP Address normally, you can choose this option. (You need not check this option usually).

If you are also given a user name and a password for 802.1x authentication, you should select **802.1x + DHCP** for **WAN Connection Type**, and a user name and a password will appear shown in figure 5-4a:

The screenshot shows a configuration window for WAN Connection Type. At the top, 'WAN Connection Type:' is set to '802.1X + DHCP' in a dropdown menu. Below this are two text input fields: 'User Name:' and 'Password:'. At the bottom of the form are two buttons: 'Login' and 'Logout'.

Figure 5-4a: WAN - 802.1X + DHCP

- **User Name** - Enter the user name for 802.1x authentication provided by your ISP
  - **Password** - Enter the password for 802.1x authentication provided by your ISP. Click **Login** button to start 802.1x authentication. Click **Logout** button to end 802.1x authentication.
2. If you choose **Static IP**, you should have fixed IP Parameters specified by ISP. The Static IP settings page will appear that shown in figure 5-5:

The screenshot shows the 'WAN' configuration page. The title 'WAN' is at the top left. Below it, 'WAN Connection Type:' is set to 'Static IP' in a dropdown menu. The form contains several input fields: 'IP Address:' (0.0.0.0), 'Subnet Mask:' (0.0.0.0), 'Default Gateway:' (0.0.0.0) with '(optional)' to its right, 'MTU Size (in bytes):' (1500) with '(The default is 1500, don't change it if not necessary.)' to its right, 'Primary DNS:' (empty) with '(optional)' to its right, and 'Secondary DNS:' (empty) with '(optional)' to its right. At the bottom center is a 'Save' button.

Figure 5-5: WAN - Static IP

You should type the following parameters on the page:

- **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, type 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 are also given a user name and a password for 802.1x authentication, you should select **802.1x + Static IP** for **WAN Connection Type**, and a user name and a password will appear shown in figure 5-5a:

The screenshot shows a configuration panel for 'WAN Connection Type'. The dropdown menu is set to '802.1X + Static IP'. Below this, there are two text input fields: 'User Name' and 'Password'. At the bottom of the panel are two buttons: 'Login' and 'Logout'.

Figure 5-5a: WAN - 802.1X + Static IP

- **User Name:** Enter the user name for 802.1x authentication provided by your ISP
- **Password:** Enter the password for 802.1x authentication provided by your ISP. Click **Login** button to start 802.1x authentication. Click **Logout** button to end 802.1x authentication.

3. If you choose **PPPoE**, you should enter the following parameters (figure 5-6):

The screenshot shows the 'WAN' configuration page. The 'WAN Connection Type' dropdown is set to 'PPPoE'. Below it, the 'User Name' field contains 'username' and the 'Password' field contains '\*\*\*\*\*'. The 'WAN Connection Mode' section has 'Connect on Demand' selected, with a 'Max Idle Time' of 0 minutes. There are also options for 'Connect Automatically', 'Time-based Connecting', and 'Connect Manually'. At the bottom are 'Connect', 'Disconnect', 'Save', and 'Advanced' buttons.

Figure 5-6: WAN - PPPoE

- **User Name/Password:** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **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.
- **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 connecting or disconnecting based on time. Enter the start time in HH:MM for connecting and end time in HH:MM for disconnecting in the **Period of Time** fields.  
Note: Only when you have set the system time on **System Tools -> Time** page, the **Time-based Connecting** function can take effect.
- **Connect Manually:** You can configure the Router connecting or disconnecting manually. After a specified period of inactivity (**Max Idle Time**), the Router will disconnect your Internet connection, and not be able to re-establish automatically your connection 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 you want to have the Internet connecting last unless a new linking requested.
- Click the **Connect** button to connect immediately, Click the **Disconnect** button to disconnect immediately.

Click the **Advanced Settings** button to set up advanced option, the page that shown in figure 5-7 will appear:

**PPPoE Advanced Settings**

**MTU Size (in bytes):**  (The default is 1492, don't change it if not necessary.)

**Service Name:**

**AC Name:**

Use IP address specified by ISP

**ISP specified IP Address:**

**Detect Online Interval:**  Seconds (0 ~ 120 seconds, 0 means don't detect.)

Use These DNS Servers

**Primary DNS:**

**Secondary DNS:**  (optional)

Figure 5-7: PPPoE Advanced Settings

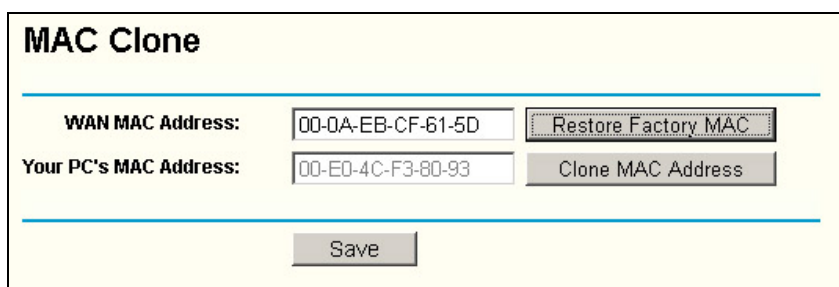
- **Packet MTU:** The default MTU size is usually fine. The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1492 bytes. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.
- **Service Name/AC Name:** The service name and AC (Access Concentrator) name, this should not be done unless you are sure it is necessary for your ISP.
- **ISP Specified IP Address:** If you know that your ISP does not automatically transmit 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 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 every interval seconds. If the value is 0, it means not detecting.
- **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 too.

Click the Save button to save your settings.

### 5.4.3 MAC Clone

You can configure the MAC address of the WAN port on this page, figure 5-8:





**MAC Clone**

**WAN MAC Address:** 00-0A-EB-CF-61-5D

**Your PC's MAC Address:** 00-E0-4C-F3-80-93

Figure 5-8: MAC Address Clone

Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable or DSL modem during installation. Usually, Don't change anything here.

**WAN MAC Address:** This field displayed the current MAC address of WAN port, which is used for 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 displayed the MAC address of the PC that is managing the Router. If the MAC address is desired, 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:**

- 1) Only the PCs on your LAN can use the **MAC Address Clone** feature.
- 2) If you click the **Save** button, the Router will prompt you to reboot.

## 5.5 Wireless



Figure 5-9: Wireless menu

There are three submenus under the Wireless menu (shown in figure 5-9): **Wireless Settings**, **MAC Filtering** and **Wireless Statistics**. Click any of them, and you can configure the corresponding function. The detailed explanations for every submenu are provided below.

### 5.5.1 Wireless Settings

The basic settings for Wireless network are set on this page, figure 5-10:

**Wireless Settings**

SSID:

Channel:

Mode:

Enable Wireless Router Radio

Enable SSID Broadcast

Authentication Type:

WEP Key Format:

Key Selected	WEP Key	Key Type
Key 1: <input type="radio"/>	<input type="text"/>	<input type="text" value="Disabled"/>
Key 2: <input type="radio"/>	<input type="text"/>	<input type="text" value="Disabled"/>
Key 3: <input type="radio"/>	<input type="text"/>	<input type="text" value="Disabled"/>
Key 4: <input type="radio"/>	<input type="text"/>	<input type="text" value="Disabled"/>

Figure 5-10: 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, but it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, *TP-LINK* is NOT the same as *TP-Link*.
- **Channel** - This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Mode** - Select the desired wireless mode. The options are:
  - 54Mbps (802.11g) - Both 802.11g and 802.11b wireless stations can connect to the Router.
  - 11Mbps (802.11b) - Only 802.11b wireless stations can connect to the Router.

**Note:** The default is "54Mbps (802.11g)", which allows both 802.11g and 802.11b wireless stations to connect to the Router.

- **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 the Router.
- **Enable SSID Broadcast** - If you select the **Enable SSID Broadcast** checkbox, the Wireless Router SSID will broadcast its name (SSID) on the air.
- **Authentication Type** - You can select one of the following authentication types:
  - **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station request.
  - **Shared Key** - Select 802.11 Shared Key authentication.
  - **Open System** - Select 802.11 Open System authentication.
  - **WPA-PSK** - Select WPA authentication type based on pre-shared passphrase.
  - **WPA** - Select WPA authentication type based on Radius Server.
- **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII Code Format stands for any combination of keyboard characters in specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in specified length.
- **WEP Key settings** - 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 this 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 illegal) 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 illegal) 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 illegal) or 16 ASCII characters.
- **Encryption** - When you select **WPA-PSK** or **WPA** for **Authentication Type** you can select either **Automatic**, or **TKIP** or **AES** for **Data Encryption**.

<b>Authentication Type:</b>	<input type="text" value="WPA-PSK"/>
<b>WEP Key Format:</b>	<input type="text" value="Automatic"/>
<b>WPA-PSK Passphrase:</b>	<input type="text"/>
	(The Passphrase is between 8 and 63 characters long)
<b>Group Key Update Period:</b>	<input type="text" value="30"/> (in second, minimum is 30, 0 means no update)

Figure 5-10a: WPA-PSK

- **WPA-PSK Passphrase** –You can enter a WPA passphrase between 8 and 63 characters long.
- **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.

<b>Authentication Type:</b>	<input type="text" value="WPA"/>
<b>WEP Key Format:</b>	<input type="text" value="Automatic"/>
<b>Radius Server IP:</b>	<input type="text"/>
<b>Radius Port:</b>	<input type="text" value="1812"/> (1-65535, 0 means the default port 1812)
<b>Radius password:</b>	<input type="text"/>
<b>Group Key Update Period:</b>	<input type="text" value="30"/> (in second, minimum is 30, 0 means no update)

Figure 5-10b: WPA

- **Radius Server IP** - You can enter the IP address of the Radius Server
- **Radius Port** - You can enter the port that radius service used.
- **Radius Password** - You can enter the password for the Radius Server.

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

**Note:** The Router will reboot automatically after you click **save** button.

## 5.5.2 MAC Filtering

The Wireless MAC address Filtering for Wireless network are set on this page, figure 5-11:

### Wireless MAC Filtering

---

Wireless MAC Address Filtering: Disabled

---

**Filtering Rules:**

**Allow** the stations not specified by any enabled entries in the list to access

**Deny** the stations not specified by any enabled entries in the list to access

ID	MAC Address	Status	Privilege	<input checked="" type="radio"/> Description	<input type="radio"/> Key	Modify
1	00-0A-EB-00-01-08	Enabled	allow	Station A		<a href="#">Modify</a> <a href="#">Delete</a>
2	00-0A-EB-00-01-1A	Enabled	64 bit	Station B		<a href="#">Modify</a> <a href="#">Delete</a>

---

Figure 5-11: 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.

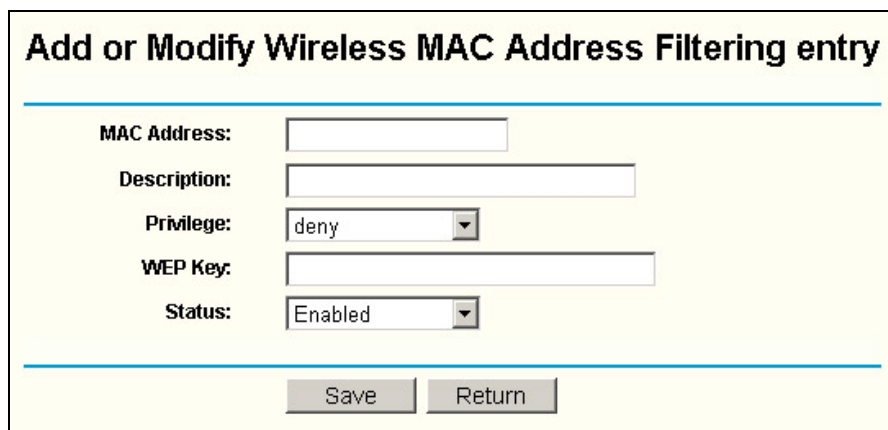
- **MAC Address** - The wireless station's MAC address that you want to access control.
- **Description** - A simple description of the wireless station.
- **Privilege** - **Allow** means allowing the station to access the Router. **Deny** means denying the station to access the Router. **64-bit**, or **128-bit**, or **152-bit** means assigning a unique WEP key to access the Router.
- **WEP Key** - Specify a unique WEP key (in Hexadecimal format) to access the Router.
- **Status** - The status of this entry, either **Enabled** or **Disabled**.

To disable the Wireless MAC Address Filters feature, keep the default setting, **Disable**.

To set up an entry, click **Enable**, and follow these instructions:

First, you must decide that the unspecified wireless stations can or cannot access the Router. 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, clicking the **Add New...** button. The "**Add or Modify Wireless MAC Address Filtering entry**" page will appear that shown in figure 5-12:



The screenshot shows a web form titled "Add or Modify Wireless MAC Address Filtering entry". The form contains the following fields and controls:

- MAC Address:** A text input field.
- Description:** A text input field.
- Privilege:** A dropdown menu with "deny" selected.
- WEP Key:** A text input field.
- Status:** A dropdown menu with "Enabled" selected.

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

Figure 5-12: Add or Modify Wireless 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 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. **Privilege** - Selects the privileges for this entry, one of **Allow** / **Deny** / **64-bit** / **128-bit** / **152-bit**.
4. **WEP Key** - If you select **64-bit**, **128-bit** or **152-bit** in the **Privilege** field, enter

any combination of hexadecimal digits (0-9, a-f, A-F) in specified length. For example: 2F34D20BE2.

5. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
6. Click the **Save** button to save this entry.

To add additional entries, repeat steps 1-6.

Note: When 64-bit, or 128-bit, or 152-bit is selected, WEP Key will be enabled.

To modify or delete a exist entry:

1. Click the **Edit** or **Delete** button in the **Modify** column in the MAC Address Filtering Table.
2. Enter the value as desired in the **Add or Modify Wireless MAC Address Filtering** entry page, and click the **Save** button.

You can click the **Enable All** button to make all the entries effective, click the **Disable All** button to make all the entries ineffective, click the **Delete All** button to delete all the 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 can access the Router, the wireless station B with MAC address 00-0A-EB-00-07-5F cannot access the Router, and the wireless station C with MAC address 00-0A-EB-00-07-8A can access the Router when its WEP key is 2F34D20BE2E54B326C5476586A, while all other wireless stations cannot access the Router, you should configure the **Wireless MAC Address Filtering** list 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 exist 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.
6. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07- 8A in the **MAC Address** field, enter wireless station C in the **Description** field, select **128-bit** in the **Privilege** pull-down list, enter 2F34D20BE2E54B326C5476586A in the **WEP Key** field and select **Enabled** in the **Status** pull-down list. Click the **Save** and the **Return** button.
7. 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 still cannot

access the Router, however, other wireless stations that are not in the list can access the Router.

**Note:** 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, all wireless stations cannot access the Router.

### 5.5.3 Wireless Statistics

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

**Wireless Statistics**

Number of connected Wireless Stations: 0 Refresh

ID	MAC Address	Current Status	Received Packets	Sent Packets
----	-------------	----------------	------------------	--------------

Previous Next

Figure 5-13: 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 / 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.

## 5.6 DHCP

- DHCP
  - DHCP settings
  - DHCP Clients List
  - Address Reservation

Figure 5-14: the DHCP menu

There are three submenus under the DHCP menu (shown in figure 5-14): **DHCP Settings**, **DHCP Clients List** and **Address Reservation**. Click any of them, and you can configure the corresponding function. The detailed explanations for every submenu are provided below.

### 5.6.1 DHCP Settings

The Router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for the all the PCs that are connected to the Router on the LAN. The DHCP Server can be configured on the page (shown in figure 5-15):

**DHCP Settings**

**DHCP Server:**  Enable  Disable

**Start IP Address:**

**End IP Address:**

**Address Lease Time:**  minutes (1~2880 minutes, the default value is 120)

**Default Gateway:**  (optional)

**Default Domain:**  (optional)

**Primary DNS:**  (optional)

**Secondary DNS:**  (optional)

**Save**

Figure 5-15: 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 a network user will be allowed connection to the Router with their current dynamic IP Address. Enter the amount of time, in minutes, that 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. You can 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.

### 5.6.2 DHCP Clients List

This page shows **Client Name**, **MAC Address**, **Assigned IP** and **Lease Time** for each DHCP Client attached to the Router (figure 5-16):

DHCP Clients List				
Index	Client Name	MAC Address	Assigned IP	Lease Time
1	TP-7XSIHL12MYS	00-0A-EB-00-00-08	192.168.1.100	01:59:52

Figure 5-16: 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 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.

### 5.6.3 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 (shown in figure 5-17).

ID	MAC Address	Reserved IP Address
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>

Figure 5-17: Address Reservation

- **MAC Address** – The MAC address of the PC that you want to reserve IP Address.
- **Assigned IP Address** –The IP Address of Router reserved.

**To Reserve IP addresses:**

1. 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.
2. Click the **Save** button when finished.

**To modify A Reserved IP address:**

1. Select the reserved address entry as you desired, modify it. If you want to delete the entry, make all of the entry fields blank.
2. Click the **Save** button.

**To delete all Reserved IP addresses:**

1. Click the **Clear All** button.
2. Click the **Save** button

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

**Note:** The function won't take effect until the Router reboots.

## 5.7 Forwarding

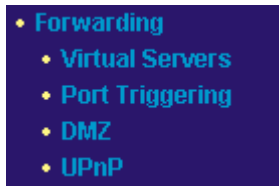


Figure 5-18: the Forwarding menu

There are four submenus under the Forwarding menu (shown in figure 5-18): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you can configure the corresponding function. The detailed explanations for every submenu are provided below.

### 5.7.1 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 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 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 that shown in figure 5-19:

### Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	<input type="text"/>	192.168.1. <input type="text"/>	ALL <input type="button" value="v"/>	<input type="checkbox"/>
2	<input type="text"/>	192.168.1. <input type="text"/>	ALL <input type="button" value="v"/>	<input type="checkbox"/>
3	<input type="text"/>	192.168.1. <input type="text"/>	ALL <input type="button" value="v"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.1. <input type="text"/>	ALL <input type="button" value="v"/>	<input type="checkbox"/>
5	<input type="text"/>	192.168.1. <input type="text"/>	ALL <input type="button" value="v"/>	<input type="checkbox"/>
6	<input type="text"/>	192.168.1. <input type="text"/>	ALL <input type="button" value="v"/>	<input type="checkbox"/>
7	<input type="text"/>	192.168.1. <input type="text"/>	ALL <input type="button" value="v"/>	<input type="checkbox"/>
8	<input type="text"/>	192.168.1. <input type="text"/>	ALL <input type="button" value="v"/>	<input type="checkbox"/>

Common Service Port:   ID

Figure 5-19: Virtual Servers

- **Service Port** - The numbers of External Ports. You can type the service port or service port range numbers (the format is XXX – YYY, XXX is Start port, YYY is End port).

- **IP Address** - The IP Address of the PC running the service application
- **Protocol** - The protocol used for this application, either **TCP** or **UDP**, or **All** (include all protocol that can be accessed by the Router).
- **Enable** - The Enable checkbox to enable the virtual server entry.
- **Common Service Port** – Some common services already exist in the pull-down list.

**To setup a virtual server entry:**

1. Select the service you want to use from the Common Service Port list, and select the ID you want to use, and click **Copy to** button. 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.
2. Type the IP Address of the computer in the **Server IP Address** box.
3. Select the protocol used for this application, either **TCP** or **UDP**, or **All**.
4. Select the **Enable** checkbox to enable the virtual server.
5. Click the **Save** button.

**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 a virtual server entry:**

1. Select the entry you want to modify.
2. Modify the information from the **Service Port**, the **IP Address** boxes, and the **Protocol** pull-down list.
3. Click the **Save** button.

**To delete a service entry:**

1. Clear the entry's all information except the **Protocol** pull-down list.
2. Click the **Save** button.

**To delete all service entries:**

3. Click the **Clear All** button.
4. Click the **Save** button

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.

## 5.7.2 Port Triggering

Some applications require multiple connections, like Internet games, video conferencing, Internet telephoning 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 shown in figure 5-20:

ID	Trigger Port	Trigger Protocol	Incoming Ports Range	Incoming Protocol	Enable
1	<input type="text"/>	ALL	<input type="text"/>	ALL	<input type="checkbox"/>
2	<input type="text"/>	ALL	<input type="text"/>	ALL	<input type="checkbox"/>
3	<input type="text"/>	ALL	<input type="text"/>	ALL	<input type="checkbox"/>
4	<input type="text"/>	ALL	<input type="text"/>	ALL	<input type="checkbox"/>
5	<input type="text"/>	ALL	<input type="text"/>	ALL	<input type="checkbox"/>
6	<input type="text"/>	ALL	<input type="text"/>	ALL	<input type="checkbox"/>
7	<input type="text"/>	ALL	<input type="text"/>	ALL	<input type="checkbox"/>
8	<input type="text"/>	ALL	<input type="text"/>	ALL	<input type="checkbox"/>

Common Applications:   ID

Figure 5-20: 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. The Internet host receives the PCs request, and responds using a different port number.
  4. This Router matches the response to the previous request, and forwards the response to the PC.
- **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** or **UDP**, or **All** (include all protocol that can be access the Router).
  - **Incoming Ports Range** - 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 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 (include all protocol that can be access the Router).
- **Enable** - The Enable checkbox to enable port forwarding for the application.
  - **Common Applications** – some popular applications already existing in the pull-down list.

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

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

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

#### **Modifying an existing rule:**

1. Edit the entry as desired.
2. Click the **Save** button.

#### **Deleting an existing rule:**

1. Clear all the content in **Trigger Port** field, **Open Port field** and **Enable** checkbox.
2. Click the **Save** button.

#### **To delete all rules:**

1. Click the **Clear All** button.
2. Click the **Save** button

#### **Note:**

1. When the trigger connection is released, the according opening ports will be closed.
2. Each rule allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.
3. Incoming Port Range cannot overlap each other.

### **5.7.3 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 5-21:

Figure 5-21: 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
3. Click the **Save** button.

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

#### 5.7.4 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 that shown in figure 5-22:

ID	App Info	Ext. Port	Protocol	Int. Port	IP Address	Status

Figure 5-22: UPnP Settings

- **Enable UPnP:** UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button. As allowing this may present a risk to security, this feature is disabled by default.
- **Current UPnP Settings Table:** this table displays the current UPnP information.
  - **App Info.** – The descriptions of applications, the request information when the

UPnP device currently accessing the Router.

- **Ext. Port** – external port, the device has opened for Router.
- **Protocol** – what type of protocol is opened.
- **Int. Port** – Internal port, the device has 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 Table.

## 5.8 Security



Figure 5-23: the Security menu

There are six submenus under the Security menu (shown in figure 5-23): **Firewall**, **IP Address Filtering**, **Domain Filtering**, **MAC 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.

### 5.8.1 Firewall

Using the Firewall page (shown in figure 5-24), 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.



**Firewall**

Enable firewall (the general firewall switch)

Enable IP Address Filtering

Default IP Address Filtering Rules:

All packets that do not comply with configured rules are **permitted** to pass through this Router

All packets that do not comply with configured rules are **prevented** to pass through this Router

Enable Domain Filtering

Enable MAC Address Filtering

Default MAC Address Filtering Rules:

**Permit only** these PCs with effective rules to access the Internet

**Prevent** these PCs with effective rules from accessing the Internet

Save

Figure 5-24: 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 Permit or Prevent accessing 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 Permit or Prevent accessing the Router.

### 5.8.2 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 are set on this page, figure 5-25:

### IP Address Filtering

---

**Firewall Settings (You can change it on Firewall page)**

Enable Firewall: Enabled

Enable IP Address Filtering: Enabled

Default Filtering Rules: All packets that do not comply with configured rules are permitted to pass through this Router

ID	LAN IP	LAN Port	WAN IP	WAN Port	Protocol	Pass	Status	Modify
1	192.168.1.102	6535	222.88.88.13	6550	ALL	Permitted	Effective	<a href="#">Modify</a> <a href="#">Delete</a>

ID  to ID

---

Figure 5-25: 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 5-26:

### Add or Modify an IP Address Filtering entry

---

LAN IP Address:  -

LAN Port:  -

WAN IP Address:  -

WAN Port:  -

Protocol:

Pass-through:

Status:

---

Figure 5-26: Add or Modify an IP Address Filtering entry

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

1. **LAN IP Address** – type 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. Leave the field blank, which means all LAN IP Addresses have been put into the field.
2. **LAN Port** – type a LAN Port or a range of LAN Ports in the field. Keep the field open, which means all LAN Ports have been put into the field. For example, 1030 – 2000.
3. **WAN IP Address** - type a WAN IP Address or a range of WAN IP Addresses in the field, in dotted-decimal notation format. Keep the field open, which means all WAN IP Addresses have been put into the field. For example, 61.145.238.6 – 61.145.238.47.

4. **WAN Port** - type a WAN Port or a range of WAN Port in the field. Leave the field blank, which means all WAN Port have been put into the field. For example, 25 – 110.
5. **Protocol** - select which protocol is to be used, either **TCP** or **UDP**, or **All** (Both TCP and UDP).
6. **Pass** - select either **Prevent** or **Permit** through the Router.
7. **Status** - Select **Effective** or **Ineffective** for this entry on the **Status** pull-down list.
8. Click the **Save** button to save this entry.

To add additional entries, repeat steps 1-8.

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

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.

Click the **All Entries Effective** button to make all entries effective

Click the **All Entries Ineffective** button to make all entries ineffective.

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

You can change the entry's order as desired. Fore entries are before hind entries. Type the ID number in the first box you want to move and another ID number in second box you want to move to, 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 PCs have no limit. You should specify the following IP Address filtering table:

ID	LAN IP	LAN Port	WAN IP	WAN Port	Protocol	Pass through	Status	Modify
1	192.168.1.7	-	-	25	All	No	Effective	<a href="#">Modify</a> <a href="#">Delete</a>
2	192.168.1.7	-	-	110	All	No	Effective	<a href="#">Modify</a> <a href="#">Delete</a>
3	192.168.1.8	-	202.96.134.12	-	All	No	Effective	<a href="#">Modify</a> <a href="#">Delete</a>

### 5.8.3 Domain Filtering

The Domain Filtering page (shown in figure 5-27) allows you to control access to certain websites on the Internet by specifying their domains or key words.

**Domain Filtering**

---

**Firewall Settings (You can change it on Firewall page)**

Enable Firewall: **Enabled**

Enable Domain Filtering: **Disabled**

ID	Domain Name	Status	Modify
1	www.aabbcc.com	Effective	<a href="#">modify</a> <a href="#">delete</a>
2	.net	Effective	<a href="#">modify</a> <a href="#">delete</a>

---

Figure 5-27: 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, clicking **Add New...** button. The page " **Add or Modify a Domain Filtering entry** " will appear that shown in figure 5-28:

**Add or Modify a Domain Filtering entry**

---

Domain Name:

Status:

---

Figure 5-28: Add or Modify a Domain Filtering entry

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

1. **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](http://www.xxyy.com.cn), .net.
2. **Status** - Select **Effective** or **Ineffective** for this entry on the **Status** pull-down list.
3. Click the **Save** button to save this entry.

To add additional entries, repeat steps 1-3.

When finished, click the **Return** button to return to the **Domain filtering** page.

To Modify or delete an existing entry:

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

Click the **All Entries Effective** button to make all entries effective.

Click the **All Entries Ineffective** button to make all entries ineffective.

Click the **Delete All Entries** 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 PCs on your LAN to access websites [www.xxyy.com.cn](http://www.xxyy.com.cn), [www.aabbcc.com](http://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 table:

ID	Domain Name	Status	Modify
1	<a href="http://www.xxyy.com.cn">www.xxyy.com.cn</a>	Effective	<a href="#">Modify</a> <a href="#">Delete</a>
2	<a href="http://www.aabbcc.com">www.aabbcc.com</a>	Effective	<a href="#">Modify</a> <a href="#">Delete</a>
3	.net	Effective	<a href="#">Modify</a> <a href="#">Delete</a>

#### 5.8.4 MAC Filtering

Like IP Address Filtering page, the MAC Address Filtering page (shown in figure 2-29) allows you to control to access Internet by users on your local network based on their MAC Address.

### MAC Address Filtering

---

**Firewall Settings (You can change it on Firewall page)**

Enable Firewall: Enabled

Enable MAC Address Filtering: Disabled

Default Filtering Rules: Permit only these PCs with effective rules to access the Internet.

ID	MAC Address	Description	Status	Modify
1	00-0A-E0-07-AB-C2	Alice's PC	Effective	<a href="#">modify</a> <a href="#">delete</a>

Add New...
All Entries Effective
All Entries Ineffective
Delete All Entries

---

Previous
Next

Figure 2-29: MAC address Filtering

Before setting up MAC Filtering entries, you must insure 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 that shown in figure 5-30:

Figure 5-30: 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 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 **Effective** or **Ineffective** 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. Find the desired entry in the table.
2. Click **Modify** or **Delete** as desired on the **Edit** column.

Click the **All Entries Effective** button to make all entries effective.

Click the **All Entries Ineffective** button to make all entries ineffective.

Click the **Delete All Entries** 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.

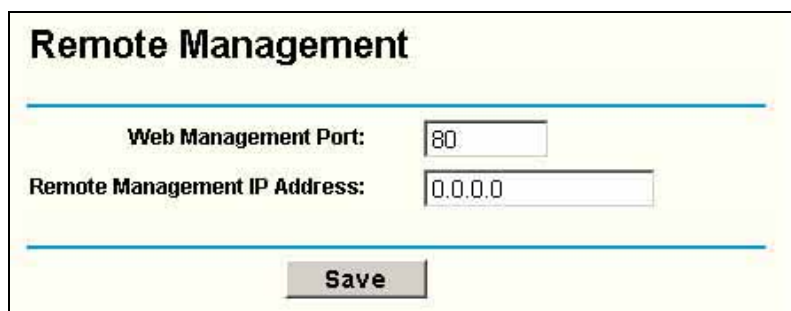
Fox example: If you want to block the PCs with MAC Addresses 00-E0-4C-00-07-BE and 00-E0-4C-00-07-5F to access the Internet, first, enable the Firewall and MAC Address Filtering on the Firewall page, then, you should specify the Default MAC Address Filtering Rule " **Prevent these PCs with effective rules from accessing the Internet** " on the Firewall page and the following MAC Address filtering table on this page:

ID	MAC Address	Description	Status	Modify
1	00-E0-4C-00-07-BE	John's computer	Effective	<a href="#">Modify</a> <a href="#">Delete</a>
2	00-E0-4C-00-07-5F	Alice's computer	Effective	<a href="#">Modify</a> <a href="#">Delete</a>

### 5.8.5 Remote Management

You can configure Remote Management function on this page shown in figure 5-31. This

feature allows you to manage your Router from a remote location, via the Internet.



**Remote Management**

Web Management Port:

Remote Management IP Address:

Save

Figure 5-31: 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.

### 5.8.6 Advanced Security

Using Advanced Settings page (shown in figure 5-32), you can protect the Router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood from LAN.

### Advanced Security

---

**Packets Statistic interval (5 ~ 60):**  Seconds

**DoS protection:**  Disable  Enable

Enable ICMP-FLOOD Attack Filtering

**ICMP-FLOOD Packets threshold: (5 ~ 3600):**  Packets/s

Enable UDP-FLOOD Filtering

**UDP-FLOOD Packets threshold: (5 ~ 3600):**  Packets/s

Enable TCP-SYN-FLOOD Attack Filtering

**TCP-SYN-FLOOD Packets threshold: (5 ~ 3600):**  Packets/s

Ignore Ping Packet From WAN Port

Forbid Ping Packet From LAN Port

---

Figure 5-32: Advanced Security settings

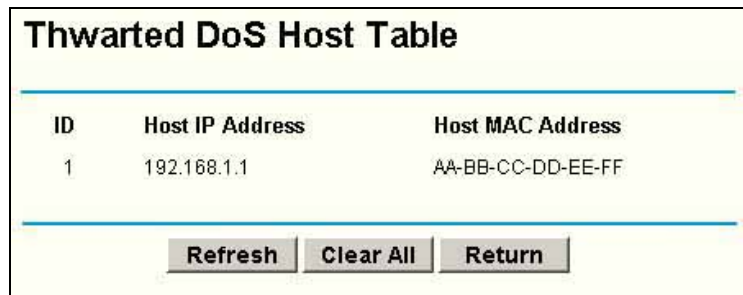
- **Packets Statistic interval (5 ~ 60)** - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The **Packets Statistic interval** value indicates the time section of the packets statistic. The result of the statistic used for analysis by **SYN Flood**, **UDP Flood** 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 thwarting 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 **UPD-FLOOD** Packets numbers is beyond the set value, the Router will start up the thwarting 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 thwarting 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 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 **Thwarted DoS Host Table** button to display the DoS host table by thwarting. The page will appear that shown in figure 5-33:



ID	Host IP Address	Host MAC Address
1	192.168.1.1	AA-BB-CC-DD-EE-FF

Refresh Clear All Return

Figure 5-33: Thwarted DoS Host Table

This page shows **Host IP Address** and **Host MAC Address** for each host thwarted by the Router.

- **Host IP Address-** The IP address that thwarted by DoS displays here.
- **Host MAC Address -** The MAC address that thwarted by DoS displays here.

To update this page and to show the current thwarted host, click on the **Refresh** button. Click the **Clear All** button to clear all displayed entry. After the table is empty the thwarted host will regain the capability to access Internet.

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

## 5.9 Static Routing

A static route is a pre-determined pathway 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 (shown in figure 5-34).

Static Routing				
ID	Destination IP Address	Subnet Mask	Gateway	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Figure 5-34: Static Routing

**To add static route entries:**

1. 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.
2. Click **Enable** checkbox.
3. Repeat steps 1-2 until you are finished.
4. If you are finished. Click the **Save** button to save it.

**To modify an existing entry:**

1. Modify the entry's **Destination IP Address**, **Subnet Mask** and **Gateway**.
2. Click the **Save** button.

**To delete an existing entry:**

1. Select the entry as you desire and select the fields, highlighting them black.
2. Click the **Save** button.

**To delete all the entries:**

1. Click the **Clear All** button.
2. Click the **Save** button.

**Note:** You can set up to 8 entries.

## 5.10 DDNS

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.oray.net](http://www.oray.net) or [www.comexe.cn](http://www.comexe.cn). The Dynamic DNS client service provider will give you a password or key.

To set up for DDNS, follow these instructions:

### 5.10.1 Oray.net DDNS

If your selected dynamic DNS **Service Provider** is [www.oray.net](http://www.oray.net). The page will appear that shown in figure 5-35:

**DDNS**

**Service Provider:**

**User Name:**

**Password:**

**Connection Status:** Connected successfully.

**Domain Name 1:** hellopig.vicp.net

**2:** hellodog.vicp.net

**3:** hellocat.vicp.net

**4:** hellobinge.vicp.net

**5:** hellocolin.vicp.net

Figure 5-35: 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.

### 5.10.2 Comexe.cn DDNS

If your selected dynamic DNS **Service Provider** is [www.comexe.cn](http://www.comexe.cn). The page will appear that shown in figure 5-36:

**DDNS**

**Service Provider:**

**Domain Name 1:**

**Domain Name 2:**

**Domain Name 3:**

**Domain Name 4:**

**Domain Name 5:**

**User Name:**

**Password:**

**Connection Status:** Connecting...

Figure 5-36: 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 the DDNS service.

**Connection Status:** The status of the DDNS service connection is displayed here.

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

## 5.11 System Tools

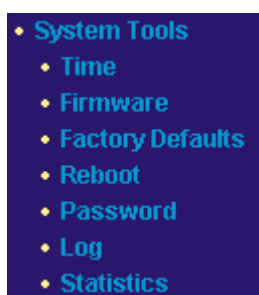


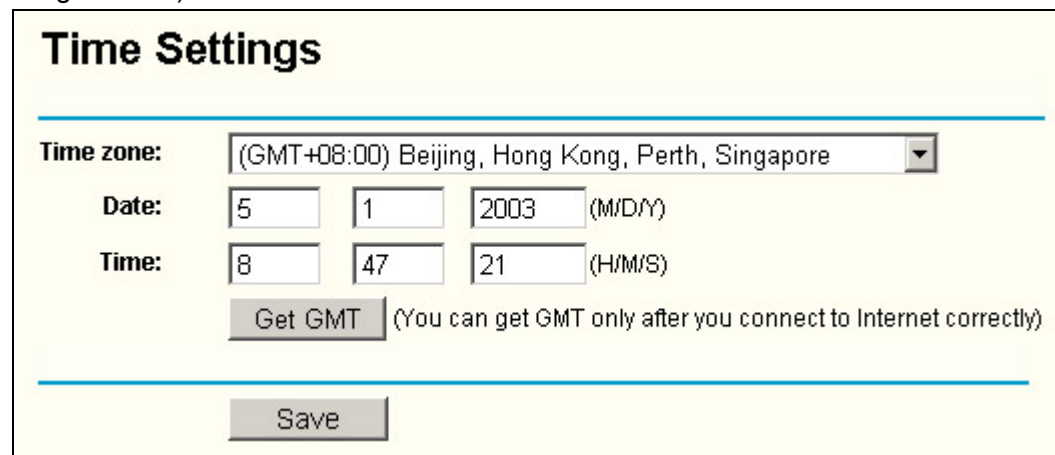
Figure 5-37: the System Tools menu

There are seven submenus under the System Tools menu (shown in figure 5-37): **Time**, **Firmware**, **Factory Defaults**, **Reboot**, **Password**, **Log** and **Statistics**. Click any of them, and you can configure the corresponding function. The detailed explanations for

every submenu are provided below.

### 5.11.1 Time

You can set time manually or get GMT from Internet for the Router on this page (shown in figure 5-38):



**Time Settings**

**Time zone:** (GMT+08:00) Beijing, Hong Kong, Perth, Singapore

**Date:** 5 1 2003 (M/D/Y)

**Time:** 8 47 21 (H/M/S)

Get GMT (You can get GMT only after you connect to Internet correctly)

Save

Figure 5-38: 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.

Time setting follows these steps below:

1. Select your local time zone.
2. Enter date and time in the right blanks
3. Click **Save**.

Click the **Get GMT** button to get GMT time from Internet if you have connected to Internet.

**Note:**

1. This setting will be used for some time-based functions such as firewall. You must specify your time zone once login to the Router successfully, or not the time limited on these functions will not take effect.
2. The time will lose if the Router is power off.
3. The Router will obtain GMT automatically from Internet if it has already connected to Internet.

### 5.11.2 Firmware

The page (shown in figure 5-39) allows you to upgrade the latest version firmware for the Router.

<b>File Name:</b>	<input type="text" value="wr541g.bin"/>
<b>TFTP Server IP Address:</b>	<input type="text" value="192.168.1.199"/>
<b>Firmware Version:</b>	2.8.0 Build 050118 Rel.57338na
<b>Hardware Version:</b>	TL-WR541Gv1 085B00C2

Figure 5-39: Firmware Upgrade

New firmware versions are posted at [www.tp-link.com](http://www.tp-link.com) and can be downloaded free. If the Router is not experiencing difficulties, there is no need to download a more recent firmware version, unless that version has a new feature that you want to use.

**Note: When you upgrade the Router's firmware, you may lose its configuration settings, so make sure you write down the Router settings before you upgrade its firmware.**

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

1. Download a more recent firmware upgrade file from the TP-LINK website ([www.tp-link.com](http://www.tp-link.com)).
  2. Run a TFTP Server on a PC on your LAN, and take the file in the TFTP server's path.
  3. Type the downloaded file name into the **File Name** box.
  4. Type the IP Address of the PC that runs the TFTP server in the **TFTP Server's IP Address** field.
  5. 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:**

1. **Do not power off the Router or press the Reset button while the firmware is being upgraded.**
2. The Router will reboot after the Upgrading has been finished.

### 5.11.3 Factory Defaults

This page (shown in figure 5-40) allows you to restore the factory default settings for the Router.

**Factory Defaults**

Click following button to reset all configuration settings to their default values

Figure 5-40: Restore Factory Default

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

- The default **User Name**: admin
- The default **Password**: admin
- The default **IP Address**: 192.168.1.1
- The default **Subnet Mask**: 255.255.255.0

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

#### 5.11.4 Reboot

This page (shown in figure 5-41) allows you to reboot the Router.

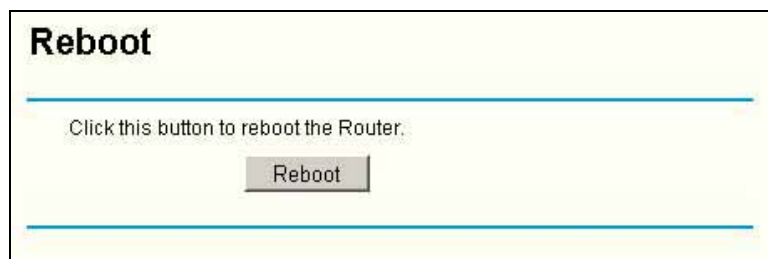


Figure 5-41: Reboot the Router

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).

#### 5.11.5 Password

This page (shown in figure 5-42) allows you to change the factory default user name and password of the Router.

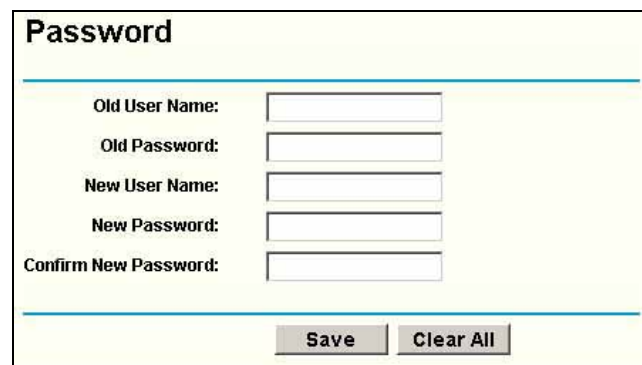


Figure 5-42: Password

It is strongly recommended 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 Setup Wizard will be prompted for the Router's user name and password.

**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.

### 5.11.6 Logs

This page (shown in figure 5-43) allows you to query the Logs of the Router.

## Log

---

Index	Log
1	0000:System: Router initialization succeeded.
2	0119:DHCP μÈ'ýÓ;ǎ~Ê±.
3	0240:DHCP μÈ'ýÓ;ǎ~Ê±.
4	0363:DHCP μÈ'ýÓ;ǎ~Ê±.

Time = 2003-05-01 8:07:03 423s

Mode = DHCP : L = 192.168.1.1 : W = 0.0.0.0

H-Ver = WR642Gv1 00000000 : S-Ver = 1.0.6 Build 050322 Rel.62009n

Free=6098, Busy=5, Bind=0, Inv=0/0, Bc=0/0, Dns=0, cl=240, fc=0/0, sq=0/0

---

Figure 5-43: 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 Log** button to clear all the logs.

### 5.11.7 Statistics

The Statistics page (shown in figure 5-44) displays the network traffic of each PC on LAN, including total traffic and traffic of the last **Packets Statistic interval** seconds.



### Statistics

---

**Current Statistics Status:** Disabled Enable

**Packets Statistics Interval(5-60):**  Seconds Save

Auto-refresh Refresh

**Sorted Rules:** Sorted by Current Bytes

IP Address	Total		Current				
	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx	TCP SYN Tx
192.168.1.234	863	143559	19	3129	0/0	0/0	2/16

Figure 5-44: 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 value indicates the time section of the packets statistic.
- **Sorted Rules**– here displays sort as desired.

**Statistics Table:**

<b>IP Address</b>	The IP Address displayed with statistics	
<b>Total</b>	<b>Packets</b>	The total amount of packets received and transmitted by this Router.
	<b>Bytes</b>	The total amount of bytes received and transmitted by this Router.
<b>Current</b>	<b>Packets</b>	The total amount of packets received and transmitted in the last <b>Packets Statistic interval</b> seconds.
	<b>Bytes</b>	The total amount of bytes received and transmitted in the last <b>Packets Statistic interval</b> seconds.
	<b>ICMP Tx</b>	The total amount of the ICMP packets transmitted to WAN in the last <b>Packets Statistic interval</b> seconds.
	<b>UDP Tx</b>	The total amount of the UDP packets transmitted to WAN in the last <b>Packets Statistic interval</b> seconds.
	<b>TCP SYN Tx</b>	The total amount of the TCP SYN packets transmitted to WAN in the last <b>Packets Statistic interval</b> 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 to 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) Log into 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".
- 4) If your ADSL lease is in "pay-according-time" mode, select "Connect on Demand" or "Manually connecting" for Internet connection mode. Type an appropriate number for "Max Idle Time" to avoid wasting paid time. Otherwise, you can select "Auto-connecting" for Internet connection mode.

### **2. How to configure the Router to access Internet by LAN users?**

- 1) Log into the Router, click the "Network" menu on the left of your browser, and click "WAN" submenu. On the WAN page, select "DHCP" 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 or DSL modem during installation. If your ISP requires MAC register, Log in 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.

### **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 responsor, you need configure Virtual Server or DMZ Host.
- 3) How to configure Virtual Server: Log into the Router, click the "Forwarding" menu on the left of your browser, and click " Virtual Servers" submenu. On the "Virtual Server" page, enter "1720" into the blank below the "Service Port", and your IP address below the IP Address, assuming 192.168.1.169 for an example, remember to "Enable" and "Save".

ID	Service Port	IP Address	Protocol	Enable
1	1720	192.168.1.169	ALL	<input checked="" type="checkbox"/>
2		192.168.1.	ALL	<input type="checkbox"/>
3		192.168.1.	ALL	<input type="checkbox"/>
4		192.168.1.	ALL	<input type="checkbox"/>

Common Service Port: DNS(53) Copy to ID 1

Previous Next Clear All Save

Figure A-1: Virtual Server

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

- How to enable DMZ Host: Log into 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, assuming 192.168.1.169 as an example, remember to click "Save" button.

DMZ

Enable  Disable

DMZ Host IP Address: 192.168.1.169

Save

Figure A-2: DMZ

#### 4. I want to construct a WEB Sever 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: Log into 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 88, into the "Web Management Port" field. Click "Save" and reboot the Router.

Remote Management

Web Management Port: 88

Remote Management IP Address: 0.0.0.0

Save

Figure A-3: Remote Management

**Note:** Type <http://192.168.1.1:88> into browser to log into the Router if the above configuration takes effect.

- 3) Log into the Router, click the "Forwarding" menu on the left of your browser, and click " 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 "Enable" and "Save".

### Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	<input type="text" value="80"/>	192.168.1.188	ALL	<input checked="" type="checkbox"/>
2	<input type="text"/>	192.168.1.	ALL	<input type="checkbox"/>
3	<input type="text"/>	192.168.1.	ALL	<input type="checkbox"/>
4	<input type="text"/>	192.168.1.	ALL	<input type="checkbox"/>

Common Service Port:   ID

Figure A-4: Virtual Server

#### 5. *The wireless stations cannot connect to the Router.*

- 1) Make sure the "Wireless Router Radio" is enabled.
- 2) Make sure that the wireless stations' SSID accord with the Router's SSID.
- 3) Make sure the wireless stations have right KEY for encryption when the Router is encrypted.
- 4) If wireless connection is ready, but you can't access the Router, check the IP Address of your wireless stations.

## Appendix B: Configuring the PCs

In this section, we'll introduce how to install and configure the TCP/IP correctly in Windows 95/98. First make sure your Ethernet Adapter is working, refer to the adapter's manual if needed.

### 1. Install TCP/IP component

- 1) On the Windows taskbar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
- 2) Double-click the **Network** icon, click on the **Configuration** tab in the appearing **Network** window.
- 3) Click on the **Add** button. Select **Protocol**, and then click **Add**.

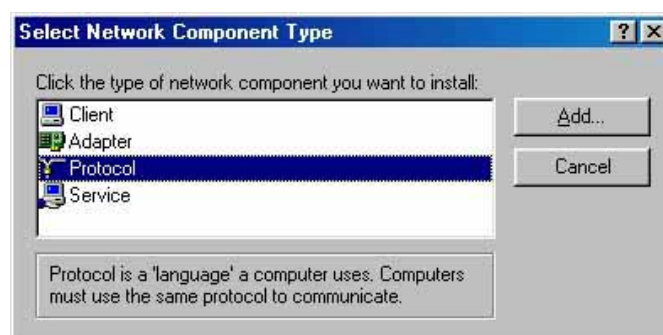


Figure B-1: Add Network Protocol

- 4) Under **Manufacturers** on **Select Network Protocol** page, highlight **Microsoft**. Under **Network Protocols**, highlight **TCP/IP**. Click **OK**. **TCP/IP** protocol will take effect after reboot.

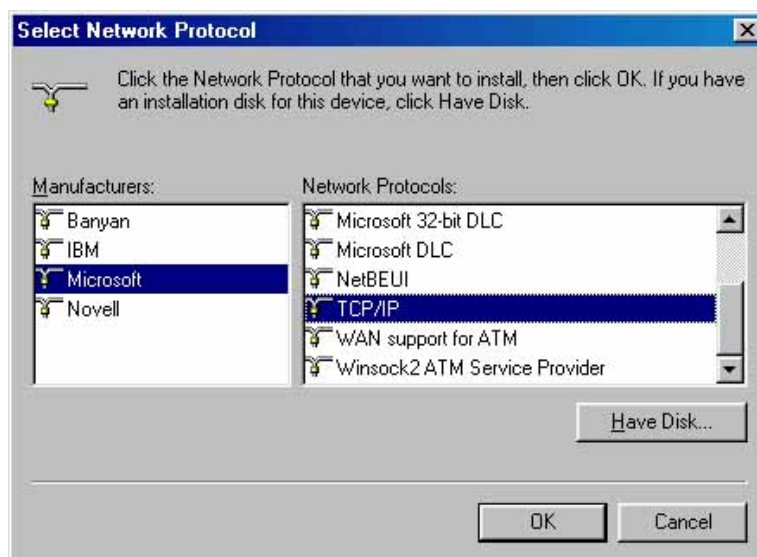


Figure B-2: Select Network Protocol

### 2. Configure TCP/IP for your computer

- 1) On the Windows taskbar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
- 2) Double-click the **Network** icon, highlight the bound **TCP/IP** tab in the appearing **Network** window. An example shown in the following figure:

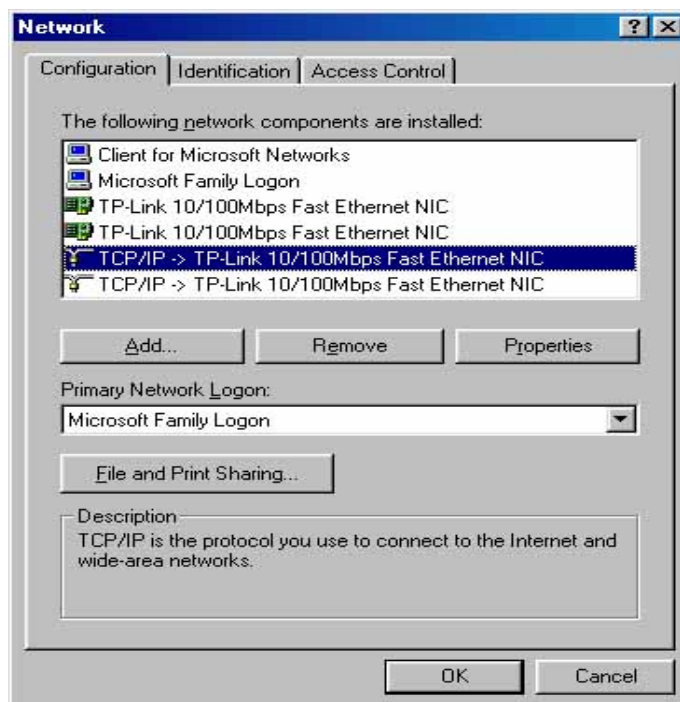


Figure B-3: Configuration tab

- 3) Click on **Properties**. The following **TCP/IP Properties** window will display and the **IP Address** tab is open on this window by default.
- 4) Now you have two ways to configure the **TCP/IP** protocol below:
  - Assigned by DHCP Sever
    - a. Select **Obtain an IP address automatically**, as shown in the figure below:

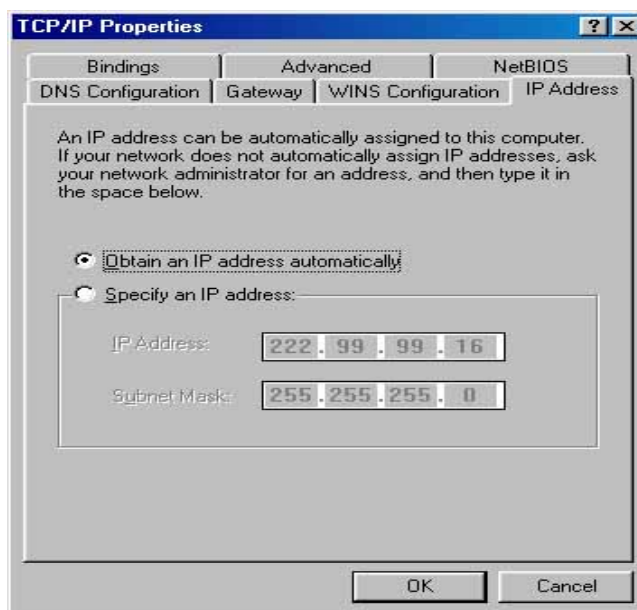


Figure B-4: IP Address tab

- b. Do not type anything into the **New gateway** field on the **Gateway** tab.



Figure B-5: Gateway tab

- c. Choose Disable DNS on the DNS configuration tab, as shown in the following figure:

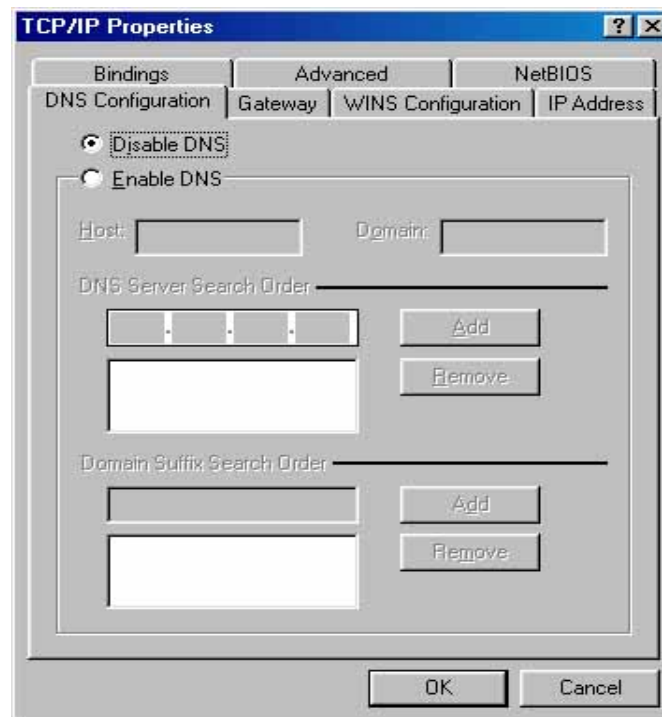


Figure B-6: DNS Configuration tab

- Setting IP address manually

- a. Select Specify an IP address on IP Address tab, as shown in the following figure. If the Router's LAN IP address is 192.168.1.1 type IP address is 192.168.1.x (x is from 2 to 254), Subnet mask is 255.255.255.0.

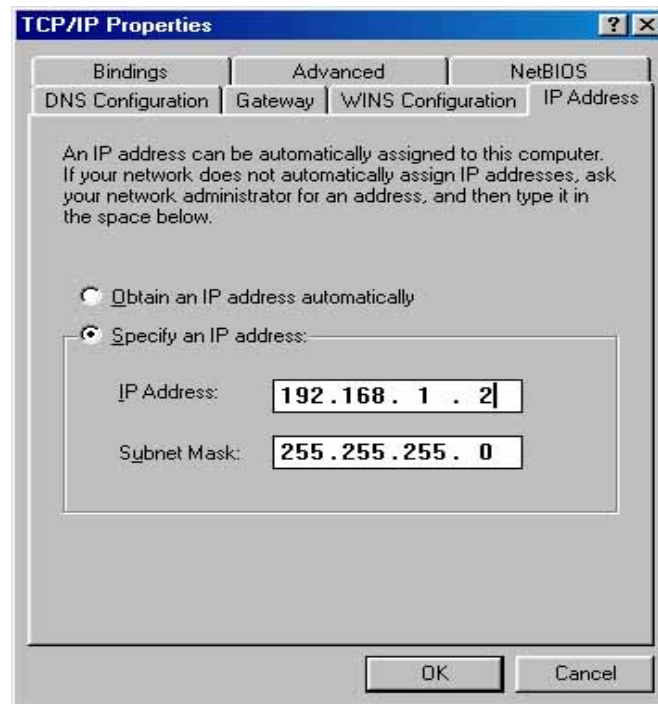


Figure B-7: IP Address tab

- b. Type the Router's LAN IP address (the default IP is 192.168.1.1) into the **New gateway** field on the **Gateway** tab, and click on the **Add** button, as shown in the figure:

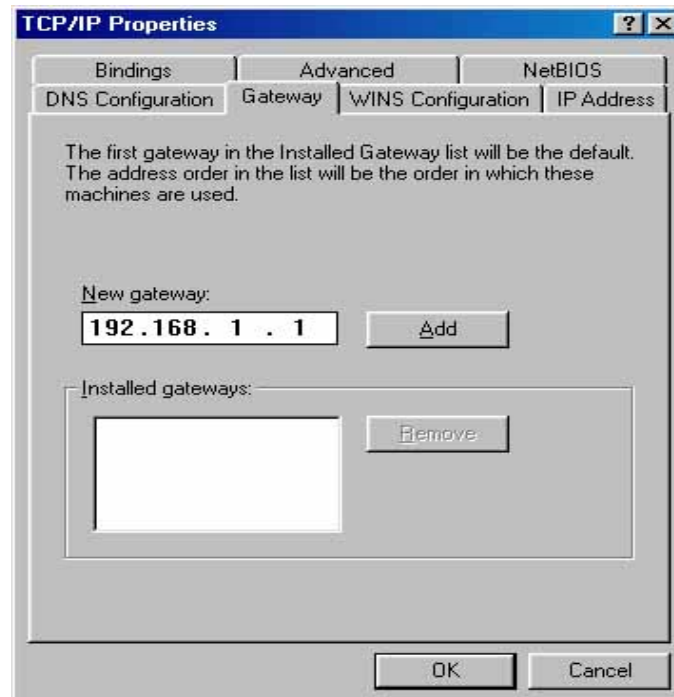


Figure B-8: Gateway tab



- c. On the **DNS Configuration** tab, click **Enable DNS** radio, and type your computer name in to the **Host** field and a Domain (such as szonline.com) into the **Domain** field. In the **DNS Server Search Order** field you can type the NDS server IP addresses, which have been provided by your ISP, and click **Add** button. Shown below:

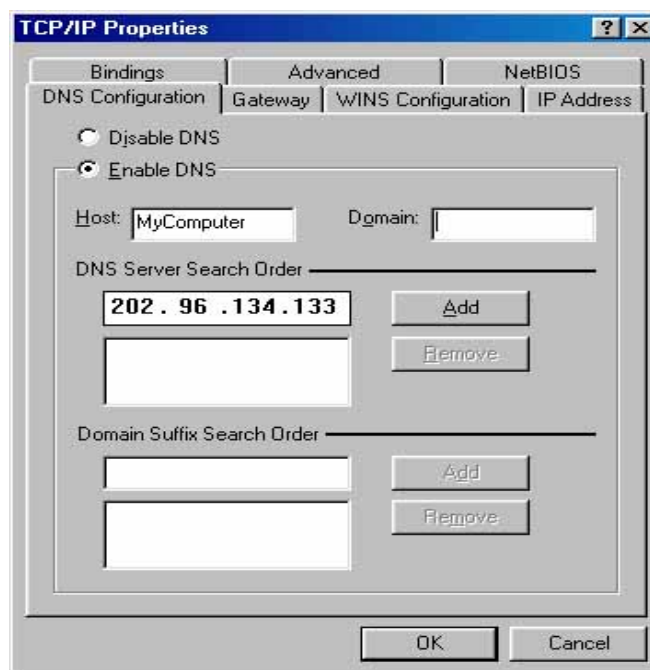


Figure B-9: DNS Configuration tab

**Now**, all the configurations are finished, it will take effect after reboot.

## Appendix C: Specifications

<b>General</b>	
Standards	IEEE 802.3, 802.3u, 802.11b and 802.11g
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Channel	13
Ports	One 10/100M Auto-Negotiation WAN RJ45 port, Four 10/100M Auto-Negotiation LAN RJ45 ports supporting Auto MDI/MDIX
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m) 100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
Radio Data Rate	54/48/36/24/18/12/9/6/11/5.5/3/2/1/0.5/0.25Mbps
Power Supply	9V~ 0.8A
LEDs	Power, System, WLAN, Link/Act, Speed

<b>Environmental and Physical</b>	
Operating Temp.	0°C~40°C (32°F~104°F)
Operating Humidity	10% - 95% RH, Non-condensing
Dimensions (W×D×H)	186×146×44 mm (7.3×5.7×1.7 in.) (Excluding antenna)

## Appendix D: Glossary

**2x to 3x eXtended Range™ WLAN Transmission Technology** - The WLAN device with 2x to 3x eXtended Range™ WLAN transmission technology make its sensitivity up to 105 dB, which gives users the ability to have robust, longer-range wireless connections. With this range-enhancing technology, a 2x to 3x eXtended Range™ based client and access point can maintain a connection at as much as three times the transmission distance of traditional 802.11b and 802.11g products, for a coverage area that is up to nine times greater. A traditional 802.11b and 802.11g product transmission distance is about 300m, A TP-LINK 2x to 3x eXtended Range™ based client and access point can maintain a connection transmission distance may be up to 830m.

**802.11b** - The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.

**802.11g** - specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.

**DDNS (Dynamic Domain Name System)** - The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.

**DHCP (Dynamic Host Configuration Protocol)** - A protocol that automatically configure the TCP/IP parameters for the all the PCs that are connected to a DHCP server.

**DMZ (Demilitarized Zone)** - A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.

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

**Domain Name** - A descriptive name for an address or group of addresses on the Internet.

**DoS (Denial of Service)** - A hacker attack designed to prevent your computer or network from operating or communicating.

**DSL (Digital Subscriber Line)** - A technology that allows data to be sent or received over existing traditional phone lines.

**ISP (Internet Service Provider)** - A company that provides access to the Internet

**MTU (Maximum Transmission Unit)** - The size in bytes of the largest packet that can be transmitted

**NAT (Network Address Translation)** - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

**PPPoE (Point to Point Protocol over Ethernet)** - PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

**SSID - A Service Set Identification** is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name. See *also* Wireless Network Name and ESSID.

**WEP (Wired Equivalent Privacy)** - A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.

**Wi-Fi** - A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see <http://www.wi-fi.net>), an industry standards group promoting interoperability among 802.11b devices.

**WLAN (Wireless Local Area Network)** - A group of computers and associated devices that communicate with each other wirelessly.

## Appendix E: Contact Information

For help with the installation or operation of the TP-LINK TL-WR542G 54Mbps Wireless Router, please contact us.

**Tel:** +86-755-2661-2350, 2652-5723

**Fax:** +86-755-2663-6921

**E-mail:** [export@tp-link.com.cn](mailto:export@tp-link.com.cn)

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