

TP-LINK®

User Guide

TL-WR740N

150Mbps Wireless N Router



COPYRIGHT & TRADEMARKS

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

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-LINK TECHNOLOGIES CO., LTD. Copyright © 2012 TP-LINK TECHNOLOGIES CO., LTD. All rights reserved.

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

FCC STATEMENT



This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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

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

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

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

FCC RF Radiation Exposure Statement

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

“To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.”

CE Mark Warning



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

National restrictions

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

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

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

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: **150Mbps Wireless N Router**

Model No.: **TL-WR740N**

Trademark: **TP-LINK**

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

Directives 1999/5/EC, Directives 2004/108/EC, Directives 2006/95/EC, Directives 1999/519/EC, Directives 2011/65/EU

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

ETSI EN 300 328 V1.7.1: 2006

ETSI EN 301 489-1 V1.8.1:2008& ETSI EN 301 489-17 V2.1.1:2009

EN 55022:2010

EN 55024:2010

EN 61000-3-2:2006+A1:2009+A2:2009

EN 61000-3-3:2008

EN60950-1:2006+A11: 2009+A1:2010+A12:2011

EN62311:2008

The product carries the CE Mark:

CE 1588 

Person is responsible for marking this declaration:



Yang Hongliang

Product Manager of International Business

Date of issue:2012

CONTENTS

Package Contents	1
Chapter 1. Introduction.....	2
1.1 Overview of the Router.....	2
1.2 Conventions	2
1.3 Main Features	3
1.4 Panel Layout	4
1.4.1 The Front Panel.....	4
1.4.2 The Rear Panel	5
Chapter 2. Connecting the Router	6
2.1 System Requirements	6
2.2 Installation Environment Requirements	6
2.3 Connecting the Router	6
Chapter 3. Quick Installation Guide.....	8
3.1 TCP/IP Configuration	8
3.2 Quick Installation Guide	9
Chapter 4. Configuring the Router	16
4.1 Login	16
4.2 Trạng thái	16
4.3 Cài đặt nhanh.....	17
4.4 QSS.....	17
4.5 Mạng	25
4.5.1 WAN	25
4.5.2 LAN.....	34
4.5.3 Bản sao MAC	34
4.6 Không dây	35
4.6.1 Cài đặt không dây.....	35
4.6.2 Bảo mật không dây.....	38
4.6.3 Lọc địa chỉ MAC không dây	41
4.6.4 Không dây nâng cao.....	43
4.6.5 Thống kê không dây	44
4.7 DHCP	45
4.7.1 Cài đặt DHCP	45
4.7.2 Danh sách máy khách DHCP	46

4.7.3	Dành riêng địa chỉ.....	47
4.8	Đang chuyển tiếp	48
4.8.1	Server ảo.....	48
4.8.2	Cổng kích hoạt	50
4.8.3	DMZ.....	52
4.8.4	UPnP	52
4.9	Bảo mật.....	53
4.9.1	Bảo mật cơ bản	54
4.9.2	Bảo mật nâng cao	55
4.9.3	Quản lý nội bộ	56
4.9.4	Quản lý từ xa.....	57
4.10	Quyền kiểm soát của phụ huynh.....	58
4.11	Kiểm soát truy cập.....	61
4.11.1	Điều luật	61
4.11.2	Máy chủ.....	66
4.11.3	Đích đến	68
4.11.4	Thời gian biểu.....	69
4.12	Định tuyến nâng cao	71
4.12.1	Danh sách định tuyến tĩnh	71
4.12.2	Bảng định tuyến hệ thống.....	72
4.13	Kiểm soát băng thông	73
4.13.1	Cài đặt kiểm soát băng thông	73
4.13.2	Danh sách điều luật.....	74
4.14	Kết hợp IP & MAC.....	75
4.14.1	Cài đặt liên kết.....	75
4.14.2	Danh sách ARP	77
4.15	DNS động.....	77
4.15.1	Comexe.cn DDNS	78
4.15.2	Dyndns.org DDNS	78
4.15.3	No-ip.com DDNS	79
4.16	Công cụ hệ thống	81
4.16.1	Cài đặt thời gian	81
4.16.2	Công cụ chẩn đoán	83
4.16.3	Nâng cấp Firmware	84
4.16.4	Cài đặt gốc	85
4.16.5	Sao lưu & Phục hồi.....	86
4.16.6	Khởi động lại	87

4.16.7 Mật mã.....	87
4.16.8 Bản ghi hệ thống	88
4.16.9 Thống kê.....	90
Appendix A: FAQ.....	92
Appendix B: Configuring the PCs.....	97
Appendix C: Specifications	100
Appendix D: Glossary.....	101

Package Contents

The following items should be found in your package:

- TL-WR740N 150Mbps Wireless N Router
- DC Power Adapter for TL-WR740N 150Mbps Wireless N Router
- Quick Installation Guide
- Resource CD for TL-WR740N 150Mbps Wireless N Router, including:
 - This Guide
 - Other Helpful Information

 **Note:**

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

Chapter 1. Introduction

1.1 Overview of the Router

The TL-WR740N 150Mbps Wireless N Router integrates 4-port Switch, Firewall, NAT-Router and Wireless AP. The 150Mbps Wireless N Router delivers exceptional range and speed, which can fully meet the need of Small Office/Home Office (SOHO) networks and the users demanding higher networking performance.

Incredible Speed

The TL-WR740N 150Mbps Wireless N Router provides up to 150Mbps wireless connection with other 802.11n wireless clients. The incredible speed makes it ideal for handling multiple data streams at the same time, which ensures your network stable and smooth. The performance of this 802.11n wireless Router will give you the unexpected networking experience at speed 650% faster than 802.11g. It is also compatible with all IEEE 802.11g and IEEE 802.11b products.

Multiple Security Protections

With multiple protection measures, including SSID broadcast control and wireless LAN 64/128/152-bit WEP encryption, Wi-Fi protected Access (WPA2-PSK, WPA-PSK), as well as advanced Firewall protections, the TL-WR740N 150Mbps Wireless N Router provides complete data privacy.

Flexible Access Control

The TL-WR740N 150Mbps Wireless N Router provides flexible access control, so that parents or network administrators can establish restricted access policies for children or staff. It also supports Virtual Server and DMZ host for Port Triggering, and then the network administrators can manage and monitor the network in real time with the remote management function.

Simple Installation

Since the Router is compatible with virtually all the major operating systems, it is very easy to manage. Quick Setup Wizard is supported and detailed instructions are provided step by step in this user guide. Before installing the Router, please look through this guide to know all the Router's functions.

1.2 Conventions

The Router TL-WR740N mentioned in this guide stands for TL-WR740N 150Mbps Wireless N Router without any explanation.

1.3 Main Features

- Make use of IEEE 802.11n wireless technology to provide a wireless data rate of up to 150Mbps
- One 10/100M Auto-Negotiation RJ45 WAN port, four 10/100M Auto-Negotiation RJ45 LAN ports, supporting Auto MDI/MDIX
- Provides WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security
- Shares data and Internet access for users, supporting Dynamic IP/Static IP/PPPoE Internet access
- Supports Virtual Server, Special Application and DMZ host
- Supports UPnP, Dynamic DNS, Static Routing
- Provides Automatic-connection and Scheduled Connection on certain time to the Internet
- Connects Internet on demand and disconnects from the Internet when idle for PPPoE
- Built-in NAT and DHCP server supporting static IP address distributing
- Supports Stateful Packet Inspection
- Supports VPN Passthrough
- Supports Parental Control and Access Control
- Provides 64/128/152-bit WEP encryption security and wireless LAN ACL (Access Control List)
- Supports Flow Statistics
- Supports firmware upgrade and Web management
- Provide a switch for the power

1.4 Panel Layout

1.4.1 The Front Panel

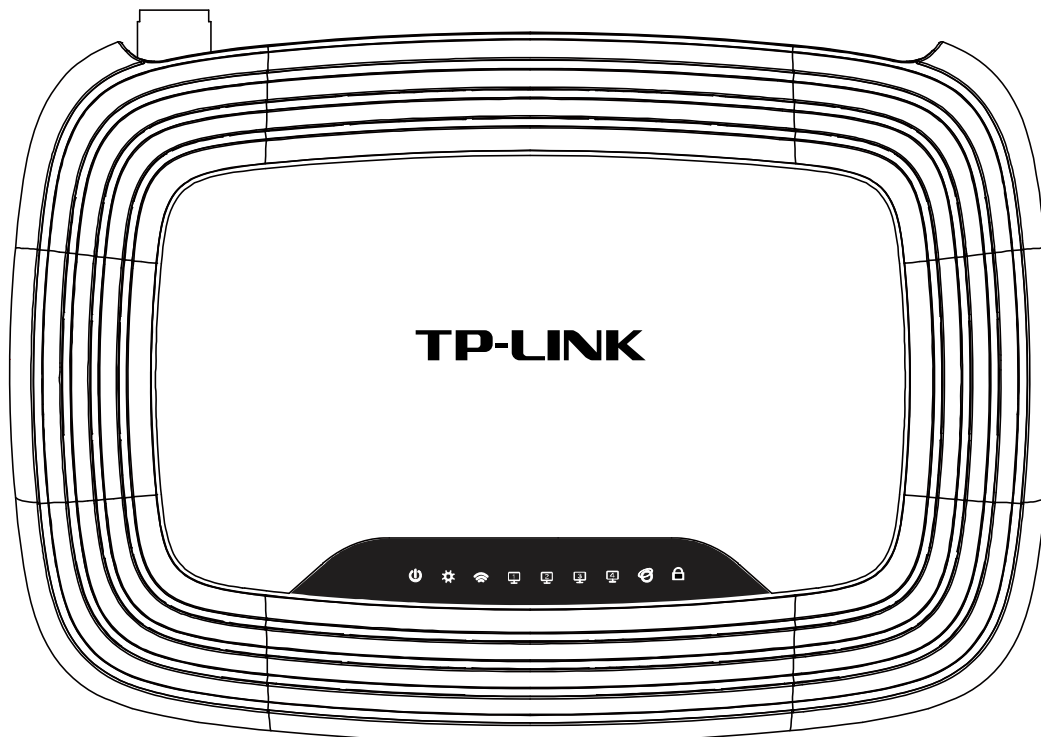


Figure 1-1 Front Panel sketch

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

Name	Status	Indication
⏻ (Power)	Off	Power is off.
	On	Power is on.
⚙️ (System)	Flashing	The Router is working properly.
	On /Off	The Router has a system error.
📶 (WLAN)	Off	The Wireless function is disabled.
	Flashing	The Wireless function is enabled.
🌐 (WAN), 📡 (LAN 1-4)	Off	There is no device linked to the corresponding port.
	On	There is a device linked to the corresponding port but there is no activity.
	Flashing	There is an active device linked to the corresponding port.
🔒 (QSS)	Slow Flash	A wireless device is connecting to the network by QSS function. This process will last in the first 2 minutes.
	On	A wireless device has been successfully added to the network by QSS function.
	Quick Flash	A wireless device failed to be added to the network by QSS function.

Table 1-1 The LEDs description

Note:

After a device is successfully added to the network by QSS function, the QSS LED will keep on for about 5 minutes and then turn off.

1.4.2 The Rear Panel

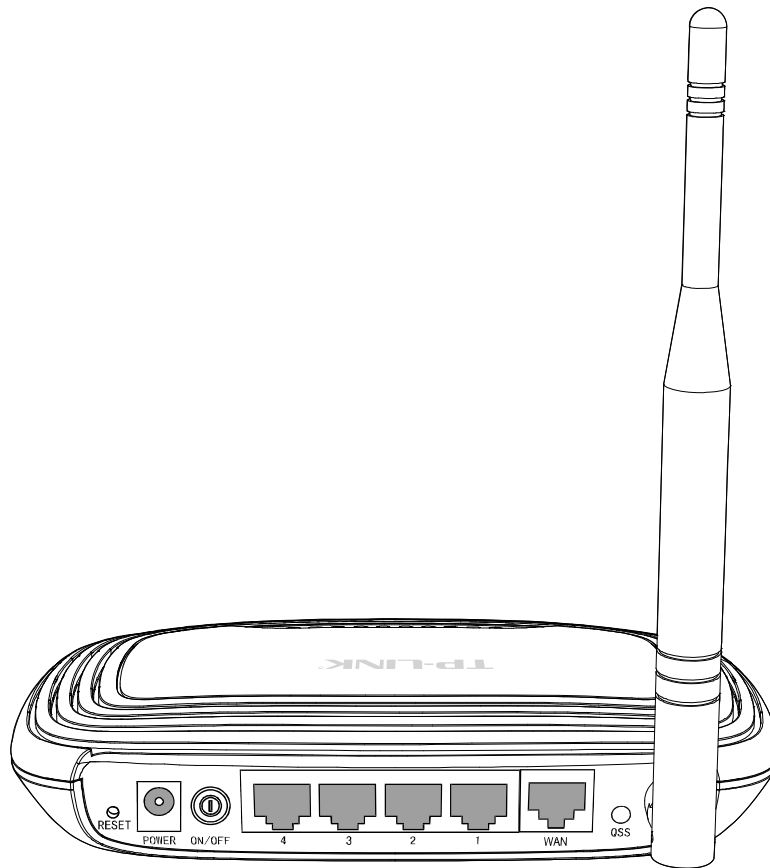


Figure 1-2 Rear Panel sketch

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

➤ **RESET:**

There are two ways to reset to 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: Press the Reset button for five seconds and then wait for the Router to reboot.

➤ **POWER:** The Power socket is where you will connect the power adapter. Please use the power adapter provided with this TL-WR740N 150Mbps Wireless N Router.

➤ **ON/OFF:** The switch for the power.

➤ **1,2,3,4 (LAN):** These ports (1, 2, 3, 4) connect the Router to the local PC(s).

➤ **WAN:** This WAN port is where you will connect the DSL/cable Modem, or Ethernet.

➤ **Wireless antenna:** To receive and transmit the wireless data.

Chapter 2. Connecting the Router

2.1 System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable Modem that has an RJ45 connector (which is not necessary if the Router is connected directly to the Ethernet.)
- PCs with a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- TCP/IP protocol on each PC
- Web browser, such as Microsoft Internet Explorer 5.0 , Netscape Navigator 6.0 or above

2.2 Installation Environment Requirements

- Place the Router in a well ventilated place far from any heater or heating vent
- Avoid direct irradiation of any strong light (such as sunlight)
- Keep at least 2 inches (5 cm) of clear space around the Router
- Operating Temperature: 0°C~40°C (32°F~104°F)
- Operating Humidity: 10%~90%RH, Non-condensing

2.3 Connecting the Router

Before installing the Router, make sure your PC is connected to the Internet through the 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 PC, Cable/DSL Modem, and the Router.
2. Locate an optimum location for the Router. The best place is usually at the center of your wireless network. 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 PC(s) and each Switch/Hub in your LAN to the LAN Ports on the Router, shown in Figure 2-1. (If you have the wireless NIC and want to use the wireless function, you can skip this step.)
5. Connect the DSL/Cable Modem to the WAN port on the Router, shown in Figure 2-1.
6. Connect the power adapter to the power socket on the Router, and the other end into an

electrical outlet. The Router will start to work automatically.

7. Power on your PC and Cable/DSL Modem.

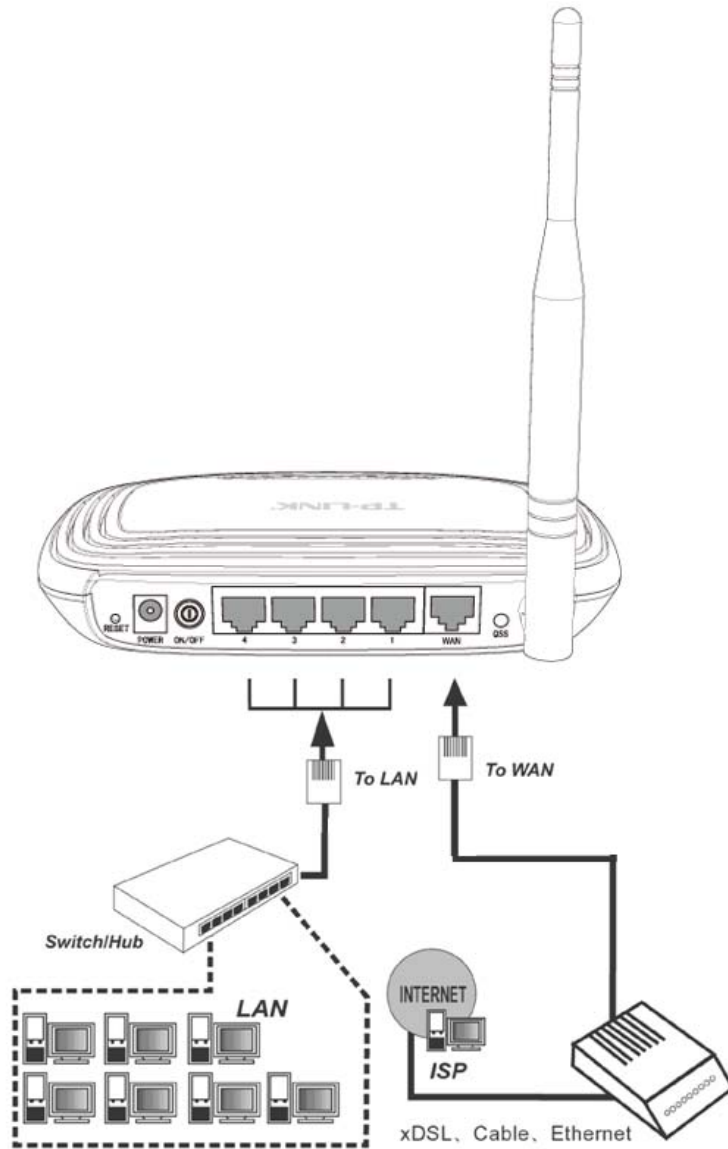


Figure 2-1 Hardware Installation of the TL-WR740N 150Mbps Wireless N Router

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your TL-WR740N 150Mbps Wireless N Router using **Quick Setup Wizard** within minutes.

3.1 TCP/IP Configuration

The default domain name of the TL-WR740N 150Mbps Wireless N Router is <http://tplinklogin.net>, the default IP address is 192.168.0.1, and the default Subnet Mask is 255.255.255.0. These values can be changed as you desire. In this guide, we all use the default values for description.

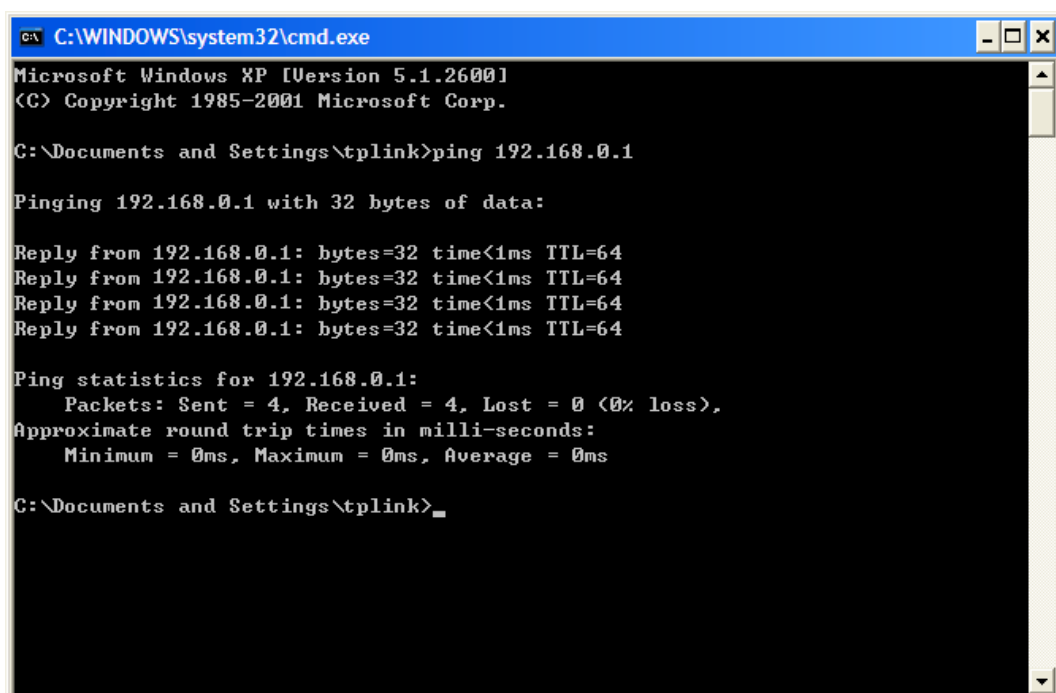
Connect the local PC to the LAN ports of the Router, and then you can configure the IP address for your PC by following the steps below:

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

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

Open a command prompt, and type *ping 192.168.0.1*, and then press **Enter**.

- If the result displayed is similar to the Figure 3-1, it means the connection between your PC and the Router has been established well.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\tplink>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

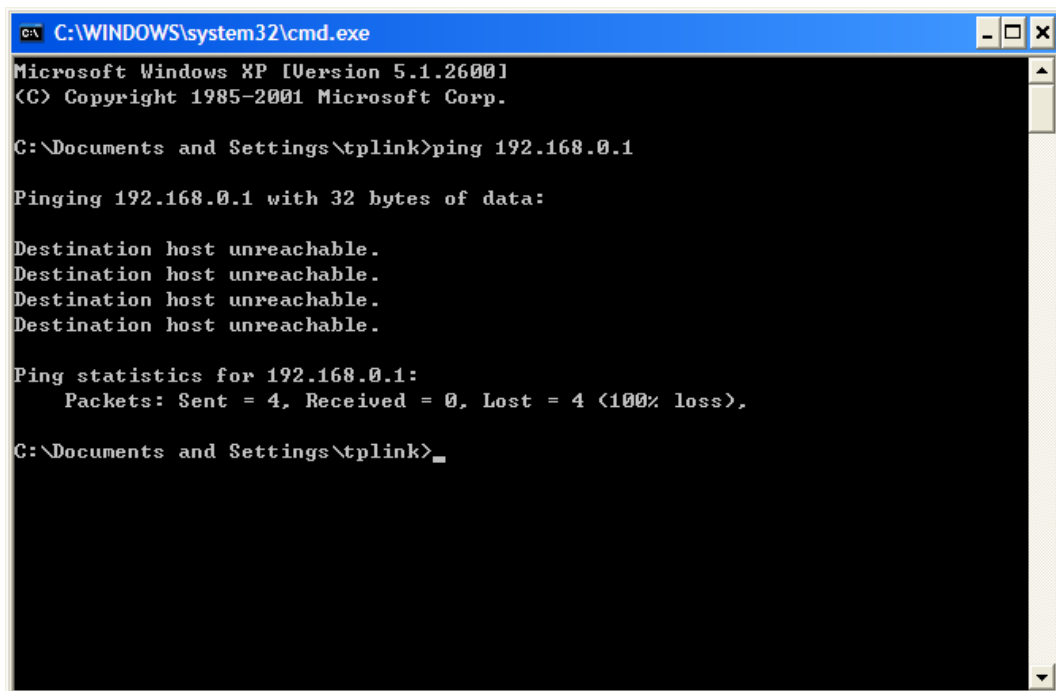
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\tplink>
```

Figure 3-1 Success result of Ping command

- If the result displayed is similar to the Figure 3-2, it means the connection between your PC and the Router failed.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\tplink>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\tplink>
```

Figure 3-2 Failure result of Ping command

Please check the connection following these steps:

1. Is the connection between your PC and the Router correct?

Note:

The 1/2/3/4 LEDs of LAN ports which you link to on the Router and LEDs on your PC's adapter should be lit.

2. Is the TCP/IP configuration for your PC correct?

Note:

If the Router's IP address is 192.168.0.1, your PC's IP address must be within the range of 192.168.0.2 ~ 192.168.0.254.

3. Try the IP address 192.168.1.1.

Note:

If the LAN IP of the modem connected with your router is 192.168.0.x, the default LAN IP of the Router will automatically switch from 192.168.0.1 to 192.168.1.1 to avoid IP conflict. Therefore, in order to verify the network connection between your PC and the Router, you can open a command prompt, and type *ping 192.168.1.1*, and then press **Enter**.

3.2 Quick Installation Guide

With a Web-based (Internet Explorer or Netscape® Navigator) utility, it is easy to configure and manage the TL-WR740N 150Mbps Wireless N Router. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser.

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



Figure 3-3 Login the Router

After a moment, a login window will appear, similar to the Figure 3-4. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.



Figure 3-4 Login Windows

Note:

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

2. After successfully login, you can click the **Cài đặt nhanh** to quickly configure your Router.

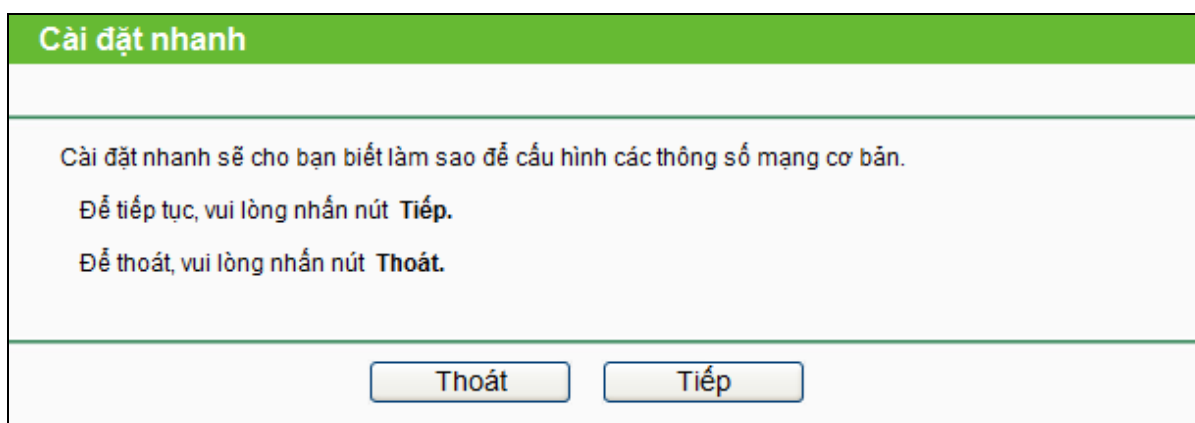


Figure 3-5 Quick Setup

3. Click **Tiếp**, and then **Dạng kết nối WAN** page will appear as shown in Figure 3-6.

Cài đặt nhanh – Dạng kết nối WAN

Cài đặt nhanh đang chuẩn bị thiết lập dạng kết nối của bạn cho cổng WAN.

Router sẽ cố gắng phát hiện dạng kết nối Internet do nhà cung cấp dịch vụ Internet của bạn cung cấp nếu bạn chọn tùy chọn **Phát hiện tự động**. Ngược lại, bạn cần phải xác định dạng kết nối theo cách thủ công.

- Phát hiện tự động** - Để Router tự động phát hiện dạng kết nối do nhà cung cấp dịch vụ Internet của bạn cung cấp.
- PPPoE** - Thường đối với Modem ADSL và bạn cần tên đăng nhập và mật mã PPPoE từ nhà cung cấp dịch vụ Internet của bạn.
- IP động** - Thường cho Modem dây cáp và router sẽ tự động lấy địa chỉ IP từ server DHCP.
- IP tĩnh** - Dạng kết nối này dùng địa chỉ IP (tĩnh) cố định, vĩnh viễn mà nhà cung cấp dịch vụ Internet của bạn đã gán.

Figure 3-6 Choose WAN Connection Type

The Router provides **Phát hiện tự động** function and supports three popular ways **PPPoE**, **IP Động** and **IP Tĩnh** to connect to the Internet. It's recommended that you make use of the **Phát hiện tự động** function. If you are sure of what kind of connection type your ISP provides, you can select the very type and click **Tiếp** to go on configuring.

4. If you select **Phát hiện tự động**, the Router will automatically detect the connection type your ISP provides. Make sure the cable is securely plugged into the WAN port before detection. The appropriate configuration page will be displayed when an active Internet service is successfully detected by the Router.
 - If the connection type detected is **PPPoE**, the next screen will appear as shown in Figure 3-7.

Cài đặt nhanh - PPPoE

Tên đăng nhập:

Mật mã:

Mật mã xác nhận:

Figure 3-7 Quick Setup – PPPoE

- **Tên đăng nhập and Mật mã** - Enter the **Tên đăng nhập** and **Mật mã** provided by your ISP. These fields are case sensitive. If you have difficulty with this process, please contact your ISP.
- **Mật mã xác nhận** - Re-enter the password provided by your ISP to ensure the Password you entered is correct. If the Password is different from the Confirm Password, the screen will appear as shown below. Click **OK**, and re-enter the Password and Confirm Password.



- If the connection type detected is Dynamic IP, the next screen will appear as shown in Figure 3-8.
 - If you are visiting the Router from the main computer, please select **Đúng**, and then click **Sao địa chỉ MAC đến**.

Sao địa chỉ MAC

Vui lòng đọc mục **Giúp đỡ ở bên phải một cách cẩn thận.**

Đúng, Tôi đã kết nối bằng máy tính chính (địa chỉ MAC bản sao)
 Không, Tôi đang kết nối bằng một máy tính khác (không phải địa chỉ MAC bản sao)

Địa chỉ MAC WAN:	00-08-01-00-00-05	Khôi phục địa chỉ MAC gốc
Địa chỉ MAC máy tính của bạn:	00-19-66-80-54-2B	Sao địa chỉ MAC đến

Figure 3-8 Quick Setup – MAC Clone

- If you are visiting the Router from another computer, rather than the main computer, please select **Không**, and then enter the main computer's MAC in the field **Địa chỉ MAC WAN**.

Sao địa chỉ MAC

Vui lòng đọc mục **Giúp đỡ ở bên phải một cách cẩn thận.**

Đúng, Tôi đã kết nối bằng máy tính chính (địa chỉ MAC bản sao)
 Không, Tôi đang kết nối bằng một máy tính khác (không phải địa chỉ MAC bản sao)

Địa chỉ MAC WAN:	00-1D-0F-01-06-17	Khôi phục địa chỉ MAC gốc
Địa chỉ MAC máy tính của bạn:	40-61-86-e5-b2-dc	Sao địa chỉ MAC đến

Figure 3-9 Quick Setup – MAC Clone

- If the connection type detected is Static IP, the next screen will appear as shown in Figure 3-10.

Figure 3-10 Quick Setup - Static IP

- **Địa chỉ IP** - This is the WAN IP address seen by external users on the Internet (including your ISP). Enter the IP address into the field.
- **Subnet Mask** - The Subnet Mask is used for the WAN IP address, it is usually 255.255.255.0.
- **Gateway mặc định** - Enter the gateway IP address into the box if required.
- **DNS chính** - Enter the DNS Server IP address into the box if required.
- **DNS thứ hai** - If your ISP provides another DNS server, enter it into this field.

5. Click **Tiếp** to continue, the Wireless settings page will appear as shown in Figure 3-11.

Figure 3-11 Quick Setup – Wireless

- **Vô tuyến không dây** - Enable or disable the wireless radio by choosing from the drop-down list.

- **SSID** - Enter a value of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security, the default SSID is set to be TP-LINK_XXXXXX (XXXXXX indicates the last unique six numbers of each Router's MAC address). This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- **Khu vực** - Select your region from the drop-down list. This field specifies the region where the wireless function of the Router can be used. It may be illegal to use the wireless function of the Router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.
- **Kênh** - This field determines which operating frequency will be used. The default channel is set to **Tự động**, so the AP will choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Chế độ** - This field determines the wireless mode which the Router works on.
- **Độ rộng kênh** - Select any channel width from the drop-down list. The default setting is automatic, which can automatically adjust the channel width for your clients.
- **Tỷ lệ Tx tối đa** - You can limit the maximum transmission rate of the Router through this field.
- **Vô hiệu hóa bảo mật** - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Router without encryption. It is strongly recommended that you choose one of following options to enable security.
- **WPA-Cá nhân/WPA2-Cá nhân** - Select WPA based on pre-shared passphrase.
 - **Mật mã** - You can enter **mã ASCII** or **Thập lục phân** characters.

For **ASCII**, the key can be made up of any numbers from 0 to 9 and any letters from A to Z, and the length should be between 8 and 63 characters.

For **Thập lục phân**, the key can be made up of any numbers from 0 to 9 and letters from A to F, and the length should be between 8 and 64 characters.

Please also note the key is case sensitive, which means that upper and lower case keys will affect the outcome. It would also be a good idea to write down the key and all related wireless security settings.
- **Sử dụng cài đặt trước** - If you choose this option, wireless security configuration will not change!

These settings are only for basic wireless parameters. For advanced settings, please refer to [4.6: "Không dây"](#).

6. Click the **Tiếp** button. You will then see the **Hoàn tất** page.

If you don't make any changes on the **Không dây** page, you will see the **Hoàn tất** page as shown in Figure 3-12. Click the **Hoàn tất** button to finish the **Cài đặt nhanh**.

Cài đặt nhanh – Hoàn tất	
<p>Xin chúc mừng! Bây giờ Router đã kết nối bạn đến mạng Internet. Để cài đặt chi tiết, vui lòng bấm chọn các thanh khác nếu cần thiết.</p>	
<input type="button" value="Quay lại"/>	<input type="button" value="Hoàn tất"/>

Figure 3-12 Quick Setup – Finish

If there is something changed on the **Không dây** page, you will see the **Hoàn tất** page as shown in Figure 3-13. Click the **Khởi động lại** button to make your wireless configuration take effect and finish the **Cài đặt nhanh**.

Cài đặt nhanh – Hoàn tất	
<p>Xin chúc mừng! Bây giờ Router đã kết nối bạn đến mạng Internet. Để cài đặt chi tiết, vui lòng bấm chọn các thanh khác nếu cần thiết.</p> <p style="color: red;">Thay đổi cấu hình không dây sẽ không có hiệu lực cho đến khi Router khởi động lại.</p>	
<input type="button" value="Quay lại"/>	<input type="button" value="Khởi động lại"/>

Figure 3-13 Quick Setup - Finish

Chapter 4. Configuring the Router

This chapter will show each Web page's key functions and the configuration way.

4.1 Login

After your successful login, you will see the sixteen main menus on the left of the Web-based utility. On the right, there are the corresponding explanations and instructions.

Trạng thái
Cài đặt nhanh
QSS
Mạng
Không dây
DHCP
Đang chuyển tiếp
Bảo mật
Kiểm soát của phụ huynh
Kiểm soát truy cập
Định tuyến nâng cao
Kiểm soát băng thông
Kết hợp IP & MAC
DNS động
Công cụ hệ thống

The detailed explanations for each Web page's key function are listed below.

4.2 Trạng thái

The Status page provides the current status information about the Router. All information is read-only.

Trạng thái		
Phiên bản Firmware:	3.12.11 Build 120614 Rel.51047n	
Phiên bản phần cứng:	WR740N v4 00000000	
LAN		
Địa chỉ MAC:	00-1D-0F-01-06-16	
Địa chỉ IP:	192.168.0.1	
Subnet Mask:	255.255.255.0	
Không dây		
Vô tuyến không dây:	Kích hoạt	
Tên (SSID):	TP-LINK_010616	
Kênh:	Tự động (Kênh hiện tại 1)	
Chế độ:	Hỗn hợp 11bgn	
Độ rộng kênh:	Tự động	
Địa chỉ MAC:	00-1D-0F-01-06-16	
Trạng thái WDS:	Vô hiệu hóa	
WAN		
Địa chỉ MAC:	00-1D-0F-01-06-17	
Địa chỉ IP:	0.0.0.0	PPPoE(Kết nối theo yêu cầu)
Subnet Mask:	0.0.0.0	
Gateway mặc định:	0.0.0.0	
Server DNS:	0.0.0.0, 0.0.0.0	
Thời gian sử dụng mạng:	0 ngày 00:00:00	<input type="button" value="Kết nối"/>
Thống kê lưu lượng		
	Đã nhận	Đã gửi
Byte:	0	0
Gói tin:	0	0
Thời gian hoạt động của hệ thống:	0 ngày 00:20:17	<input type="button" value="Làm mới"/>

Figure 4-1 Router Status

4.3 Cài đặt nhanh

Please refer to [3.2: "Quick Installation Guide."](#)

4.4 QSS

This section will guide you to add a new wireless device to an existing network quickly by **QSS (Thiết lập bảo mật nhanh)** function.

a). Choose menu “**QSS**”, and you will see the next screen (shown in Figure 4-2).

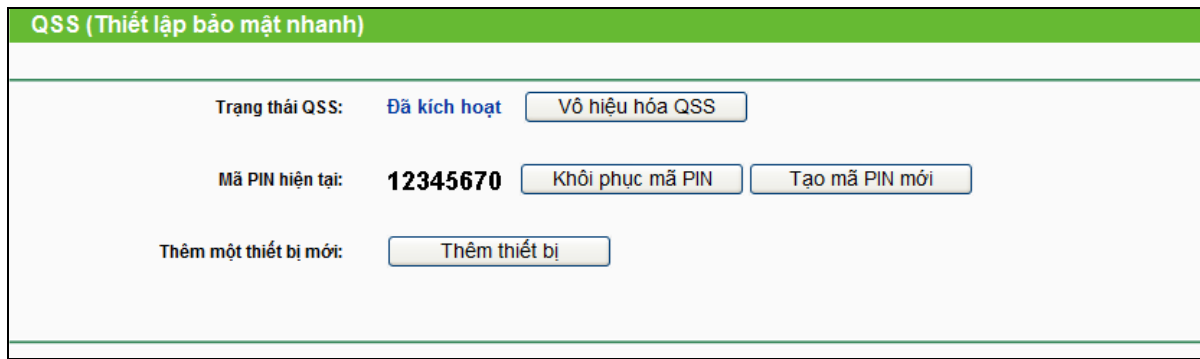


Figure 4-2 QSS

- **Trạng thái QSS** - Enable or disable the QSS function here.
- **Mã PIN hiện tại** - The current value of the Router's PIN displayed here. The default PIN of the Router can be found in the label or User Guide.
- **Khôi phục mã PIN** - Restore the PIN of the Router to its default.
- **Tạo mã PIN mới** - Click this button, and then you can get a new random value for the Router's PIN. You can ensure the network security by generating a new PIN.
- **Thêm thiết bị** - You can add the new device to the existing network manually by clicking this button.

b). To add a new device:

If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless adapter and Router using either Push Button Configuration (PBC) method or PIN method.

 **Note:**

To build a successful connection by QSS, you should also do the corresponding configuration of the new device for QSS function meanwhile.

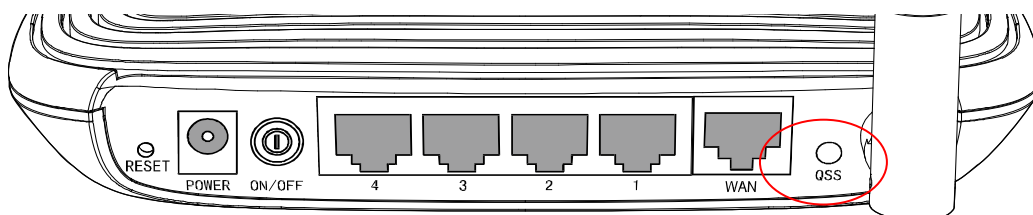
For the configuration of the new device, here takes the Wireless Adapter of our company for example.

I. By PBC

If the wireless adapter supports Wi-Fi Protected Setup (also called QSS) and the Push Button Configuration (PBC) method, you can add it to the network by PBC with the following two methods.

Method One:

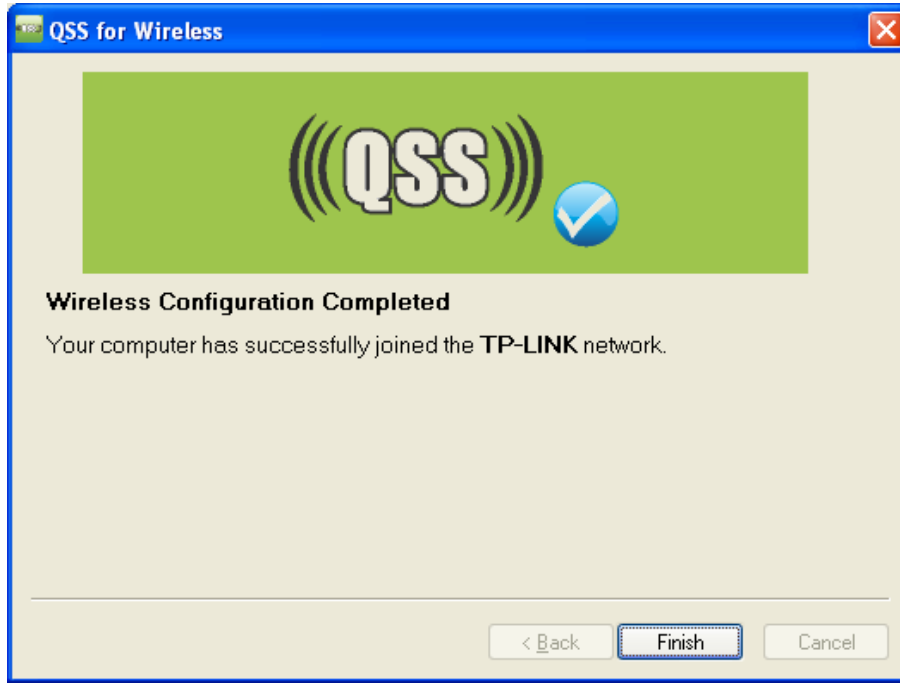
Step 1. Press the QSS button on the front panel of the Router.



Step 2. Press and hold the QSS button of the adapter directly for 2 or 3 seconds.



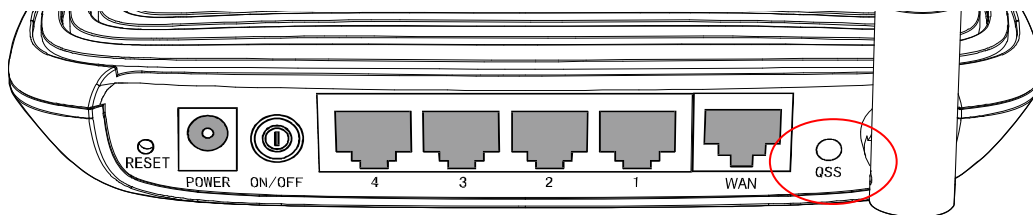
Step 3. Wait for a while until the next screen appears. Click **Finish** to complete the QSS configuration.



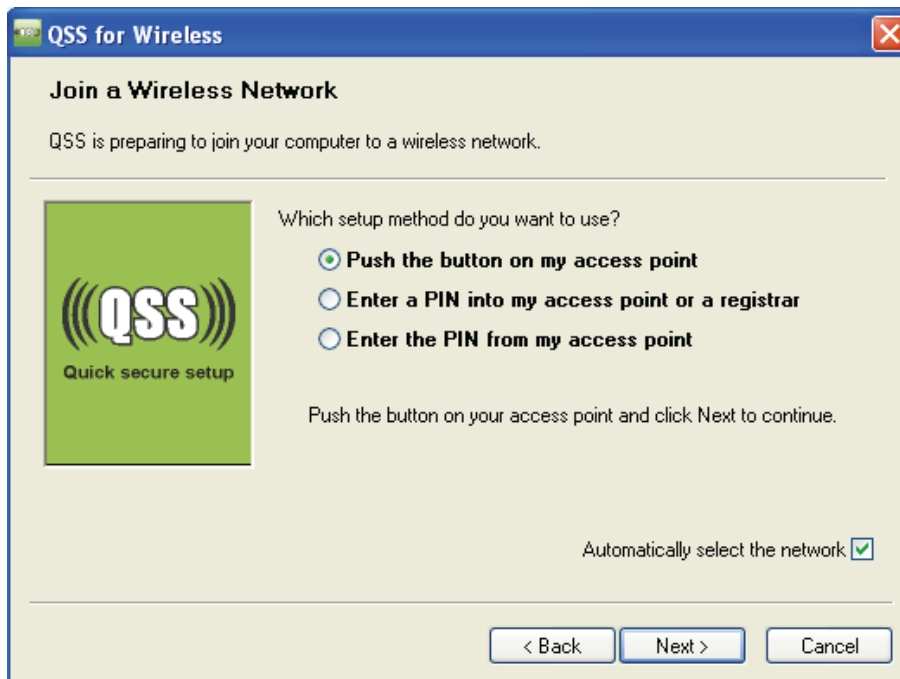
The QSS Configuration Screen of Wireless Adapter

Method Two:

Step 1. Press the QSS button on the front panel of the Router.

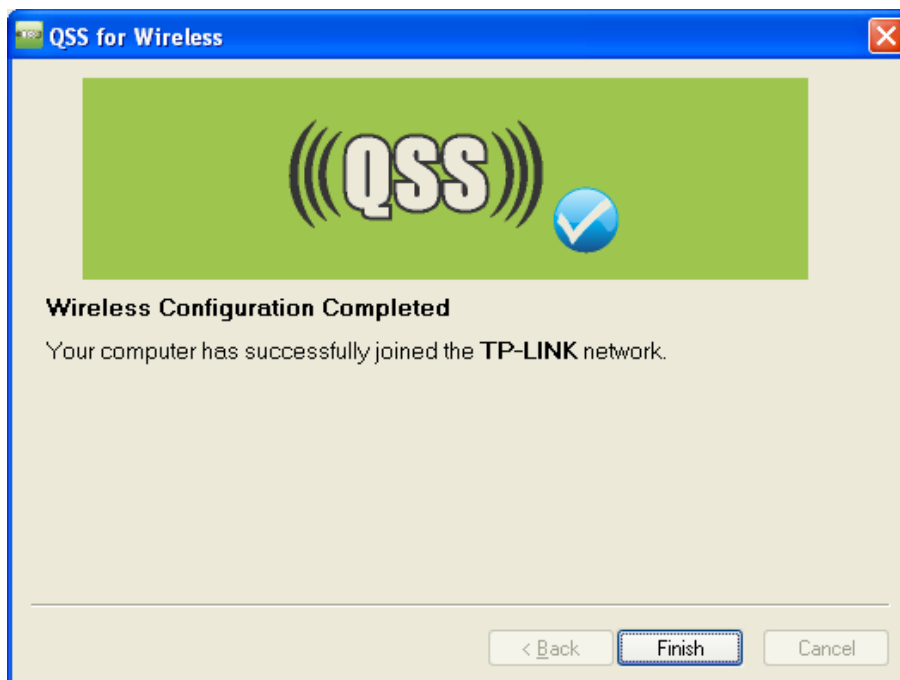


Step 2. For the configuration of the wireless adapter, please choose **Push the button on my access point** in the configuration utility of the QSS as below, and click **Next**.



The QSS Configuration Screen of Wireless Adapter

Step 3. Wait for a while until the next screen appears. Click **Finish** to complete the QSS configuration.



The QSS Configuration Screen of Wireless Adapter

Method Three:

Step 1. Keep the default QSS Status as **Đã kích hoạt** and click the **Thêm thiết bị mới** button in Figure 4-2, then the following screen will appear.

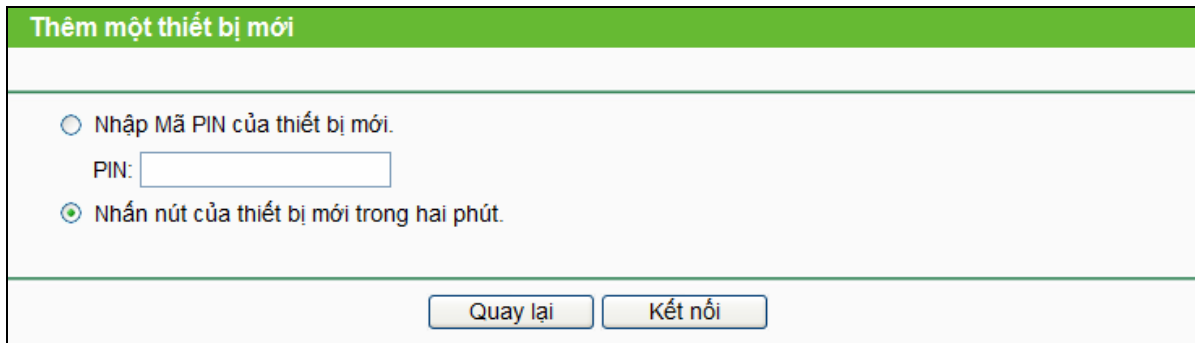
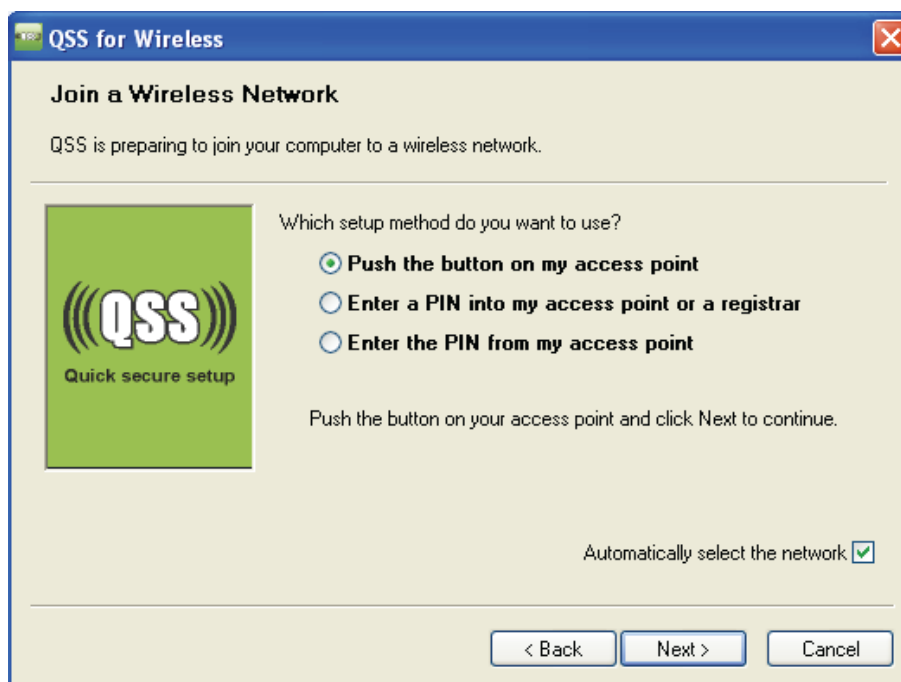


Figure 4-3 Add A New Device

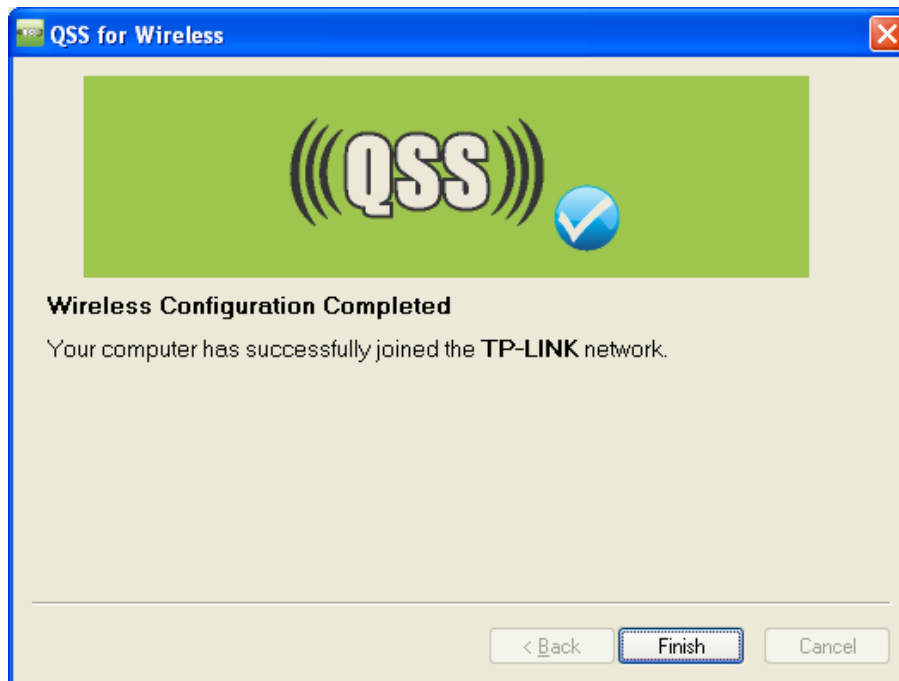
Step 2. Choose **Nhấn nút của thiết bị mới** in two minutes and click **Kết nối**.

Step 3. For the configuration of the wireless adapter, please choose **Push the button on my access point** in the configuration utility of the QSS as below, and click **Next**.



The QSS Configuration Screen of Wireless Adapter

Step 4. Wait for a while until the next screen appears. Click **Finish** to complete the QSS configuration.



The QSS Configuration Screen of Wireless Adapter

II. By PIN

If the new device supports Wi-Fi Protected Setup and the PIN method, you can add it to the network by PIN with the following two methods.

Method One: Enter the PIN into my Router

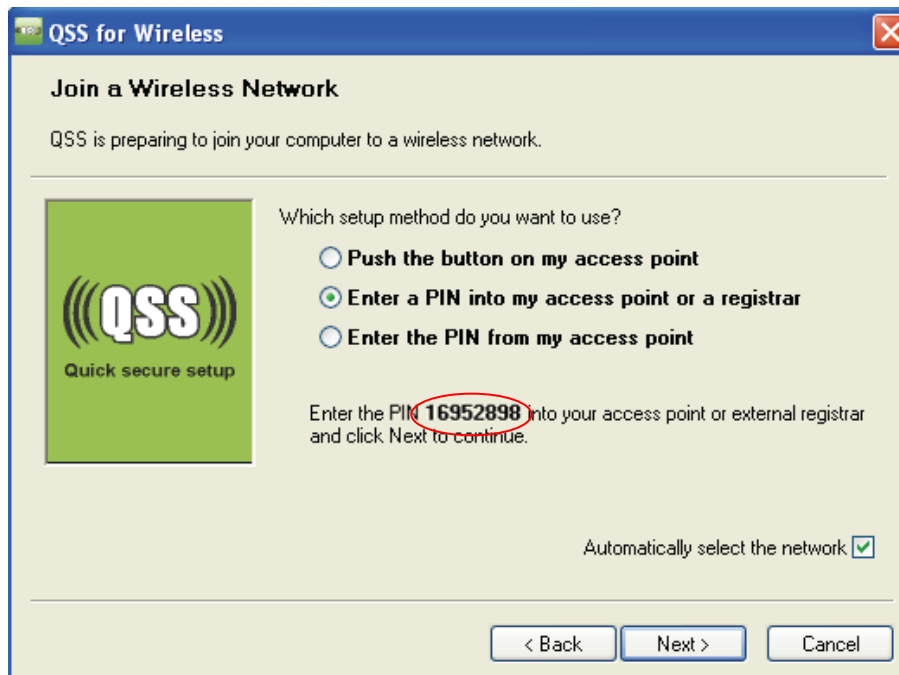
Step 1. Keep the default QSS Status as **Đã kích hoạt** and click the **Thêm thiết bị mới** button in Figure 4-2, then the following screen will appear.

Step 2. Choose **Nhập Mã PIN của thiết bị mới** and enter the PIN code of the wireless adapter in the field behind PIN in the above figure. Then click **Kết nối**.

 **Note:**

The PIN code of the adapter is always displayed on the QSS configuration screen

- Step 3. For the configuration of the wireless adapter, please choose **Enter a PIN into my access point or a registrar** in the configuration utility of the QSS as below, and click **Next**.



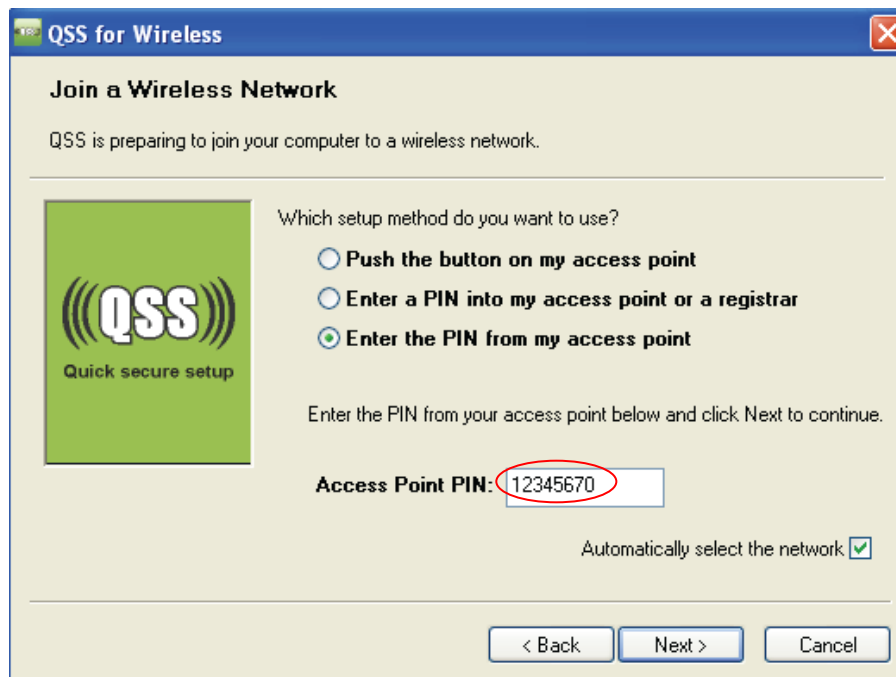
The QSS Configuration Screen of Wireless Adapter

Note:

In this example, the default PIN code of this adapter is 16952898 as the above figure shown.

Method Two: Enter the PIN from my Router

- Step 1. Get the Current PIN code of the Router in Figure 4-2 (each Router has its unique PIN code. Here takes the PIN code 12345670 of this Router for example).
- Step 2. For the configuration of the wireless adapter, please choose **Enter a PIN from my access point** in the configuration utility of the QSS as below, and enter the PIN code of the Router into the field behind Access Point PIN. Then click **Next**.

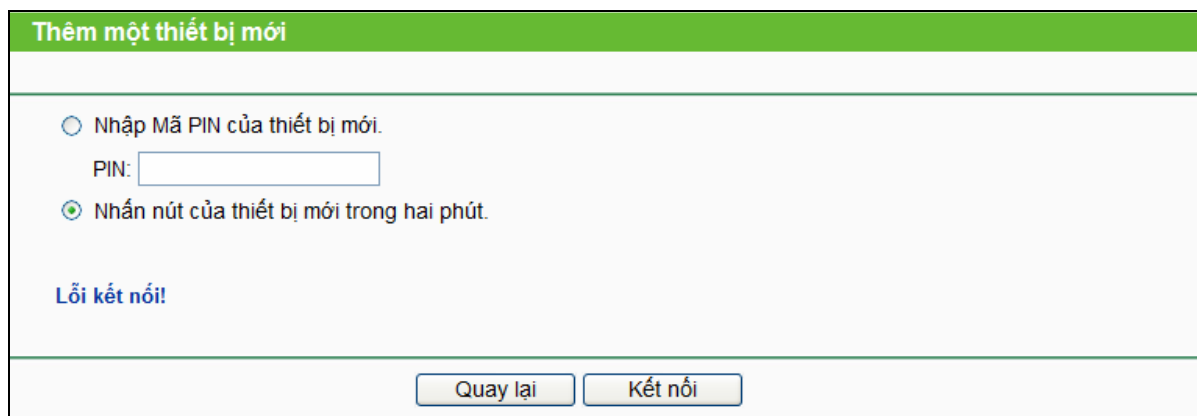


The QSS Configuration Screen of Wireless Adapter

Note:

The default PIN code of the Router can be found in its label or the QSS configuration screen as Figure 4-2.

Step 3. You will see the following screen when the new device successfully connected to the network.



Note:

1. The status LED on the Router will light green all the time if the device has been successfully added to the network.
2. The QSS function cannot be configured if the Wireless Function of the Router is disabled. Please make sure the Wireless Function is enabled before configuring the QSS.

4.5 Mạng



Figure 4-4 the Network menu

There are three submenus under the Network menu (shown in Figure 4-4): **WAN**, **LAN** and **Bản sao MAC**. Click any of them, and you will be able to configure the corresponding function.

4.5.1 WAN

Choose menu “**Mạng**→**WAN**”, and then you can configure the IP parameters of the WAN on the screen below.

1. If your ISP provides the DHCP service, please choose **IP động** type, and the Router will automatically get IP parameters from your ISP. You can see the page as follows (Figure 4-5):

 A screenshot of the WAN configuration page. The title bar is green and says 'WAN'. The main content area has a white background with green borders. It contains several configuration fields:

- 'Dạng kết nối WAN:' with a dropdown menu set to 'IP động' and a 'Phát hiện' button.
- 'Địa chỉ IP:' with the value '0.0.0.0'.
- 'Subnet Mask:' with the value '0.0.0.0'.
- 'Gateway mặc định:' with the value '0.0.0.0'.
- Below these are 'Làm mới' and 'Giải phóng' buttons, followed by a red error message: 'Cổng WAN hiện không kết nối!'.
- 'Kích thước MTU (đơn vị byte):' with a text box containing '1500' and a note: '(Giá trị mặc định là 1500, vui lòng không thay đổi trừ trường hợp cần thiết.)'
- A checkbox 'Sử dụng các Server DNS sau' which is unchecked.
- 'DNS chính:' with a text box containing '0.0.0.0'.
- 'DNS thứ hai:' with a text box containing '0.0.0.0' and '(Tùy chọn)'.
- 'Tên máy chủ:' with a text box containing 'TL-WR740N'.
- Another checkbox 'Lấy IP bằng Unicast DHCP (Thường không được yêu cầu.)' which is unchecked.
- At the bottom is a 'Lưu' button.

Figure 4-5 WAN - Dynamic IP

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

- **Kích thước MTU (đơn vị Byte)** - The normal **MTU** (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default **Kích thước MTU (đơn vị Byte)** unless required by your ISP.
- **Sử dụng các Server DNS sau** - If your ISP gives you one or two DNS addresses, select **Sử dụng các Server DNS sau** and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from your ISP.

 **Note:**

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

- **Lấy IP bằng Unicast DHCP** - A few ISPs' DHCP servers do not support the broadcast applications. If you cannot get the IP Address normally, you can choose this option. (It is rarely required.)
2. If your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting, select **IP tĩnh**. The Static IP settings page will appear as shown in Figure 4-6.

WAN	
Dạng kết nối WAN:	IP tĩnh <input type="button" value="Phát hiện"/>
Địa chỉ IP:	<input type="text" value="0.0.0.0"/>
Subnet Mask:	<input type="text" value="0.0.0.0"/>
Gateway mặc định:	<input type="text" value="0.0.0.0"/> (Tùy chọn)
Kích thước MTU (tính bằng bytes):	<input type="text" value="1500"/> (Giá trị mặc định là 1500, vui lòng không thay đổi trừ trường hợp cần thiết.)
DNS chính:	<input type="text" value="0.0.0.0"/> (Tùy chọn)
DNS thứ hai:	<input type="text" value="0.0.0.0"/> (Tùy chọn)
<input type="button" value="Lưu"/>	

Figure 4-6 WAN - Static IP

- **Địa chỉ IP** - Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask** - Enter the subnet Mask provided by your ISP in dotted-decimal notation. Usually, the Sub Mask is 255.255.255.0.
- **Gateway mặc định** - (Optional) Enter the gateway IP address provided by your ISP in dotted-decimal notation.
- **Kích thước MTU (tính bằng bytes)** - The normal **MTU** (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default **Kích thước MTU (tính bằng bytes)** unless required by your ISP.

- **DNS chính/DNS thứ hai** - (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.
3. If your ISP provides a PPPoE connection, select **PPPoE/Russia PPPoE** option. And you should enter the following parameters (Figure 4-7):

Figure 4-7 WAN - PPPoE

- **Tên đăng nhập/Mật mã** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Xác nhận mật mã** - Re-enter the Password provided by your ISP to ensure the Password you entered is correct.
- **Kết nối thứ hai** - It's available only for PPPoE Connection. If your ISP provides an extra Connection type such as Dynamic/Static IP to connect to a local area network, then you can check the radio button of Dynamic/Static IP to activate this secondary connection.
 - **Đã vô hiệu hóa** - The Secondary Connection is disabled by default, so there is PPPoE connection only. This is recommended.
 - **IP Động** - You can check this radio button to use Dynamic IP as the secondary connection to connect to the local area network provided by ISP.
 - **IP Tĩnh** - You can check this radio button to use Static IP as the secondary connection to connect to the local area network provided by ISP.
- **Kết nối theo yêu cầu** - In this mode, the Internet connection can be terminated automatically after a specified inactivity period (**Thời gian nghỉ tối đa**) and **be** re-established when you

attempt to access the Internet again. If you want your Internet connection keeps active all the time, please enter “0” in the **Thời gian nghỉ tối đa** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.

- **Kết nối tự động** - The connection can be re-established automatically when it was down.
- **Kết nối dựa trên thời gian** - The connection will only be established in the period from the start time to the end time (both are in HH:MM format).

 **Note:**

Only when you have configured the system time on **Công cụ hệ thống -> Cài đặt thời gian** page, will the **Time-based Connecting** function can take effect.

- **Kết nối thủ công** - You can click the **Kết nối/ Ngắt kết nối** button to connect/disconnect immediately. This mode also supports the **Thời gian nghỉ tối đa** function as **Kết nối theo yêu cầu** mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again.

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

If you want to do some advanced configurations, please click the **Nâng cao** button, and the page shown in Figure 4-8 will then appear:

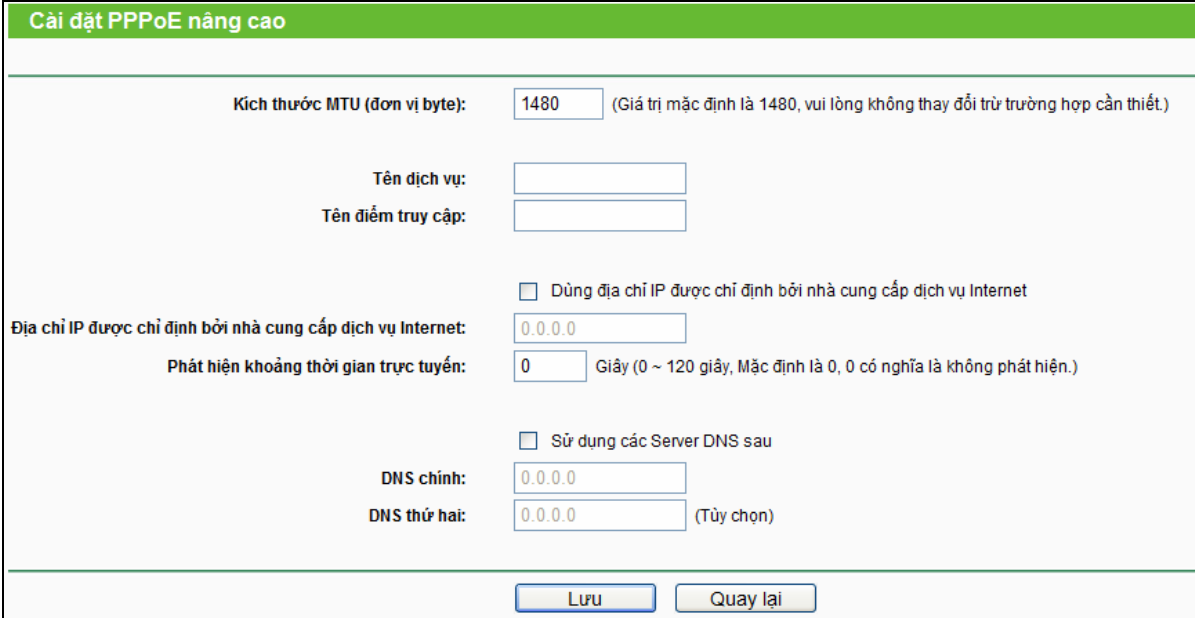


Figure 4-8 PPPoE Advanced Settings

- **Kích thước MTU (đơn vị byte)** - The default MTU size is “1480” bytes, which is usually fine. It is not recommended that you change the default **Kích thước MTU (đơn vị byte)** unless required by your ISP.
- **Tên dịch vụ/Tên điểm truy cập** - The service name and AC (Access Concentrator) name,

which should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.

- **Địa chỉ IP được chỉ định bởi nhà cung cấp dịch vụ Internet** - If your ISP does not automatically assign IP addresses to the Router during login, please click “**Địa chỉ IP được chỉ định bởi nhà cung cấp dịch vụ Internet**” check box and enter the IP address provided by your ISP in dotted-decimal notation.
- **Phát hiện khoảng thời gian trực tuyến** - The Router will detect Access Concentrator online at every interval. The default value is “0”. You can input the value between “0”and “120”. The value “0” means no detect.
- **Địa chỉ IP DNS** - If your ISP does not automatically assign DNS addresses to the Router during login, please click “**Sử dụng các Server DNS sau**” check box and enter the IP address in dotted-decimal notation of your ISP’s primary DNS server. If a secondary DNS server address is available, enter it as well.

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

4. If your ISP provides BigPond Cable (or Heart Beat Signal) connection, please select **Cấp BigPond**. And you should enter the following parameters (Figure 4-9):

The screenshot shows the WAN configuration interface for a BigPond Cable connection. The 'WAN' header is at the top. The 'Dạng kết nối WAN:' dropdown is set to 'Cấp BigPond'. Below it are input fields for 'Tên đăng nhập:' (username) and 'Mật mã:' (password). The 'Server Auth:' field contains 'sm-server'. The 'Kích thước MTU (đơn vị byte):' is set to 1500. Under 'Connection Mode:', the 'Kết nối theo yêu cầu' radio button is selected, with a 'Thời gian nghỉ tối đa:' of 15 minutes. Other options include 'Kết nối tự động' and 'Kết nối thủ công'. At the bottom, there are buttons for 'Kết nối', 'Ngắt kết nối', 'Đã ngắt kết nối', and 'Lưu'.

Figure 4-9 WAN – BigPond Cable

- **Tên đăng nhập/Mật mã** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Server Auth** - Enter the authenticating server IP address or host name.

- **Domain Auth** - Type in the domain suffix server name based on your location.

e.g.

NSW / ACT - **nsw.bigpond.net.au**

VIC / TAS / WA / SA / NT - **vic.bigpond.net.au**

QLD - **qld.bigpond.net.au**

- **Kích thước MTU (đơn vị byte)** - The normal **MTU** (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default **Kích thước MTU (đơn vị byte)** unless required by your ISP.
- **Kết nối theo yêu cầu** - In this mode, the Internet connection can be terminated automatically after a specified inactivity period (**Thời gian nghỉ tối đa**) and be re-established when you attempt to access the Internet again. If you want your Internet connection keeps active all the time, please enter "0" in the **Thời gian nghỉ tối đa** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.
- **Kết nối tự động** - The connection can be re-established automatically when it was down.
- **Kết nối thủ công** - You can click the **Kết nối/Ngắt kết nối** button to connect/disconnect immediately. This mode also supports the **Thời gian nghỉ tối đa** function as **Kết nối theo yêu cầu** mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again.

Click the **Kết nối** button to connect immediately. Click the **Ngắt kết nối** button to disconnect immediately.

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

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

5. If your ISP provides L2TP connection, please select **L2TP/Russia L2TP** option. And you should enter the following parameters (Figure 4-11):

WAN

Dạng kết nối WAN Connection: L2TP/Russia L2TP ▼

Tên đăng nhập: username

Mật mã: ●●●●●●

Kết nối
Ngắt kết nối
Đã ngắt kết nối!

IP Động IP Tĩnh

Địa chỉ IP/Tên Server:

Địa chỉ IP: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

DNS: 0.0.0.0 , 0.0.0.0

Địa chỉ IP Internet: 0.0.0.0

DNS Internet: 0.0.0.0 , 0.0.0.0

Kích thước MTU (bằng byte): 1460 (Giá trị mặc định là 1460, vui lòng không thay đổi trừ trường hợp cần thiết.)

Chế độ kết nối:

Kết nối theo yêu cầu
 Kết nối tự động
 Kết nối thủ công

Thời gian nghỉ tối đa: 15 phút (0 có nghĩa là luôn kích hoạt.)

Lưu

Figure 4-10 WAN –L2TP

- **Tên đăng nhập/Mật mã** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **IP Động/ IP Tĩnh** - Choose either as you are given by your ISP. Click the **Kết nối** button to connect immediately. Click the **Ngắt kết nối** button to disconnect immediately.
- **Kết nối theo yêu cầu** - You can configure the Router to disconnect from your Internet connection after a specified period of inactivity (**Thời gian nghỉ tối đa**). If your Internet connection has been terminated due to inactivity, **Kết nối theo yêu cầu** enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Kết nối theo yêu cầu**, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Thời gian nghỉ tối đa** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- **Kết nối tự động** - Connect automatically after the Router is disconnected. To use this option, click the radio button.
- **Kết nối thủ công** - You can configure the Router to make it connect or disconnect manually.

After a specified period of inactivity (**Thời gian nghỉ tối đa**), the Router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Thời gian nghỉ tối đa** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to **Thời gian nghỉ tối đa**, since some applications is visiting the Internet continually in the background.

- If your ISP provides PPTP connection, please select **PPTP/Russia PPTP** option. And you should enter the following parameters (Figure 4-12):

The screenshot shows the WAN configuration interface for a PPTP/Russia PPTP connection. The 'WAN' title is at the top left. The configuration includes:

- Dạng kết nối WAN:** PPTP/Russia PPTP (dropdown menu)
- Tên đăng nhập:** username (text input)
- Mật mã:** masked with dots (password input)
- Buttons:** 'Kết nối' (Connect), 'Ngắt kết nối' (Disconnect), and 'Đã ngắt kết nối!' (Already disconnected!).
- IP Type:** Radio buttons for 'IP Động' (selected) and 'IP Tĩnh' (Static).
- Địa chỉ IP/Tên Server:** (text input)
- Địa chỉ IP:** 0.0.0.0
- Subnet Mask:** 0.0.0.0
- Gateway:** 0.0.0.0
- DNS:** 0.0.0.0, 0.0.0.0
- Địa chỉ IP Internet:** 0.0.0.0
- DNS Internet:** 0.0.0.0, 0.0.0.0
- Kích thước MTU (đơn vị byte):** 1420 (with a note: '(Giá trị mặc định là 1420, vui lòng không thay đổi trừ trường hợp cần thiết.)')
- Chế độ kết nối:** Radio buttons for 'Kết nối theo yêu cầu' (selected), 'Kết nối tự động', and 'Kết nối thủ công'.
- Thời gian nghỉ tối đa:** 15 phút (0 có nghĩa là luôn ở trạng thái kích hoạt.)
- Save Button:** 'Lưu' (Save)

Figure 4-11 WAN –PPTP

- **Tên đăng nhập/Mật mã** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **IP Động/ IP Tĩnh**- Choose either as you are given by your ISP and enter the ISP's IP address or the domain name.

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

Click the **Kết nối** button to connect immediately. Click the **Ngắt kết nối** button to disconnect immediately.

- **Kết nối theo yêu cầu** - You can configure the Router to disconnect from your Internet connection after a specified period of inactivity (**Thời gian nghỉ tối đa**). If your Internet connection has been terminated due to inactivity, **Kết nối theo yêu cầu** enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Kết nối theo yêu cầu**, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Thời gian nghỉ tối đa** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- **Kết nối tự động** - Connect automatically after the Router is disconnected. To use this option, click the radio button.
- **Kết nối thủ công** - You can configure the Router to make it connect or disconnect manually. After a specified period of inactivity (**Thời gian nghỉ tối đa**), the Router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Thời gian nghỉ tối đa** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

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

 **Note:**

If you don't know how to choose the appropriate connection type, click the **Phát hiện** button to allow the Router to automatically search your Internet connection for servers and protocols. The connection type will be reported when an active Internet service is successfully detected by the Router. This report is for your reference only. To make sure the connection type your ISP provides, please refer to the ISP. The various types of Internet connections that the Router can detect are as follows:

- **PPPoE** - Connections which use PPPoE that requires a user name and password.
- **IP Động** - Connections which use dynamic IP address assignment.
- **IP Tĩnh** - Connections which use static IP address assignment.

The Router can not detect PPTP/L2TP/BigPond connections with your ISP. If your ISP uses one of these protocols, then you must configure your connection manually.

4.5.2 LAN

Choose menu “**Mạng**→**LAN**”, and then you can configure the IP parameters of the LAN on the screen as below.

Figure 4-12 LAN

- **Địa chỉ MAC** - The physical address of the Router, as seen from the LAN. The value can't be changed.
- **Địa chỉ IP** - Enter the IP address of your Router or reset it in dotted-decimal notation (factory default: 192.168.0.1).
- **Subnet Mask** - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

 **Note:**

1. If you change the IP Address of LAN, you must use the new IP Address to login the Router.
2. If the new LAN IP Address you set is not in the same subnet, the IP Address pool of the DHCP server will change accordingly at the same time, while the Virtual Server and DMZ Host will not take effect until they are re-configured.

4.5.3 Bản sao MAC

Choose menu “**Mạng**→**Bản sao MAC**”, and then you can configure the MAC address of the WAN on the screen below, Figure 4-13:

Figure 4-13 MAC Address Clone

Some ISPs require that you register the MAC Address of your adapter. Changes are rarely needed here.

- **Địa chỉ MAC WAN** - This field displays the current MAC address of the WAN port. If your ISP requires you to register the MAC address, please enter the correct MAC address into this field in XX-XX-XX-XX-XX-XX format(X is any hexadecimal digit).

- **Địa chỉ MAC máy tính của bạn** - This field displays the MAC address of the PC that is managing the Router. If the MAC address is required, you can click the **Sao địa chỉ MAC đến** button and this MAC address will fill in the **Địa chỉ MAC WAN** field.

Click **Khôi phục địa chỉ MAC gốc** to restore the MAC address of WAN port to the factory default value.

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

 **Note:**

Only the PC on your LAN can use the **Bản sao MAC** function.

4.6 Không dây



Figure 4-14 Wireless menu

There are five submenus under the Wireless menu (shown in Figure 4-14): **Cài đặt không dây**, **Bảo mật không dây**, **Lọc địa chỉ MAC không dây**, **Không dây nâng cao** and **Thống kê không dây**. Click any of them, and you will be able to configure the corresponding function.

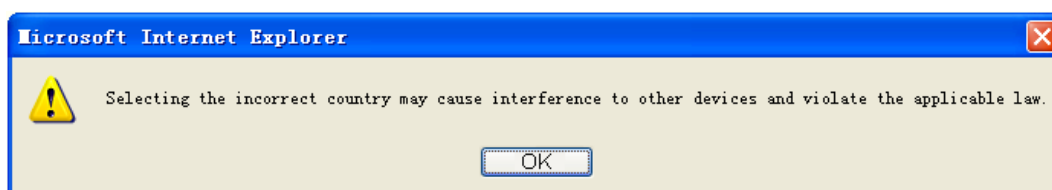
4.6.1 Cài đặt không dây

Choose menu “**Không dây**→**Cài đặt không dây**”, and then you can configure the basic settings for the wireless network on this page.

Figure 4-15 Wireless Settings

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

When you select your local region from the drop-down list, click the **Lưu** button, and then the Note Dialog will appear. Click **OK**.



Note Dialog

Note:

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

- **Kênh** - This field determines which operating frequency will be used. The default channel is set to **Tự động**, so the AP will choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

- **Chế độ**- Select the desired mode. The default setting is 11bgn mixed.

Chỉ 11b - Select if all of your wireless clients are 802.11b.

Chỉ 11g - Select if all of your wireless clients are 802.11g.

Chỉ 11n - Select only if all of your wireless clients are 802.11n.

Hỗn hợp 11bg - Select if you are using both 802.11b and 802.11g wireless clients.

Hỗn hợp 11bgn - Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.

Select the desired wireless mode. When 802.11g mode is selected, only 802.11g wireless stations can connect to the Router. When 802.11n mode is selected, only 802.11n wireless stations can connect to the AP. It is strongly recommended that you set the Mode to **802.11b&g&n**, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the Router.

- **Độ rộng kênh** - Select any channel width from the drop-down list. The default setting is automatic, which can automatically adjust the channel width for your clients.

 **Note:**

If **Chỉ 11b**, **Chỉ 11g**, or **Hỗn hợp 11bg** is selected in the **Chế độ** field, the **Độ rộng kênh** selecting field will turn grey and the value will become 20M, which is unable to be changed.

- **Tỷ lệ Tx tối đa** - You can limit the maximum tx rate of the Router through this field.
- **Kích hoạt Router không dây** - The wireless radio of this Router can be enabled or disabled to allow wireless stations access.
- **Kích hoạt Broadcast SSID** - When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. If you select the **Kích hoạt Broadcast SSID** checkbox, the Wireless Router will broadcast its name (SSID) on the air.
- **Kích hoạt WDS Bridging** - Check this box to enable WDS. With this function, the Router can bridge two or more WLANs. If this checkbox is selected, you will have to set the following parameters as shown below. Make sure the following settings are correct.

	<input checked="" type="checkbox"/> Kích hoạt WDS Bridging
SSID(được nối):	<input type="text"/>
BSSID(được nối):	<input type="text"/> Ví dụ:00-1D-0F-11-22-33
	<input type="button" value="Khảo sát"/>
Dạng mã:	<input type="text" value="Không"/> ▾
Chỉ số WEP:	<input type="text" value="1"/> ▾
Dạng xác thực:	<input type="text" value="mở"/> ▾
Mật mã:	<input type="text"/>

- **SSID (được nối)** - The SSID of the AP your Router is going to connect to as a client. You can also use the search function to select the SSID to join.
- **BSSID (được nối)** - The BSSID of the AP your Router is going to connect to as a client. You can also use the search function to select the BSSID to join.

- **Khảo sát** - Click this button, you can search the AP which runs in the current channel.
- **Dạng mã** - This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type
- **Chỉ số WEP** - This option should be chosen if the key type is WEP (ASCII) or WEP (HEX).It indicates the index of the WEP key.
- **Dạng xác thực** - This option should be chosen if the key type is WEP (ASCII) or WEP (HEX).It indicates the authorization type of the Root AP.
- **Mật mã** - If the AP your Router is going to connect needs password, you need to fill the password in this blank.

4.6.2 Bảo mật không dây

Choose menu “**Không dây**→**Bảo mật không dây**”, and then you can configure the security settings of your wireless network.

There are five wireless security modes supported by the Router: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2), WPA2-PSK (Pre-Shared Key) and WPA-PSK (Pre-Shared Key).

Bảo mật không dây

Vô hiệu hóa bảo mật

WEP

Dạng:

Dạng mã WEP:

Chọn mã	Mã WEP (Mật mã)	Dạng mã
Mã 1: <input type="text"/>	<input type="text"/>	<input type="text" value="Đã vô hiệu hóa"/>
Mã 2: <input type="text"/>	<input type="text"/>	<input type="text" value="Đã vô hiệu hóa"/>
Mã 3: <input type="text"/>	<input type="text"/>	<input type="text" value="Đã vô hiệu hóa"/>
Mã 4: <input type="text"/>	<input type="text"/>	<input type="text" value="Đã vô hiệu hóa"/>

WPA/WPA2 - Doanh nghiệp

Phiên bản:

Mã hóa:

IP Server Radius:

Cổng Radius: (1-65535, 0 thay cho cổng 1812 mặc định)

Mật mã Radius:

Thời gian cập nhật mã nhóm: (tính bằng giây, giá trị nhỏ nhất là 30, 0 có nghĩa là không cập nhật)

WPA/WPA2 - Cá nhân

Phiên bản:

Mã hóa:

Mật mã:

(Bạn có thể nhập ký tự ASCII với độ dài trong khoảng 8 đến 63 hoặc ký tự thập lục phân với độ dài trong khoảng 8 đến 64.)

Thời gian cập nhật mã nhóm: (tính bằng giây, giá trị nhỏ nhất là 30, 0 có nghĩa là không cập nhật)

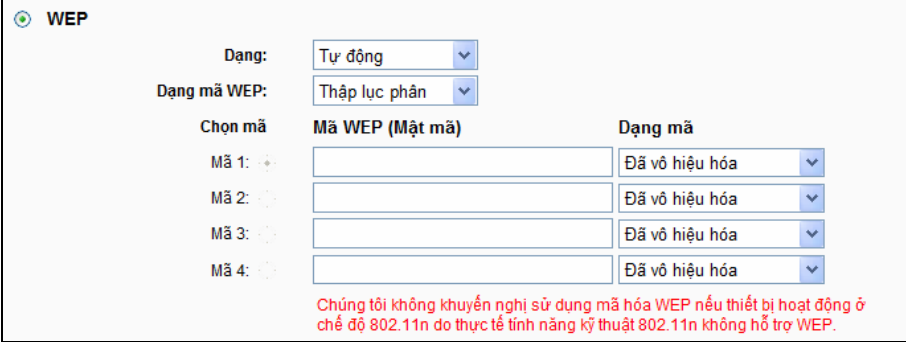
Thay đổi cấu hình không dây sẽ không có hiệu lực cho đến khi Router khởi động lại, vui lòng [bấm vào đây](#) để khởi động lại.

Figure 4-16

- **Vô hiệu hóa bảo mật** - If you do not want to use wireless security, select this check box, but

it's strongly recommended to choose one of the following modes to enable security.

- **WEP** - It is based on the IEEE 802.11 standard. If you select this check box, you will find a notice in red as show in Figure 4-17.



WEP

Dạng: Tự động

Dạng mã WEP: Thập lục phân

Chọn mã	Mã WEP (Mật mã)	Dạng mã
Mã 1: <input type="radio"/>	<input type="text"/>	Đã vô hiệu hóa
Mã 2: <input type="radio"/>	<input type="text"/>	Đã vô hiệu hóa
Mã 3: <input type="radio"/>	<input type="text"/>	Đã vô hiệu hóa
Mã 4: <input type="radio"/>	<input type="text"/>	Đã vô hiệu hóa

Chúng tôi không khuyến nghị sử dụng mã hóa WEP nếu thiết bị hoạt động ở chế độ 802.11n do thực tế tính năng kỹ thuật 802.11n không hỗ trợ WEP.

Figure 4-17

- **Dạng** - you can choose the type for the WEP security on the drop-down list. The default setting is **Tự động**, which can select **Hệ thống mở** or **Mật mã chia sẻ** authentication type automatically based on the wireless station's capability and request.
- **Dạng mã WEP** – **Thập lục phân** and **ASCII** formats are provided. **Thập lục phân** format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. **ASCII** format stands for any combination of keyboard characters in the specified length.
- **Mã WEP**- Select which of the four keys will be used and enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your network.
- **Dạng mã** - You can select the WEP key length (64-bit, or 128-bit, or 152-bit.) for encryption. "Đã vô hiệu hóa" means this WEP key entry is invalid.

64-bit - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 5 ASCII characters.

128-bit - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 13 ASCII characters.

152-bit - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 16 ASCII characters.

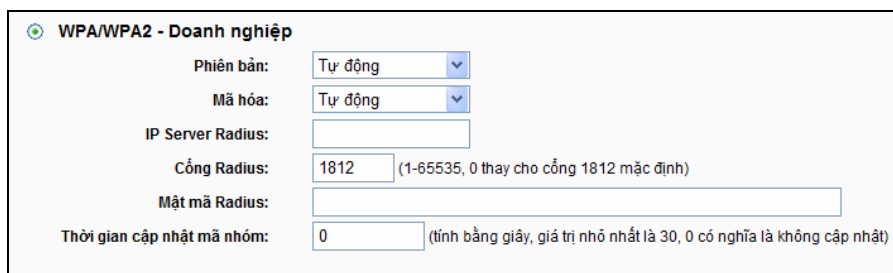
 **Note:**

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

- **WPA /WPA2** - It's based on Radius Server.
- **Phiên bản** - you can choose the version of the WPA security on the drop-down list. The default setting is **Tự động**, which can select **WPA** (Wi-Fi Protected Access) or **WPA2** (WPA version 2) automatically based on the wireless station's capability and request.
- **Mã hóa** - You can select either **Tự động**, or **TKIP** or **AES**.

 **Note:**

If you check the **WPA/WPA2** radio button and choose TKIP encryption, you will find a notice in red as shown in Figure 4-18



WPA/WPA2 - Doanh nghiệp

Phiên bản:

Mã hóa:

IP Server Radius:

Cổng Radius: (1-65535, 0 thay cho cổng 1812 mặc định)

Mật mã Radius:

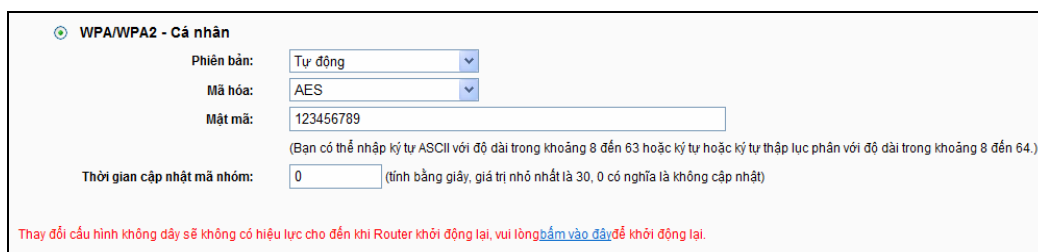
Thời gian cập nhật mã nhóm: (tính bằng giây, giá trị nhỏ nhất là 30, 0 có nghĩa là không cập nhật)

Figure 4-18

- **IP Server Radius** - Enter the IP address of the Radius Server.
 - **Cổng Radius** - Enter the port that radius service used.
 - **Mật mã Radius** - Enter the password for the Radius Server.
 - **Thời gian cập nhật mã nhóm**- Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.
- **WPA-PSK/WPA2-PSK** - It's the WPA/WPA2 authentication type based on pre-shared passphrase.
- **Phiên bản** - you can choose the version of the WPA-PSK security on the drop-down list. The default setting is **Tự động**, which can select **WPA-PSK** (Pre-shared key of WPA) or **WPA2-PSK** (Pre-shared key of WPA) automatically based on the wireless station's capability and request.
 - **Mã hóa** - When **WPA-PSK** or **WPA** is set as the Authentication Type, you can select either **Tự động**, or **TKIP** or **AES** as Encryption.

 **Note:**

If you check the **WPA-PSK/WPA2-PSK** radio button and choose TKIP encryption, you will find a notice in red as shown in Figure 4-19.



WPA/WPA2 - Cá nhân

Phiên bản:

Mã hóa:

Mật mã:

(Bạn có thể nhập ký tự ASCII với độ dài trong khoảng 8 đến 63 hoặc ký tự thập lục phân với độ dài trong khoảng 8 đến 64.)

Thời gian cập nhật mã nhóm: (tính bằng giây, giá trị nhỏ nhất là 30, 0 có nghĩa là không cập nhật)

Thay đổi cấu hình không dây sẽ không có hiệu lực cho đến khi Router khởi động lại, vui lòng **bấm vào đây** để khởi động lại.

Figure 4-19

- **Mật mã** - You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters.

- **Thời gian cập nhật mã nhóm**- Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

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

4.6.3 Lọc địa chỉ MAC không dây

Choose menu “**Không dây**→**Lọc địa chỉ MAC**”, and then you can control the wireless access by configuring the Wireless MAC Address Filtering function, shown in Figure 4-20.

Figure 4-20 Wireless MAC address Filtering

To filter wireless users by MAC Address, click **Kích hoạt**. The default setting is **Vô hiệu hóa**.

- **Địa chỉ MAC**- The wireless station's MAC address that you want to filter.
- **Trạng thái** - The status of this entry either **Đã kích hoạt** or **Đã vô hiệu hóa**.
- **Mô tả** - A simple description of the wireless station.

To Add a Wireless MAC Address filtering entry, click the **Thêm mới...** button. The "**Thêm hoặc tùy chỉnh một mục lọc địa chỉ MAC không dây**" page will appear as shown in Figure 4-21:

Figure 4-21 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 **Địa chỉ MAC** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0A-EB-00-07-8A.

2. Enter a simple description of the wireless station in the **Mô tả** field. For example: Wireless station A.
3. **Trạng thái** - Select **Đã kích hoạt** or **Đã vô hiệu hóa** for this entry on the **Trạng thái** drop-down list.
4. Click the **Lưu** button to save this entry.

To modify or delete an existing entry:

1. Click the **Tùy chỉnh** in the entry you want to modify. If you want to delete the entry, click the **Xóa**.
2. Modify the information.
3. Click the **Lưu** button.

Click the **Kích hoạt tất cả** button to make all entries enabled.

Click the **Vô hiệu hóa tất cả** button to make all entries disabled.

Click the **Xóa tất cả** button to delete all entries.

Click the **Tiếp** button to go to the next page

Click the **Trước** button to return to the previous page.

For example: If you desire that the wireless station A with MAC address 00-0A-EB-00-07-8A and the wireless station B with MAC address 00-0A-EB-00-23-11 are able to access the Router, but all the other wireless stations cannot access the Router, you can configure the **Lọc địa chỉ MAC không dây** list by following these steps:

1. Click the **Kích hoạt** button to enable this function.
2. Select the radio button: **Cấm các trạm được xác định bởi các mục được kích hoạt trong danh sách truy cập** for **Điều luật lọc**.
3. Delete all or disable all entries if there are any entries already.
4. Click the **Thêm mới...** button and enter the MAC address 00-0A-EB-00-07-8A /00-0A-EB-00-23-11 in the **Địa chỉ MAC** field, then enter wireless station A/B in the **Mô tả** field, while select **Đã kích hoạt** in the **Trạng thái** drop-down list. Finally, click the **Lưu** and the **Quay lại** button.

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

Điều luật lọc

Cấm các trạm được xác định bởi các mục được kích hoạt trong danh sách truy cập.

Cho phép các trạm được xác định bởi các mục được kích hoạt trong danh sách truy cập.

STT	Địa chỉ MAC	Trạng thái	Mô tả	Tùy chỉnh
1	00-0A-EB-00-07-8A	Đã kích hoạt		Tùy chỉnh Xóa
2	00-0A-EB-00-23-11	Đã kích hoạt		Tùy chỉnh Xóa

4.6.4 Không dây nâng cao

Choose menu “**Không dây** → **Không dây nâng cao**”, and then you can configure the advanced settings of your wireless network.

Không dây nâng cao

Khoảng thời gian Beacon : (40-1000)

Ngưỡng RTS: (256-2346)

Ngưỡng phân mảnh: (256-2346)

Khoảng thời gian DTIM: (1-255)

Kích hoạt WMM

Kích hoạt Short GI

Kích hoạt chức năng cô lập điểm truy cập

Figure 4-22 Wireless Advanced

- **Công suất truyền tải** - Here you can specify the transmit power of Router. You can select High, Middle or Low which you would like. High is the default setting and is recommended.
- **Khoảng thời gian Beacon** - Enter a value between 20-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- **Ngưỡng RST** - Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Ngưỡng phân mảnh** - This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.
- **Khoảng thời gian DTIM** - This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the

next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.

- **Kích hoạt WMM - WMM** function can guarantee the packets with high- priority messages being transmitted preferentially. It is strongly recommended enabled.
- **Kích hoạt Short GI** - This function is recommended for it will increase the data capacity by reducing the guard interval time.
- **Kích hoạt chức năng cô lập điểm truy cập** - This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, check this box. AP Isolation is disabled by default.

 **Note:**

If you are not familiar with the setting items in this page, it's strongly recommended to keep the provided default values; otherwise it may result in lower wireless network performance.

4.6.5 Thống kê không dây

Choose menu “**Không dây**→**Thống kê không dây**”, and then you can see the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

Thống kê không dây	
Số lượng trạm không dây kết nối hiện tại:	0 <input type="button" value="Làm mới"/>
<input type="button" value="Trước"/> <input type="button" value="Tiếp"/>	

Figure 4-23 The Router attached wireless stations

- **Địa chỉ MAC** - The connected wireless station's MAC address
- **Trạng thái hiện tại** - The connected wireless station's running status, one of **STA-AUTH / STA-ASSOC / STA-JOINED / WPA / WPA-PSK / WPA2 / WPA2-PSK / AP-UP / AP-DOWN / Disconnected**
- **Gói tin đã nhận** - Packets received by the station
- **Gói tin đã gửi** - 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 **Làm mới** button.

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

 **Note:**

This page will be refreshed automatically every 5 seconds.

4.7 DHCP

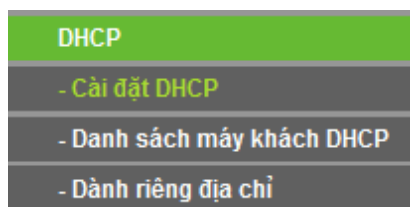


Figure 4-24 The DHCP menu

There are three submenus under the DHCP menu (shown in Figure 4-24): **Cài đặt DHCP**, **Danh sách máy khách DHCP** and **Dành riêng địa chỉ**. Click any of them, and you will be able to configure the corresponding function.

4.7.1 Cài đặt DHCP

Choose menu “**DHCP**→**Cài đặt DHCP**”, and then you can configure the DHCP Server on the page (shown in Figure 4-25). The Router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PC(s) that are connected to the Router on the LAN.

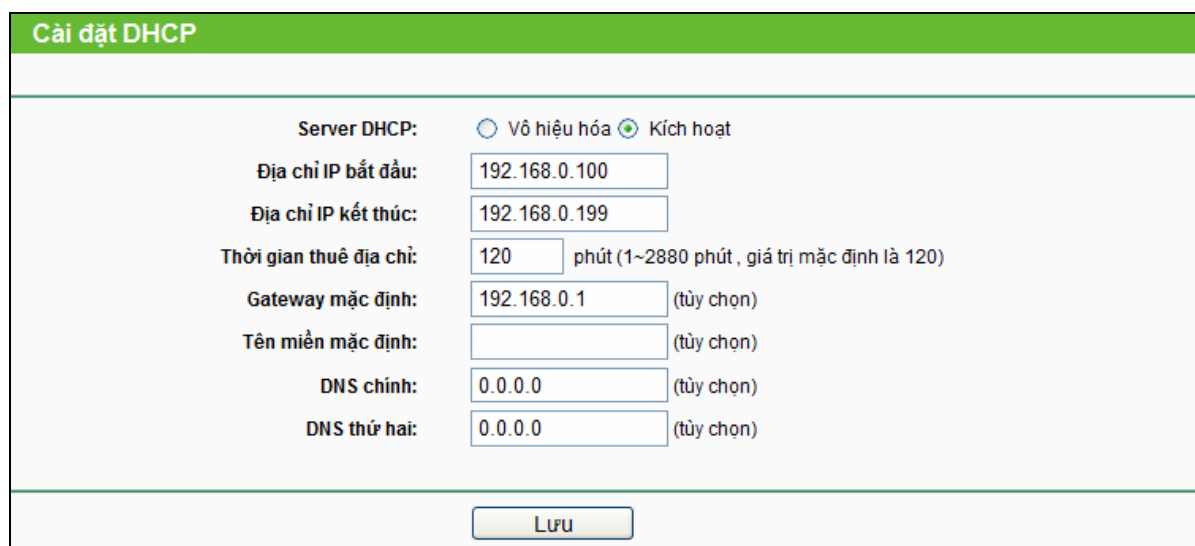


Figure 4-25 DHCP Settings

- **Server DHCP – Kích hoạt** or **Vô hiệu hóa** the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must configure the computer manually.
- **Địa chỉ IP bắt đầu** - Specify an IP address for the DHCP Server to start with when assigning

IP addresses. 192.168.0.100 is the default start address.

- **Địa chỉ IP kết thúc** - Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168.0.199 is the default end address.
- **Thời gian thuê địa chỉ** - The **Thời gian thuê địa chỉ** 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 and the user will be "leased" this dynamic IP Address. After the time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.
- **Gateway mặc định** - (Optional.) Suggest to input the IP address of the LAN port of the Router, default value is 192.168.0.1
- **Tên miền mặc định** - (Optional.) Input the domain name of your network.
- **DNS chính** - (Optional.) Input the DNS IP address provided by your ISP. Or consult your ISP.
- **DNS thứ hai** - (Optional.) Input the IP address of another DNS server if your ISP provides two DNS servers.

 **Note:**

To use the DHCP server function of the Router, you must configure all computers on the LAN as "Obtain an IP Address automatically" mode.

4.7.2 Danh sách máy khách DHCP

Choose menu "**DHCP→Danh sách máy khách DHCP**", and then you can view the information about the clients attached to the Router in the next screen (shown in Figure 4-26).

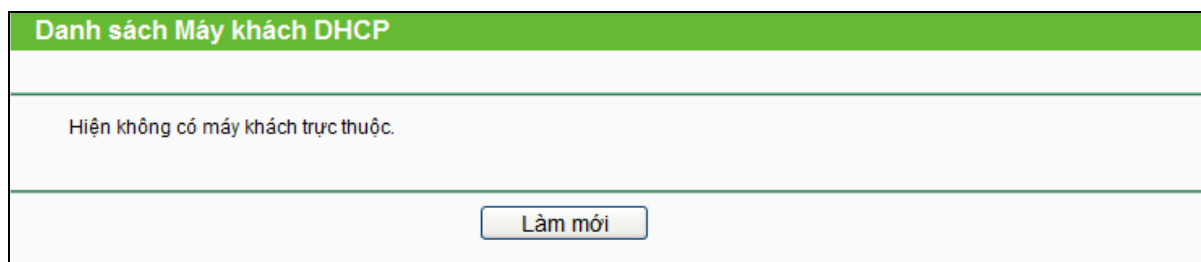


Figure 4-26 DHCP Clients List

- **STT** - The index of the DHCP Client.
- **Tên máy khách** - The name of the DHCP client.
- **Địa chỉ MAC** - The MAC address of the DHCP client.
- **IP được gán** - The IP address that the Router has allocated to the DHCP client.
- **Thời gian thuê** - The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP address will be automatically assigned to the user.

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

4.7.3 Dành riêng địa chỉ

Choose menu “**DHCP→Dành riêng địa chỉ**”, and then you can view and add a reserved address for clients via the next screen (shown in Figure 4-27). 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 the servers that require permanent IP settings.

Dành riêng địa chỉ				
STT	Địa chỉ MAC	Địa chỉ IP dành riêng	Trạng thái	Tùy chỉnh
1	40-61-86-C4-98-43	192.168.0.100	Đã kích hoạt	Tùy chỉnh Xóa

Figure 4-27 Address Reservation

- **Địa chỉ MAC** - The MAC address of the PC for which you want to reserve IP address.
- **Địa chỉ IP dành riêng** - The IP address of the Router reserved.
- **Trạng thái** - The status of this entry, either **Đã kích hoạt** or **Đã vô hiệu hóa**.

To Reserve IP addresses:

1. Click the **Thêm mới ...** button. (Pop-up Figure 4-28)
2. Enter the MAC address (in XX-XX-XX-XX-XX-XX format) and IP address of the computer you wish to add in dotted-decimal notation.
3. Click the **Lưu** button when finished.

Thêm hoặc Tùy chỉnh một Mục Dành riêng địa chỉ	
Địa chỉ MAC:	<input type="text"/>
Địa chỉ IP dành riêng:	<input type="text"/>
Trạng thái:	Đã kích hoạt <input type="button" value="v"/>

Figure 4-28 Add or Modify an Address Reservation Entry

To modify or delete an existing entry:

1. Click the **Tùy chỉnh** in the entry you want to modify. If you want to delete the entry, click the **Xóa**.
2. Modify the information.

3. Click the **Lưu** button.

Click the **Kích hoạt tất cả/ Vô hiệu hóa tất cả** button to make all entries enabled/disabled

Click the **Xóa tất cả** button to delete all entries

Click the **Tiếp** button to go to the next page and Click the **Trước** button to return to the previous page.

4.8 Đang chuyển tiếp



Figure 4-29 The Forwarding menu

There are four submenus under the Forwarding menu (shown in Figure 4-29): **Server ảo**, **Cổng kích hoạt**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function.

4.8.1 Server ảo

Choose menu "**Đang chuyển tiếp**→**Servers ảo**", and then you can view and add virtual servers in the next screen (shown in Figure 4-30). Virtual servers can be used for setting up public services on your LAN. 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 a static or reserved IP address because its IP address may change when using the DHCP function.

Server ảo							
STT	Cổng dịch vụ	Cổng trong	Địa chỉ IP	Giao thức	Trạng thái	Tùy chỉnh	
1	80	80	192.168.0.169	Tất cả	Đã kích hoạt	Tùy chỉnh Xóa	
<div style="display: flex; justify-content: space-around; margin-top: 10px;"> Thêm mới... Kích hoạt tất cả Vô hiệu hóa tất cả Xóa tất cả </div>							
Trước Tiếp							

Figure 4-30 Virtual Servers

- **Cổng dịch vụ** - The numbers of External Service Ports. You can enter a service port or a range of service ports (the format is XXX – YYY; XXX is the Start port and YYY is the End port).
- **Cổng trong** - The Internal Service Port number of the PC running the service application. You can leave it blank if the **Cổng trong** is the same as the **Cổng dịch vụ**, or enter a

specific port number when **Cổng kích hoạt** is a single one.

- **Địa chỉ IP** - The IP address of the PC running the service application.
- **Giao thức** - The protocol used for this application, either **TCP**, **UDP**, or **Tất cả** (all protocols supported by the Router).
- **Trạng thái** - The status of this entry, "Đã kích hoạt" means the virtual server entry is enabled.
- **Cổng dịch vụ phổ biến** - Some common services already exist in the drop-down list.
- **Tùy chỉnh** - To modify or delete an existing entry.

To setup a virtual server entry:

1. Click the **Thêm mới...** button. (pop-up Figure 4-31)
2. Select the service you want to use from the **Cổng dịch vụ phổ biến** list. If the **Cổng dịch vụ phổ biến** menu does not list the service that you want to use, enter the number of the service port or service port range in the **Cổng dịch vụ** field.
3. Enter the IP address of the computer running the service application in the **Địa chỉ IP** field.
4. Select the protocol used for this application in the **Giao thức** drop-down list, either **TCP**, **UDP**, or **Tất cả**.
5. Select the **Đã kích hoạt** option in the **Trạng thái** drop-down list.
6. Click the **Lưu** button.

The screenshot shows a web interface for adding or modifying a virtual server entry. The title bar reads "Thêm hoặc Tùy chỉnh một mục Server ảo". The form includes the following fields:

- Cổng dịch vụ:** Input field containing "80" with a hint "(XX-XX hoặc XX)".
- Cổng trong:** Input field containing "80" with a hint "(XX, Chỉ hợp lệ cho cổng dịch vụ đơn hoặc để trống)".
- Địa chỉ IP:** Input field containing "192.168.0.169".
- Giao thức:** Dropdown menu set to "Tất cả".
- Trạng thái:** Dropdown menu set to "Đã kích hoạt".
- Cổng dịch vụ phổ biến:** Dropdown menu set to "--Chọn một--".

At the bottom of the form are two buttons: "Lưu" (Save) and "Quay lại" (Back).

Figure 4-31 Add or Modify a Virtual Server Entry

Note:

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

To modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Tùy chỉnh** or **Xóa** as desired on the **Tùy chỉnh** column.

Click the **Kích hoạt tất cả/Vô hiệu hóa tất cả** button to make all entries enabled/ disabled.

Click the **Xóa tất cả** button to delete all entries.

Click the **Tiếp** button to go to the next page and click the **Trước** button to return to the previous page.

 **Note:**

If you set the service port of the virtual server as 80, you must set the Web management port on **Công cụ hệ thống → Quản lý từ xa** page to be any other value except 80 such as 8080. Otherwise there will be a conflict to disable the virtual server.

4.8.2 Cổng kích hoạt

Choose menu “**Đang chuyển tiếp → Cổng kích hoạt**”, you can view and add port triggering in the next screen (shown in Figure 4-32). Some applications require multiple connections, like Internet games, video conferencing, Internet telephoning and so on. Port Triggering is used for some of these applications that cannot work with a pure NAT Router.

Cổng kích hoạt						
STT	Cổng kích hoạt	Giao thức kích hoạt	Cổng vào	Giao thức vào	Trạng thái	Tùy chỉnh
1	554	Tất cả	8970-8999	Tất cả	Đã kích hoạt	Tùy chỉnh Xóa

Figure 4-32 Port Triggering

To add a new rule, follow the steps below.

1. Click the **Thêm mới...** button, the next screen will pop-up as shown in Figure 4-33.
2. Select a common application from the **Ứng dụng phổ biến** drop-down list, then the **Cổng kích hoạt** field and the **Cổng vào** field will be automatically filled. If the **Ứng dụng phổ biến** do not have the application you need, enter the **Cổng kích hoạt** and the **Cổng vào** manually.
3. Select the protocol used for Trigger Port from the **Giao thức kích hoạt** drop-down list, either **TCP**, **UDP**, or **Tất cả**.
4. Select the protocol used for Incoming Ports from the **Giao thức vào** drop-down list, either **TCP** or **UDP**, or **Tất cả**.
5. Select **Kích hoạt** in **Trạng thái** field.
6. Click the **Lưu** button to save the new rule.

Thêm hoặc Tùy chỉnh một mục cổng kích hoạt	
Cổng kích hoạt:	<input type="text"/>
Giao thức kích hoạt:	Tất cả ▾
Cổng vào:	<input type="text"/>
Giao thức vào:	Tất cả ▾
Trạng thái:	Đã kích hoạt ▾
Các ứng dụng phổ biến:	--Chọn một-- ▾
<input type="button" value="Lưu"/> <input type="button" value="Quay lại"/>	

Figure 4-33 Add or Modify a Triggering Entry

- **Cổng kích hoạt** - The port for outgoing traffic. An outgoing connection using this port will trigger this rule.
- **Giao thức kích hoạt** - The protocol used for Trigger Ports, either **TCP**, **UDP**, or **Tất cả** (all protocols supported by the Router).
- **Cổng vào** - 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 which triggered this rule. You can input at most 5 groups of ports (or port sections). Every group of ports must be separated with ",", for example, 2000-2038, 2046, 2050-2051, 2085, 3010-3030.
- **Giao thức vào** - The protocol used for **Cổng vào**, either **TCP**, **UDP**, or **Tất cả** (all protocols supported by the Router).
- **Trạng thái** - The status of this entry, Enabled means the Port Triggering entry is enabled.
- **Tùy chỉnh** - To modify or delete an existing entry.
- **Ứng dụng phổ biến** - Some popular applications already listed in the drop-down list of **Giao thức vào**.

To modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Tùy chỉnh** or **Xóa** as desired on the **Tùy chỉnh** column.

Click the **Kích hoạt tất cả** button to make all entries enabled.

Click the **Vô hiệu hóa tất cả** button to make all entries disabled.

Click the **Xóa tất cả** button to delete all entries

Once the Router is configured, the operation is as follows:

1. A local host makes an outgoing connection to an external host using a destination port number defined in the **Cổng kích hoạt** field.
2. The Router records this connection, opens the incoming port or ports associated with this

entry in the **Cổng kích hoạt** table, and associates them with the local host.

- When necessary, the external host will be able to connect to the local host using one of the ports defined in the **Cổng vào** field.

 **Note:**

- When the trigger connection is released, the corresponding opened ports will be closed.
- Each rule can only be used by one host on the LAN at a time. The trigger connection of other hosts on the LAN will be refused.
- Cổng vào** ranges cannot overlap each other.

4.8.3 DMZ

Choose menu “**Đang chuyển tiếp→DMZ**”, and then you can view and configure DMZ host in the screen (shown in Figure 4-34).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. The Router forwards packets of all services to the DMZ host. 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 be changed when using the DHCP function.

DMZ	
Trạng thái DMZ hiện tại:	<input type="radio"/> Kích hoạt <input checked="" type="radio"/> Vô hiệu hóa
Địa chỉ IP máy chủ DMZ:	<input type="text" value="0.0.0.0"/>
<input type="button" value="Lưu"/>	

Figure 4-34 DMZ

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

- Click the **Kích hoạt** button.
- Enter the IP address of a local PC that is set to be DMZ host in the **Địa chỉ IP máy chủ DMZ** field.
- Click the **Lưu** button.

4.8.4 UPnP

Choose menu “**Đang chuyển tiếp→UPnP**”, and then you can view the information about **UPnP** in the screen (shown in Figure 4-35). 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.

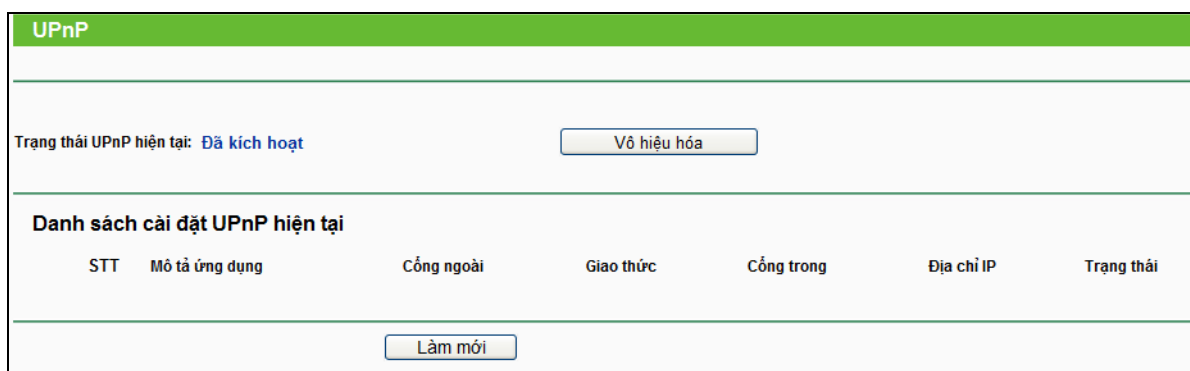


Figure 4-35 UPnP Setting

- **Trạng thái UPnP hiện tại** - UPnP can be enabled or disabled by clicking the **Kích hoạt** or **Vô hiệu hóa** button. This feature is enabled by default.
- **Danh sách cài đặt UPnP hiện tại** - This table displays the current UPnP information.
 - **Mô tả ứng dụng** - The description about the application which initiates the UPnP request.
 - **Cổng ngoài** - The port which the Router opened for the application.
 - **Giao thức** - The type of protocol which is opened.
 - **Cổng trong** - The port which the Router opened for local host.
 - **Địa chỉ IP** - The IP address of the local host which initiates the UPnP request.
 - **Trạng thái** - Either Enabled or Disabled. "Enabled" means that the port is still active; otherwise, the port is inactive.

Click the **Kích hoạt** button to enable UPnP.

Click the **Vô hiệu hóa** button to disable UPnP.

Click the **Làm mới** button to update the Current UPnP Settings List.

4.9 Bảo mật

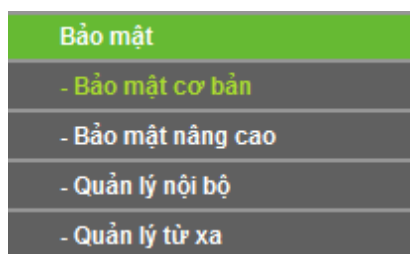


Figure 4-36 The Security menu

There are four submenus under the Security menu as shown in Figure 4-36: **Bảo mật cơ bản**, **Bảo mật nâng cao**, **Quản lý nội bộ** and **Quản lý từ xa**. Click any of them, and you will be able to configure the corresponding function.

4.9.1 Bảo mật cơ bản

Choose menu “**Bảo mật** → **Bảo mật cơ bản**”, and then you can configure the basic security in the screen as shown in Figure 4-37.

The screenshot shows the 'Bảo mật cơ bản' (Basic Security) configuration page. It is organized into three main sections, each with a title and several options:

- Tường lửa (Firewall):**
 - Tường lửa SPI: Kích hoạt Vô hiệu hóa
- VPN (Mạng riêng ảo):**
 - Truyền qua PPTP: Kích hoạt Vô hiệu hóa
 - Truyền qua L2TP: Kích hoạt Vô hiệu hóa
 - Truyền qua IPSec: Kích hoạt Vô hiệu hóa
- ALG:**
 - FTP ALG: Kích hoạt Vô hiệu hóa
 - TFTP ALG: Kích hoạt Vô hiệu hóa
 - H323 ALG: Kích hoạt Vô hiệu hóa
 - RTSP ALG: Kích hoạt Vô hiệu hóa

At the bottom of the page, there is a button labeled 'Lưu' (Save).

Figure 4-37 Basic Security

- **Tường lửa** - A firewall protects your network from the outside world. Here you can enable or disable the Router's firewall.
 - **Tường lửa SPI** - SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by factory default. If you want all the computers on the LAN exposed to the outside world, you can disable it.
- **VPN (Mạng riêng ảo)** - VPN Passthrough must be enabled if you want to allow VPN tunnels using VPN protocols to pass through the Router.
 - **Truyền qua PPTP** - Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, click **Kích hoạt**.
 - **Truyền qua L2TP** - Layer Two Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the Internet on the Layer Two level. To allow L2TP tunnels to pass through the Router, click **Kích hoạt**.
 - **Truyền qua IPSec** - Internet Protocol security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through

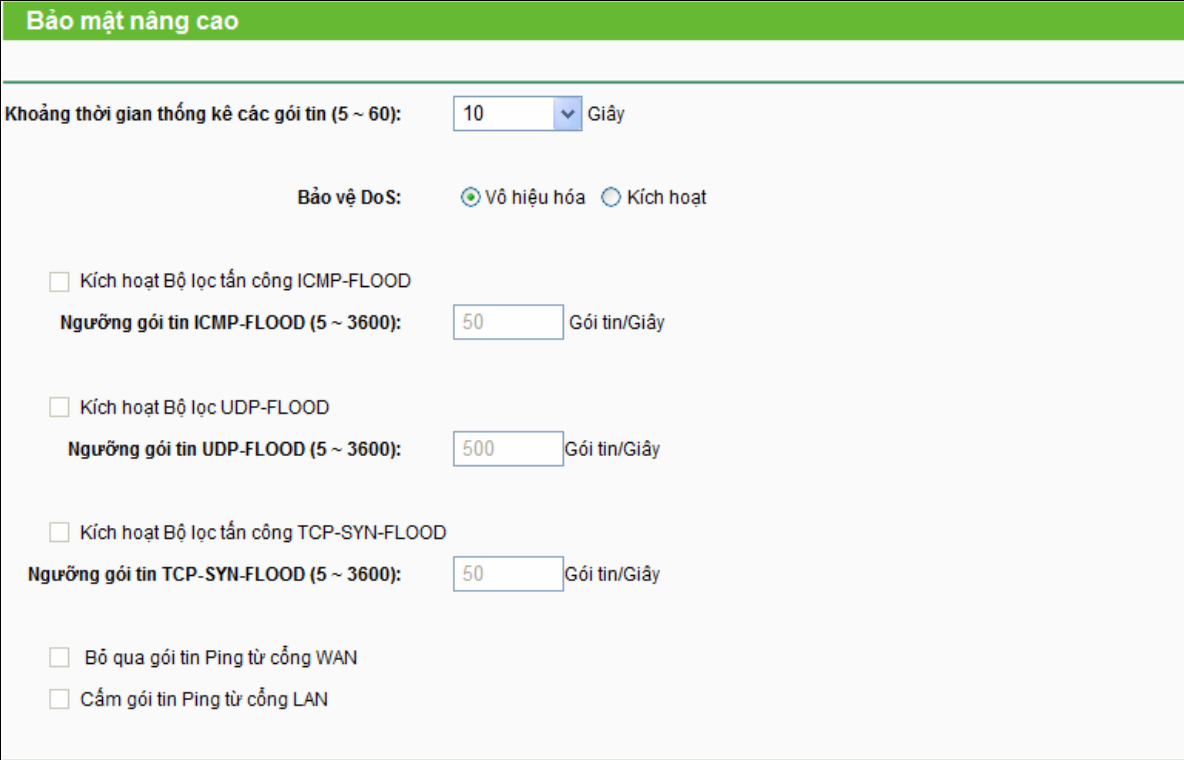
the use of cryptographic security services. To allow IPSec tunnels to pass through the Router, click **Kích hoạt**.

- **ALG** - It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.
 - **FTP ALG** - To allow FTP clients and servers to transfer data across NAT, click **Kích hoạt**.
 - **TFTP ALG** - To allow TFTP clients and servers to transfer data across NAT, click **Đã kích hoạt**.
 - **H323 ALG** - To allow Microsoft NetMeeting clients to communicate across NAT, click **Đã kích hoạt**.
 - **RTSP ALG** - To allow some media player clients to communicate with some streaming media servers across NAT, click **Kích hoạt**.

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

4.9.2 Bảo mật nâng cao

Choose menu "**Bảo mật** → **Bảo mật nâng cao**", and then you can protect the Router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood in the screen as shown in Figure 4-38.



Bảo mật nâng cao

Khoảng thời gian thống kê các gói tin (5 ~ 60): Giây

Bảo vệ DoS: Vô hiệu hóa Kích hoạt

Kích hoạt Bộ lọc tấn công ICMP-FLOOD
 Ngưỡng gói tin ICMP-FLOOD (5 ~ 3600): Gói tin/Giây

Kích hoạt Bộ lọc UDP-FLOOD
 Ngưỡng gói tin UDP-FLOOD (5 ~ 3600): Gói tin/Giây

Kích hoạt Bộ lọc tấn công TCP-SYN-FLOOD
 Ngưỡng gói tin TCP-SYN-FLOOD (5 ~ 3600): Gói tin/Giây

Bỏ qua gói tin Ping từ cổng WAN

Cấm gói tin Ping từ cổng LAN

Figure 4-38 Advanced Security

- **Khoảng thời gian thống kê các gói tin (5~60)** - The default value is 10. Select a value between 5 and 60 seconds from the drop-down list. The Packets Statistics Interval value indicates the time section of the packets statistics. The result of the statistics is used for analysis by SYN Flood, UDP Flood and ICMP-Flood.
- **Bảo vệ DoS** - Denial of Service protection. Check the Kích hoạt or Vô hiệu hóa button to enable or disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.

 **Note:**

Dos Protection will take effect only when the **Thống kê lưu lượng** in “**Công cụ hệ thống** → **Thống kê lưu lượng**” is enabled.

- **Kích hoạt Bộ lọc tấn công ICMP-FLOOD** - Enable or Disable the ICMP-FLOOD Attack Filtering.
- **Ngưỡng gói tin ICMP-FLOOD (5 ~ 3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the current ICMP-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.
- **Kích hoạt Bộ lọc UDP-FLOOD** - Enable or Disable the UDP-FLOOD Filtering.
- **Ngưỡng gói tin UDP-FLOOD (5 ~ 3600)** - The default value is 500. Enter a value between 5 ~ 3600. When the current UPD-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.
- **Kích hoạt Bộ lọc tấn công TCP-SYN-FLOOD** - Enable or Disable the TCP-SYN-FLOOD Attack Filtering.
- **Ngưỡng gói tin TCP-SYN-FLOOD (5 ~ 3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value, the Router will startup the blocking function immediately.
- **Bỏ qua gói tin Ping từ cổng WAN** - Enable or Disable Ignore Ping Packet From WAN Port. The default setting is disabled. If enabled, the ping packet from the Internet cannot access the Router.
- **Cấm gói tin Ping từ cổng LAN** - Enable or Disable Forbid Ping Packet From LAN Port. The default setting is disabled. If enabled, the ping packet from LAN cannot access the Router. This function can be used to defend against some viruses.

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

Click the **Danh sách máy chủ DoS bị chặn** button to display the DoS host table by blocking.

4.9.3 Quản lý nội bộ

Choose menu “**Bảo mật** → **Quản lý nội bộ**”, and then you can configure the management rule in the screen as shown in Figure 4-39. The management feature allows you to deny computers in LAN from accessing the Router.

Figure 4-39 Local Management

By default, the radio button “**Tất cả các máy tính trong mạng LAN được phép truy cập tiện ích web của Router**” is checked. If you want to allow PCs with specific MAC Addresses to access the Setup page of the Router's Web-Based Utility locally from inside the network, check the radio button “**Chỉ các máy tính được liệt kê có thể vào trang web tích hợp để thực hiện các thao tác Quản trị viên**”, and then enter each MAC Address in a separate field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). Only the PCs with MAC address listed can use the password to browse the built-in web pages to perform Administrator tasks while all the others will be blocked.

After click the **Thêm** button, your PC's MAC Address will be placed in the list above.

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

 **Note:**

If your PC is blocked but you want to access the Router again, use a pin to press and hold the **Reset Button** (hole) on the back panel for about 5 seconds to reset the Router's factory defaults on the Router's Web-Based Utility.

4.9.4 Quản lý từ xa

Choose menu “**Bảo mật** → **Quản lý từ xa**”, and then you can configure the Remote Management function in the screen as shown in Figure 4-40. This feature allows you to manage your Router from a remote location via the Internet.

Figure 4-40 Remote Management

- **Cổng quản lý web** - 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 port to a custom port by entering that number in the box provided. Choose a number between 1 and 65534 but do not use the number of any common service port.
- **Địa chỉ IP quản lý từ xa** - This is the current address you will use when accessing your Router from the Internet. This function is disabled when the IP address is set to the default value of 0.0.0.0. To enable this function change 0.0.0.0 to a valid IP address. If set to 255.255.255.255, then all the hosts can access the Router from internet.



Note:

1. To access the Router, you should 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 the port number used is 8080, please enter http://202.96.12.8:8080 in your browser. Later, you may be asked for the Router's password. After successfully entering the username and password, you will be able to access the Router's web-based utility.
2. Be sure to change the Router's default password to a very secure password.

4.10 Quyền kiểm soát của phụ huynh

Choose menu “**Kiểm soát của phụ huynh**”, and then you can configure the parental control in the screen as shown in Figure 4-41. The Parental Control function can be used to control the internet activities of the child, limit the child to access certain websites and restrict the time of surfing.

Cài đặt Quyền kiểm soát của phụ huynh

Các máy tính không phải của phụ huynh không được liệt kê sẽ không được truy cập Internet.

Quyền kiểm soát của phụ huynh: Vô hiệu hóa Kích hoạt

Địa chỉ MAC của máy tính phụ huynh:

Địa chỉ MAC máy tính của bạn:

STT	Địa chỉ MAC	Mô tả trang web	Thời gian biểu	Trạng thái	Tùy chỉnh
<input type="button" value="Thêm mới..."/>		<input type="button" value="Kích hoạt tất cả"/> <input type="button" value="Vô hiệu hóa tất cả"/>			
	<input type="button" value="Xóa tất cả"/>				

Số thứ tự hiện tại Trang

Figure 4-41 Parental Control Settings

To add a new entry, please follow the steps below.

1. Click the **Thêm mới...** button and the next screen will pop-up as shown in Figure 4-42.

Thêm hoặc Tùy chỉnh Mục kiểm soát của phụ huynh

Thời gian biểu dựa trên thời gian của Router. Thời gian có thể được cài đặt "Công cụ hệ thống" -> [Cài đặt thời gian](#).

Địa chỉ MAC của máy tính trẻ em:

Tất cả địa chỉ MAC trong mạng LAN hiện tại:

Mô tả trang web:

Tên miền được cho phép:

Thời gian hiệu lực:

Thời gian biểu có thể được cài đặt "Kiểm soát truy cập" -> [Thời gian biểu](#)

Trạng thái:

Figure 4-42 Add or Modify Parental Control Entry

- **Quyền kiểm soát của phụ huynh** - Check **Kích hoạt** if you want this function to take effect; otherwise, check **Vô hiệu hóa**.
 - **Địa chỉ MAC của máy tính phụ huynh** - In this field, enter the MAC address of the controlling PC, or you can make use of the **Sao chép lên trên** button below.
 - **Địa chỉ MAC máy tính của bạn** - This field displays the MAC address of the PC that is managing this Router. If the MAC Address of your adapter is registered, you can click the **Sao chép lên trên** button to fill this address to the MAC Address of Parental PC field above.
 - **Mô tả trang web** - Description of the allowed website for the PC controlled.
 - **Thời gian biểu** - The time period allowed for the PC controlled to access the Internet. For detailed information, please go to "**Kiểm soát truy cập** → **Thời gian biểu**".
 - **Kích hoạt** - Check this option to enable a specific entry.
 - **Tùy chỉnh** - Here you can edit or delete an existing entry.
2. Enter the MAC address of the PC (e.g. 00-11-22-33-44-AA) you'd like to control in the **Địa chỉ MAC của máy tính trẻ em** field, or you can choose the MAC address from the **Tất cả địa chỉ MAC trong mạng LAN hiện tại** drop-down list.
 3. Give a description (e.g. Allow Google) for the website allowed to be accessed in the **Mô tả trang web** field.
 4. Enter the allowed domain name of the website, either the full name or the keywords (e.g. google) in the **Tên miền được cho phép** field. Any domain name with keywords in it (www.google.com, www.google.com.cn) will be allowed.

5. Select from the Effective Time drop-down list the schedule (e.g. Schedule_1) you want. If there are not suitable schedules for you, click the **Thời gian biểu** in red below to go to the Advance Schedule Settings page and create the schedule you need.
6. In the Status field, you can select **Đã kích hoạt** or **Đã vô hiệu hóa** to enable or disable your entry.
7. Click the **Lưu** button.

Click the **Kích hoạt tất cả** button to enable all the rules in the list.

Click the **Vô hiệu hóa tất cả** button to disable all the rules in the list.

Click the **Xóa tất cả** button to delete all the entries in the table.

Click the **Tiếp** button to go to the next page, or click the **Trước** button to return to the previous page.

For example: If you desire that the child PC with MAC address 00-11-22-33-44-AA can access www.google.com on Saturday only while the parent PC with MAC address 00-11-22-33-44-BB is without any restriction, you should follow the settings below.

1. Click **“Quyền kiểm soát của phụ huynh”** menu on the left to enter the Parental Control Settings page. Check **Kích hoạt** and enter the MAC address 00-11-22-33-44-BB in the Địa chỉ MAC của máy tính phụ huynh field.
2. Click **“Kiểm soát truy cập → Thời gian biểu”** on the left to enter the Schedule Settings page. Click **Thêm mới...** button to create a new schedule with Mô tả Thời gian biểu is Schedule_1, Ngày is T7 and Thời gian is cả ngày-24 giờ.
3. Click **“Quyền kiểm soát của phụ huynh”** menu on the left to go back to the Add or Modify Parental Control Entry page:
 - 1) Click **Thêm mới...** button.
 - 2) Enter 00-11-22-33-44-AA in the **Địa chỉ MAC của máy tính trẻ em** field.
 - 3) Enter “Allow Google” in the **Mô tả trang web** field.
 - 4) Enter “www.google.com” in the **Tên miền được cho phép** field.
 - 5) Select “Schedule_1” you create just now from the **Thời gian hiệu lực** drop-down list.
 - 6) In **Trạng thái** field, select Enable.
4. Click **Lưu** to complete the settings.

Then you will go back to the **Cài đặt Quyền kiểm soát của phụ huynh** page and see the following list, as shown in Figure 4-43.

STT	Địa chỉ MAC	Mô tả trang web	Thời gian biểu	Trạng thái	Tùy chỉnh
1	00-11-22-33-44-AA	Allow google	Vĩnh viễn	Đã kích hoạt	Sửa Xóa

Figure 4-43 Parental Control Settings

4.11 Kiểm soát truy cập

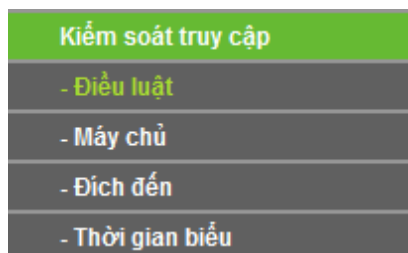


Figure 4-44 Access Control

There are four submenus under the Access Control menu as shown in Figure 4-44: **Điều luật**, **Máy chủ**, **Đích đến** and **Thời gian biểu**. Click any of them, and you will be able to configure the corresponding function.

4.11.1 Điều luật

Choose menu “**Kiểm soát truy cập** → **Điều luật**”, and then you can view and set Access Control rules in the screen as shown in Figure 4-45.

Figure 4-45 Access Control Rule Management

- **Kích hoạt Kiểm soát Truy cập Internet** - Select the check box to enable the Internet Access Control function, so the Default Filter Policy can take effect.
- **Tên điều luật** - Here displays the name of the rule and this name is unique.
- **Máy chủ** - Here displays the host selected in the corresponding rule.
- **Đích đến** - Here displays the target selected in the corresponding rule.
- **Thời gian biểu** - Here displays the schedule selected in the corresponding rule.

- **Kích hoạt** - Here displays the status of the rule, enabled or not. Check this option to enable a specific entry.
- **Tùy chỉnh** - Here you can edit or delete an existing rule.
- **Cài đặt theo hướng dẫn** - Click the **Cài đặt theo hướng dẫn** button to create a new rule entry.
- **Thêm mới...** - Click the **Thêm mới...** button to add a new rule entry.
- **Kích hoạt tất cả** - Click the **Kích hoạt tất cả** button to enable all the rules in the list.
- **Vô hiệu hóa tất cả** - Click the **Vô hiệu hóa tất cả** button to disable all the rules in the list.
- **Xóa tất cả** - Click the **Xóa tất cả** button to delete all the entries in the table.
- **Di chuyển** - You can change the entry's order as desired. Enter in the first box the ID number of the entry you want to move and in the second box another ID number, and then click the **Di chuyển** button to change the entries' order.
- **Tiếp** - Click the **Tiếp** button to go to the next page.
- **Trước** - Click the **Trước** button to return to the previous page.

There are two methods to add a new rule.

Method One:

1. Click **Cài đặt theo hướng dẫn** button and the next screen will appear as shown in Figure 4-46.

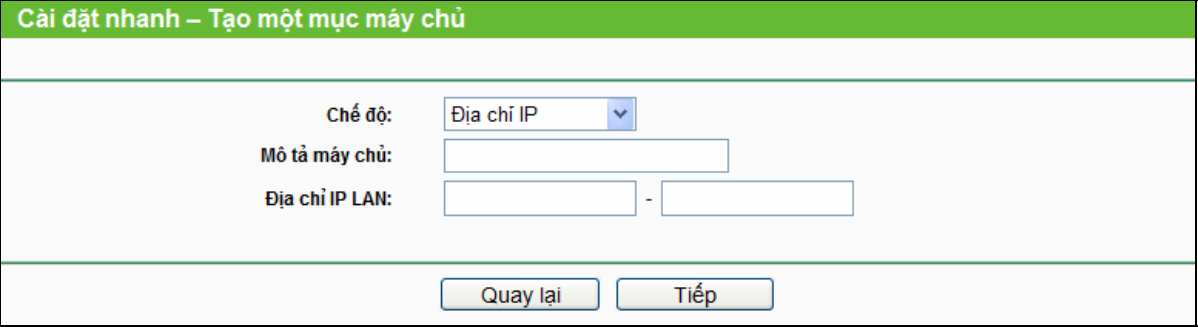


Figure 4-46 Quick Setup – Create a Host Entry

- **Mô tả máy chủ** - In this field, create a unique description for the host (e.g. Host_1).
- **Chế độ** - Here are two options, **Địa chỉ IP** and **Địa chỉ MAC**. You can select either of them from the drop-down list.

If the **Địa chỉ IP** is selected, you can see the following item:

- **Địa chỉ IP LAN**- Enter the IP address or address range of the host in dotted-decimal format (e.g. 192.168.0.23).

If the MAC Address is selected, you can see the following item:

- **Địa chỉ MAC** - Enter the MAC address of the host in XX-XX-XX-XX-XX-XX format (e.g. 00-11-22-33-44-AA).
2. Click **Tiếp** when finishing creating the host entry, and the next screen will appear as shown in Figure 4-47.

The screenshot shows a web interface titled "Cài đặt nhanh – Tạo một mục đích đến truy cập". The form contains the following fields and options:

- Chế độ:** A dropdown menu with "Địa chỉ IP" selected.
- Mô tả đích đến:** A text input field.
- Địa chỉ IP:** Two text input fields separated by a hyphen.
- Cổng đích:** Two text input fields separated by a hyphen.
- Giao thức:** A dropdown menu with "Tất cả" selected.
- Cổng dịch vụ phổ biến:** A dropdown menu with "--Vui lòng chọn--" selected.

At the bottom of the form, there are two buttons: "Quay lại" (Back) and "Tiếp" (Next).

Figure 4-47 Quick Setup – Create an Access Target Entry

- **Mô tả đích đến** - In this field, create a description for the target. Note that this description should be unique (e.g. Target_1).
- **Chế độ** - Here are two options, Địa chỉ IP and Tên miền. You can choose either of them from the drop-down list.

If the **Địa chỉ IP** is selected, you will see the following items:

- **Địa chỉ IP** - Enter the IP address (or address range) of the target (targets) in dotted-decimal format (e.g. 192.168.0.23).
- **Cổng đích** - Specify the port or port range for the target. For some common service ports, you can make use of the Cổng dịch vụ phổ biến item below.
- **Giao thức** - Here are four options, Tất cả, TCP, UDP, and ICMP. Select one of them from the drop-down list for the target.
- **Cổng dịch vụ phổ biến** - Here lists some common service ports. Select one from the drop-down list and the corresponding port number will be filled in the Target Port field automatically. For example, if you select "FTP", "21" will be filled in the Target Port automatically.

If the **Tên miền** is selected, you will see the following items:

- **Tên miền** - Here you can enter 4 domain names, either the full name or the keywords (for example, google). Any domain name with keywords in it (www.google.com, www.google.cn) will be blocked or allowed.

3. Click **Tiếp** when finishing creating the access target entry, and the next screen will appear as shown in Figure 4-48.

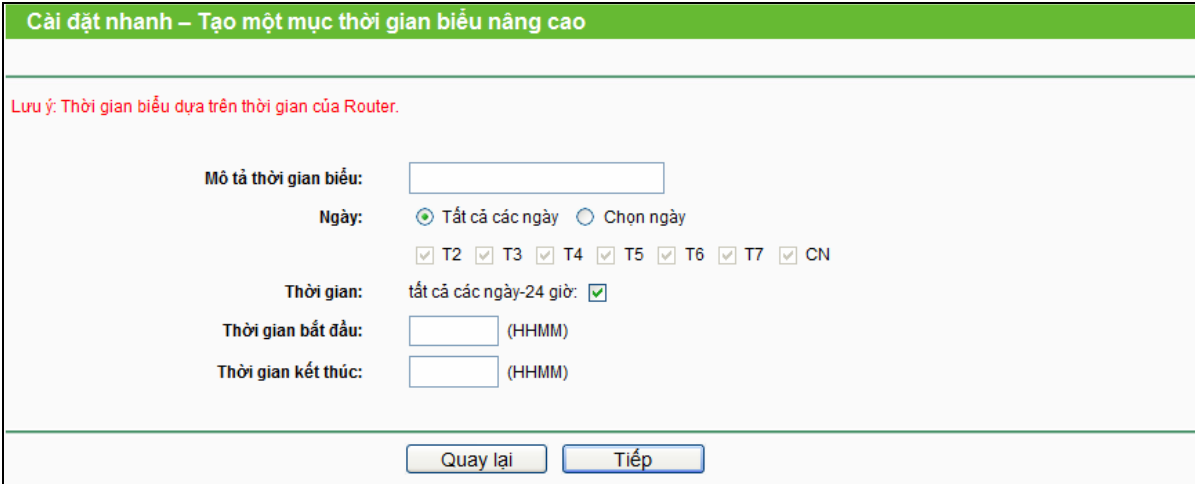


Figure 4-48 Quick Setup – Create an Advanced Schedule Entry

- **Mô tả thời gian biểu** - In this field, create a description for the schedule. Note that this description should be unique (e.g. Schedule_1).
 - **Ngày** - Choose **Chọn ngày** and select the certain day (days), or choose **Tất cả các ngày**.
 - **Thời gian** - Select " **tất cả các ngày – 24h** ", or specify the **Thời gian bắt đầu** and **Thời gian kết thúc** yourself.
 - **Thời gian bắt đầu** - Enter the start time in HHMM format (HHMM are 4 numbers). For example 0800 is 8:00.
 - **Thời gian kết thúc** - Enter the stop time in HHMM format (HHMM are 4 numbers). For example 2000 is 20:00.
4. Click **Tiếp** when finishing creating the advanced schedule entry, and the next screen will appear as shown in Figure 4-49.

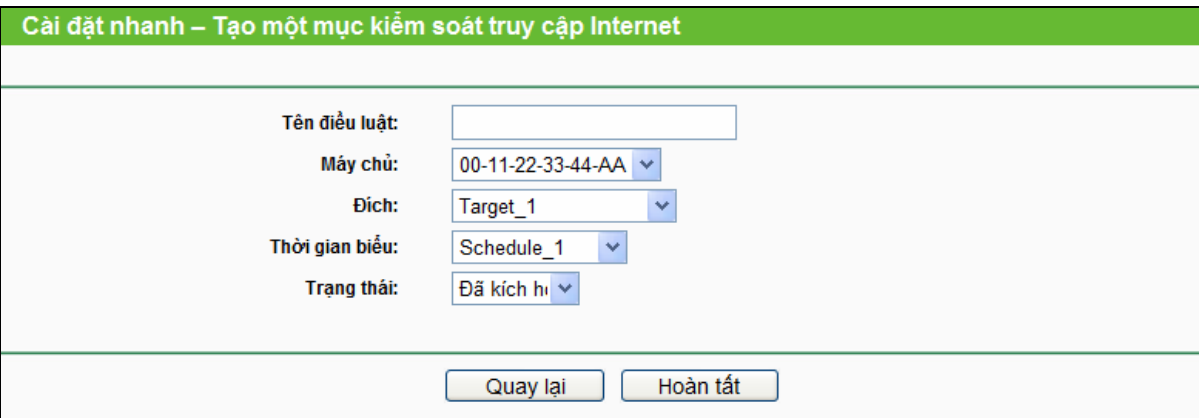


Figure 4-49 Quick Setup – Create an Internet Access Control Entry

- **Tên điều luật** - In this field, create a name for the rule. Note that this name should be unique (e.g. Rule_1).

- **Máy chủ** - In this field, select a host from the drop-down list for the rule. The default value is the **Mô tả máy chủ** you set just now.
- **Đích** - In this field, select a target from the drop-down list for the rule. The default value is the **Mô tả đích đến** you set just now.
- **Thời gian biểu** - In this field, select a schedule from the drop-down list for the rule. The default value is the **Mô tả thời gian biểu** you set just now.
- **Trạng thái** - In this field, there are two options, **Đã kích hoạt** or **Đã vô hiệu hóa**. Select **Đã kích hoạt** so that the rule will take effect. Select **Đã vô hiệu hóa** so that the rule won't take effect.

5. Click **Hoàn tất** to complete adding a new rule.

Method Two:

1. Click the **Thêm mới...** button and the next screen will pop up as shown in Figure 4-50.
2. Give a name (e.g. Rule_1) for the rule in the **Tên điều luật** field.
3. Select a host from the **Máy chủ** drop-down list or choose "**Bấm vào đây để thêm một danh sách máy chủ mới**".
4. Select a target from the **Đích đến** drop-down list or choose "**Bấm vào đây để thêm một danh sách đích đến mới**".
5. Select a schedule from the **Thời gian biểu** drop-down list or choose "**Bấm vào đây để thêm một thời gian biểu mới**".
6. In the **Trạng thái** field, select **Đã kích hoạt** or **Đã vô hiệu hóa** to enable or disable your entry.
7. Click the **Lưu** button.

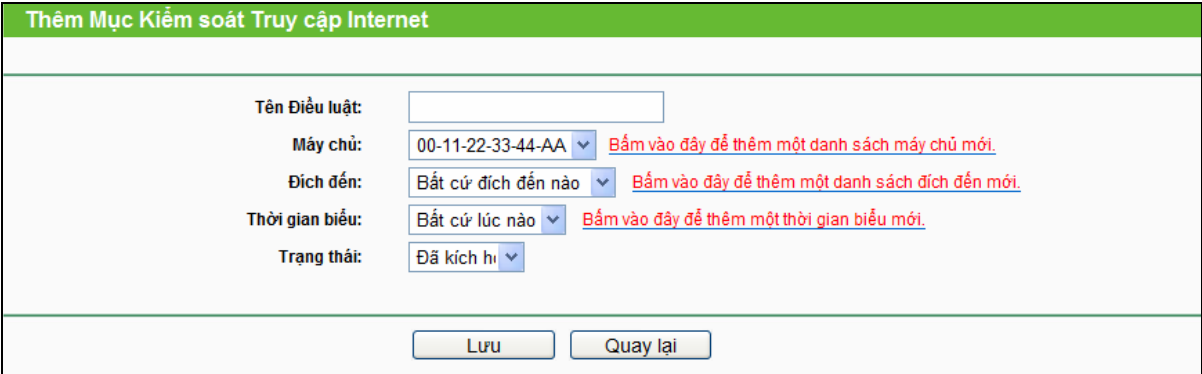


Figure 4-50 Add Internet Access Control Entry

For example: If you desire to allow the host with MAC address 00-11-22-33-44-AA to access www.google.com only from 18:00 to 20:00 on Saturday and Sunday, and forbid other hosts in the LAN to access the Internet, you should follow the settings below:

1. Click the submenu **Điều luật of Kiểm soát truy cập** in the left to return to the Rule List page. Select Enable Internet Access Control and choose "Cho phép các gói tin xác định bởi bất cứ chính sách kiểm soát truy cập được kích hoạt nào đi qua Router".

2. We recommend that you click **Cài đặt theo hướng dẫn** button to finish all the following settings.
3. Click the submenu **Máy chủ of Kiểm soát truy cập** in the left to enter the Host List page. Add a new entry with the Host Description is Host_1 and MAC Address is 00-11-22-33-44-AA.
4. Click the submenu **Đích đến of Kiểm soát truy cập** in the left to enter the Target List page. Add a new entry with the Target Description is Target_1 and Domain Name is www.google.com.
5. Click the submenu **Thời gian biểu of Kiểm soát truy cập** in the left to enter the Schedule List page. Add a new entry with the Schedule Description is Schedule_1, Day is Sat and Sun, Start Time is 1800 and Stop Time is 2000.
6. Click the submenu **Điều luật of Kiểm soát truy cập** in the left, Click **Thêm mới...** button to add a new rule as follows:
 - In Tên điều luật field, create a name for the rule. Note that this name should be unique, for example Rule_1.
 - In Máy chủ field, select Host_1.
 - In Đích đến field, select Target_1.
 - In Thời gian biểu field, select Schedule_1.
 - In Trạng thái field, select Kích hoạt.
 - Click Lưu to complete the settings.

Then you will go back to the Quản lý Điều luật Kiểm soát Truy cập page and see the following list.

STT	Tên điều luật	Máy chủ	Đích đến	Thời gian biểu	Kích hoạt	Tùy chỉnh
1	Rule_1	Host_1	Target_1	Schedule_1	<input checked="" type="checkbox"/>	Sửa Xóa

4.11.2 Máy chủ

Choose menu “**Kiểm soát truy cập** → **Máy chủ**”, and then you can view and set a Host list in the screen as shown in Figure 4-51. The host list is necessary for the Access Control Rule.

Thiết lập máy chủ			
STT	Mô tả Máy chủ	Thông tin	Tùy chỉnh
1	00-11-22-33-44-AA	IP: 192.168.0.23	Sửa Xóa
<input type="button" value="Thêm mới..."/> <input type="button" value="Xóa tất cả"/>			
<input type="button" value="Trước"/>		<input type="button" value="Tiếp"/>	
Số thứ tự hiện tại <input type="text" value="1"/> Trang			

Figure 4-51 Host Settings

- **Mô tả máy chủ** - Here displays the description of the host and this description is unique.
- **Thông tin** - Here displays the information about the host. It can be IP or MAC.
- **Tùy chỉnh** - To modify or delete an existing entry.

To add a new entry, please follow the steps below.

1. Click the **Thêm mới...** button.
2. In the **Chế độ** field, select Địa chỉ IP or Địa chỉ MAC.
 - If you select Địa chỉ IP, the screen shown is Figure 4-52.
 - 1) In **Mô tả máy chủ** field, create a unique description for the host (e.g. Host_1).
 - 2) In **Địa chỉ IP LAN** field, enter the IP address.
 - If you select Địa chỉ MAC, the screen shown is Figure 4-53.
 - 1) In **Mô tả máy chủ** field, create a unique description for the host (e.g. Host_1).
 - 2) In **Địa chỉ MAC** field, enter the MAC address.
3. Click the **Lưu** button to complete the settings.

Click the **Xóa tất cả** button to delete all the entries in the table.

Click the **Tiếp** button to go to the next page, or click the **Trước** button to return to the previous page.

Figure 4-52 Add or Modify a Host Entry

Figure 4-53 Add or Modify a Host Entry

For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA, you should first follow the settings below:

1. Click **Thêm mới...** button in Figure 4-51 to enter the Add or Modify a Host Entry page.
2. In **Chế độ** field, select Địa chỉ MAC from the drop-down list.
3. In **Mô tả máy chủ** field, create a **unique** description for the host (e.g. Host_1).
4. In **Địa chỉ MAC** field, enter 00-11-22-33-44-AA.
5. Click **Lưu** to complete the settings.

Then you will go back to the Host Settings page and see the following list.

STT	Mô tả Máy chủ	Thông tin	Tùy chỉnh
1	Host_1	MAC: 00-11-22-33-44-AA	Sửa Xóa

4.11.3 Đích đến

Choose menu “**Kiểm soát truy cập** → **Đích đến**”, and then you can view and set a Target list in the screen as shown in Figure 4-54. The target list is necessary for the Access Control Rule.

STT	Mô tả đích đến	Thông tin	Tùy chỉnh
1	Target_1	192.168.0.23/21	Sửa Xóa

Thêm mới... Xóa tất cả

Trước Tiếp Số thứ tự hiện tại 1 Trang

Figure 4-54 Target Settings

- **Mô tả đích đến** - Here displays the description about the target and this description is unique.
- **Thông tin** - The target can be IP address, port, or domain name.
- **Tùy chỉnh** - To modify or delete an existing entry.

To add a new entry, please follow the steps below.

1. Click the **Thêm mới...** button.
2. In **Chế độ** field, select **Địa chỉ IP** or **Tên miền**.
3. If you select **Địa chỉ IP**, the screen shown is Figure 4-55.

Thêm hoặc Tùy chỉnh một Mục Đích đến truy cập

Chế độ:

Mô tả đích đến:

Địa chỉ IP: -

Cổng đích đến: -

Giao thức:

Cổng dịch vụ phổ biến:

Lưu Quay lại

Figure 4-55 Add or Modify an Access Target Entry

- 1) In **Mô tả đích đến** field, create a unique description for the target (e.g. Target_1).
 - 2) In **Địa chỉ IP** field, enter the IP address of the target.
 - 3) Select a common service from **Cổng dịch vụ phổ biến** drop-down list, so that the **Cổng đích đến** will be automatically filled. If the **Cổng dịch vụ phổ biến** drop-down list doesn't have the service you want, specify the **Cổng đích** manually.
 - 4) In **Giao thức** field, select TCP, UDP, ICMP or **Tất cả** from the drop-down list.
4. If you select **Tên miền**, the screen shown is Figure 4-56.

Thêm hoặc Tùy chỉnh một Mục Đích đến truy cập

Chế độ: Tên miền ▼

Mô tả đích đến:

Tên miền:

Figure 4-56 Add or Modify an Access Target Entry

- 1) In **Mô tả đích đến** field, create a unique description for the target (e.g. Target_1).
- 2) In **Tên miền** field, enter the domain name, either the full name or the keywords (for example, google) in the blank. Any domain name with keywords in it (www.google.com, www.google.cn) will be blocked or allowed. You can enter 4 domain names.

5. Click the **Lưu** button.

Click the **Xóa tất cả** button to delete all the entries in the table.

Click the **Tiếp** button to go to the next page, or click the **Trước** button to return to the previous page.

For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA in the LAN to access www.google.com only, you should first follow the settings below:

1. Click **Thêm mới...** button in Figure 4-54 to enter the Thêm hoặc Tùy chỉnh một Mục Đích đến truy cập page.
2. In **Chế độ** field, select **Tên miền** from the drop-down list.
3. In **Mô tả đích đến** field, create a unique description for the target (e.g. Target_1).
4. In **Tên miền** field, enter www.google.com.
5. Click **Lưu** to complete the settings.

Then you will go back to the Target Settings page and see the following list.

STT	Mô tả đích đến	Thông tin	Tùy chỉnh
1	Target_1	www.google.com	Sửa Xóa

4.11.4 Thời gian biểu

Choose menu "**Kiểm soát truy cập** → **Thời gian biểu**", and then you can view and set a Schedule list in the next screen as shown in Figure 4-57. The Schedule list is necessary for the Access Control Rule.

Cài đặt Thời gian biểu				
STT	Mô tả Thời gian biểu	Ngày	Giờ	Tùy chỉnh
1	Schedule_1	Tất cả các ngày	00:00 - 24:00	Sửa Xóa

Thêm mới... Xóa tất cả

Trước Tiếp Số thứ tự hiện tại 1 Trang

Figure 4-57 Schedule Settings

- **Mô tả Thời gian biểu** - Here displays the description of the schedule and this description is unique.
- **Ngày** - Here displays the day(s) in a week.
- **Giờ** - Here displays the time period in a day.
- **Tùy chỉnh** - Here you can edit or delete an existing schedule.

To add a new schedule, follow the steps below:

1. Click **Thêm mới...** button shown in Figure 4-57 and the next screen will pop-up as shown in Figure 4-58.
2. In **Mô tả Thời gian biểu** field, create a unique description for the schedule (e.g. Schedule_1).
3. In **Ngày** field, select the day or days you need.
4. In **Giờ** field, you can select Cả ngày – 24 giờ or you may enter the Thời gian bắt đầu and Thời gian kết thúc in the corresponding field.
5. Click **Lưu** to complete the settings.

Click the **Xóa tất cả** button to delete all the entries in the table.

Click the **Tiếp** button to go to the next page, or click the **Trước** button to return to the previous page.

Cài đặt thời gian biểu nâng cao	
Lưu ý: Thời gian biểu dựa trên thời gian của Router.	
Mô tả Thời gian biểu:	<input type="text"/>
Ngày:	<input checked="" type="radio"/> Mọi ngày <input type="radio"/> Chọn ngày <input checked="" type="checkbox"/> T2 <input checked="" type="checkbox"/> T3 <input checked="" type="checkbox"/> T4 <input checked="" type="checkbox"/> T5 <input checked="" type="checkbox"/> T6 <input checked="" type="checkbox"/> T7 <input checked="" type="checkbox"/> CN
Thời gian:	<input checked="" type="checkbox"/> cả ngày-24 giờ
Thời gian bắt đầu:	<input type="text"/> (HHMM)
Thời gian kết thúc:	<input type="text"/> (HHMM)
<input type="button" value="Lưu"/> <input type="button" value="Quay lại"/>	

Figure 4-58 Advanced Schedule Settings

For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA to access www.google.com only from **18:00 to 20:00** on **Saturday** and **Sunday**, you should first follow the settings below:

- 1) Click **Thêm mới...** button shown in Figure 4-57 to enter the Advanced Schedule Settings page.
- 2) In **Mô tả thời gian biểu** field, create a unique description for the schedule (e.g. Schedule_1).
- 3) In **Ngày** field, check the **Chọn ngày** radio button and then select T7 and CN.
- 4) In **Giờ** field, enter 1800 in **Thời gian bắt đầu** field and 2000 in **Thời gian kết thúc** field.
- 5) Click **Lưu** to complete the settings.

Then you will go back to the Schedule Settings page and see the following list.

STT	Mô tả Thời gian biểu	Ngày	Giờ	Tùy chỉnh
1	Schedule_1	T7 CN	18:00 - 24:00	Sửa Xóa

4.12 Định tuyến nâng cao

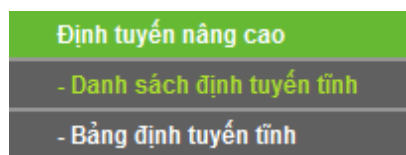


Figure 4-59 Advanced Routing

There are two submenus under the Advanced Routing menu as shown in Figure 4-59: **Danh sách định tuyến nâng cao** and **Bảng định tuyến tĩnh**. Click any of them, and you will be able to configure the corresponding function.

4.12.1 Danh sách định tuyến tĩnh

Choose menu “**Định tuyến nâng cao** → **Danh sách định tuyến tĩnh**”, and then you can configure the static route in the next screen (shown in Figure 4-60). A static route is a pre-determined path that network information must travel to reach a specific host or network.

Định tuyến tĩnh					
STT	Mạng đích	Subnet Mask	Gateway mặc định	Trạng thái	Tùy chỉnh
<div style="display: flex; justify-content: space-between; align-items: center;"> Thêm mới... Kích hoạt tất cả Vô hiệu hóa tất cả Xóa tất cả </div>					
<div style="display: flex; justify-content: center; gap: 20px;"> Trước Tiếp </div>					

Figure 4-60 Static Routing

To add static routing entries:

1. Click **Thêm mới...** shown in Figure 4-60, you will see the following screen.

Thêm hoặc Tùy chỉnh một mục định tuyến tĩnh	
Mạng đích:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Gateway mặc định:	<input type="text"/>
Trạng thái:	Đã kích hoạt <input type="button" value="v"/>
<input type="button" value="Lưu"/> <input type="button" value="Quay lại"/>	

Figure 4-61 Add or Modify a Static Route Entry

2. Enter the following data:
 - **Mạng đích** - The Destination Network 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 mặc định** - This is the IP Address of the gateway device that allows for contact between the Router and the network or host.
3. Select **Đã kích hoạt** or **Đã vô hiệu hóa** for this entry on the **Trạng thái** drop-down list.
4. Click the **Lưu** button to make the entry take effect.

Other configurations for the entries:

Click the **Xóa** button to delete the entry.

Click the **Kích hoạt tất cả** button to enable all the entries.

Click the **Vô hiệu hóa tất cả** button to disable all the entries.

Click the **Xóa tất cả** button to delete all the entries.

Click the **Trước** button to view the information in the previous screen, click the **Tiếp** button to view the information in the next screen.

4.12.2 Bảng định tuyến hệ thống

Choose menu "**Định tuyến nâng cao** → **Bảng định tuyến hệ thống**", and then you can view the System Routing Table in the next screen (shown in Figure 4-62). System routing table views all of the valid route entries in use. The Destination IP address, Subnet Mask, Gateway, and Interface will be displayed for each entry.

Bảng định tuyến hệ thống				
STT	Mạng đích	Subnet Mask	Gateway	Giao diện
1	192.168.0.0	255.255.255.0	0.0.0.0	LAN & WLAN

Figure 4-62 System Routing Table

- **Mạng đích** - The Destination Network is the address of the network or host to which the static route is assigned.
- **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.
- **Giao diện** - This interface tells you either the Destination IP Address is on the **LAN & WLAN** (internal wired and wireless networks), or on the **WAN** (Internet).

4.13 Kiểm soát băng thông

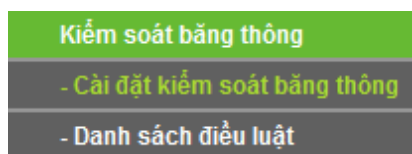


Figure 4-63 Bandwidth Control

There are two submenus under the Bandwidth Control menu as shown in Figure 4-63: **Cài đặt kiểm soát băng thông** and **Danh sách điều luật**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.13.1 Cài đặt kiểm soát băng thông

Choose menu “**Kiểm soát băng thông** → **Cài đặt kiểm soát băng thông**”, and then you can configure the Egress Bandwidth and Ingress Bandwidth in the next screen. Their values you configure should be less than 100000Kbps. For optimal control of the bandwidth, please select the right Line Type and ask your ISP for the total bandwidth of the egress and ingress.

Figure 4-64 Bandwidth Control Settings

- **Kích hoạt Kiểm soát băng thông** - Check this box so that the Bandwidth Control settings can take effect.
- **Dạng dây** - Select the right type for you network connection. If you don't know how to choose, please ask your ISP for the information.
- **Băng thông ra** - The upload speed through the WAN port.
- **Băng thông vào** - The download speed through the WAN port.

4.13.2 Danh sách điều luật

Choose menu “**Kiểm soát băng thông**→ **Danh sách điều luật**”, and then you can view and configure the Bandwidth Control rules in the screen below.

STT	Mô tả	Băng thông ra(Kbps)		Băng thông vào(Kbps)		Kích hoạt	Tùy chỉnh
		Nhỏ nhất	Lớn nhất	Nhỏ nhất	Lớn nhất		
1	192.168.0.1 - 192.168.0.23/21/TCP	0	0	0	0	<input checked="" type="checkbox"/>	Tùy chỉnh Xóa

Figure 4-65 Bandwidth Control Rules List

- **Mô tả** - This is the information about the rules such as address range.
- **Băng thông ra** - This field displays the max and mix upload bandwidth through the WAN port, the default is 0.
- **Băng thông vào** - This field displays the max and mix download bandwidth through the WAN port, the default is 0.
- **Kích hoạt** - This displays the status of the rule.
- **Tùy chỉnh** - Click **Tùy chỉnh** to edit the rule. Click **Xóa** to delete the rule.

To add/modify a Bandwidth Control rule, follow the steps below.

1. Click **Thêm mới...** shown in Figure 4-65, you will see a new screen shown in Figure 4-66.
2. Enter the information like the screen shown below.

Cài đặt điều luật kiểm soát băng thông

Kích hoạt:

Khoảng IP: -

Khoảng Cổng: -

Giao thức:

Băng thông nhỏ nhất(Kbps) Băng thông lớn nhất(Kbps)

Băng thông ra:

Băng thông vào:

Figure 4-66 Bandwidth Control Rule Settings

3. Click the **Lưu** button.

4.14 Kết hợp IP & MAC



Figure 4-67 the IP & MAC Binding menu

There are two submenus under the **Kết hợp IP & MAC** menu (shown in Figure 4-67): **Cài đặt liên kết** and **Danh sách ARP**. Click any of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

4.14.1 Cài đặt liên kết

This page displays the **Cài đặt liên kết** table; you can operate it in accord with your desire (shown in Figure 4-68).

Cài đặt liên kết

Kết hợp ARP: Vô hiệu hóa Kích hoạt

STT	Địa chỉ MAC	Địa chỉ IP	Liên kết	Tùy chỉnh
1	40-61-86-C4-98-43	192.168.0.100	<input checked="" type="checkbox"/>	Tùy chỉnh Xóa

STT hiện tại Trang

Figure 4-68 Binding Setting

- **Địa chỉ MAC** - The MAC address of the controlled computer in the LAN.
- **Địa chỉ IP** - The assigned IP address of the controlled computer in the LAN.
- **Liên kết** - Check this option to enable ARP binding for a specific device.

➤ **Tùy chỉnh** - To modify or delete an existing entry.

When you want to add or modify an IP & MAC Binding entry, you can click the **Thêm mới...** button or **Tùy chỉnh** button, and then you will go to the next page. This page is used for adding or modifying an IP & MAC Binding entry (shown in Figure 4-69).

Figure 4-69 IP & MAC Binding Setting (Add & Modify)

To add IP & MAC Binding entries, follow the steps below.

1. Click the **Thêm mới...** button as shown in Figure 4-68.
2. Enter the Địa chỉ MAC and Địa chỉ IP.
3. Select the **Kết hợp** checkbox.
4. Click the **Lưu** button to save it.

To modify or delete an existing entry, follow the steps below.

1. Find the desired entry in the table.
2. Click **Tùy chỉnh** or **Xóa** as desired on the **Tùy chỉnh** column.

To find an existing entry, follow the steps below.

1. Click the **Tìm kiếm** button as shown in Figure 4-68.
2. Enter the Địa chỉ MAC or Địa chỉ IP.
3. Click the **Tìm kiếm** button in the page as shown in Figure 4-70.

Figure 4-70 Find IP & MAC Binding Entry

Click the **Kích hoạt tất cả** button to make all entries enabled.

Click the **Xóa tất cả** button to delete all entries.

4.14.2 Danh sách ARP

To manage the computer, you could observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could also configure the items on the ARP list. This page displays the ARP List; it shows all the existing IP & MAC Binding entries (shown in Figure 4-71).

Danh sách ARP				
STT	Địa chỉ MAC	Địa chỉ IP	Trạng thái	Cấu hình
1	40-61-86-E5-B2-DC	192.168.0.20	Không kết hợp	Tải Xóa

Figure 4-71 ARP List

1. **Địa chỉ MAC** - The MAC address of the controlled computer in the LAN.
2. **Địa chỉ IP** - The assigned IP address of the controlled computer in the LAN.
3. **Trạng thái** - Indicates whether or not the MAC and IP addresses are bound.
4. **Cấu hình** - Load or delete an item.
 - **Tải**- Load the item to the IP & MAC Binding list.
 - **Xóa** - Delete the item.

Click the **Kết hợp tất cả** button to bind all the current items, available after enable.

Click the **Tải tất cả** button to load all items to the IP & MAC Binding list.

Click the **Làm mới** button to refresh all items.

 **Note:**

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

4.15 DNS động

Choose menu "**DNS động**", and you can configure the Dynamic DNS function.

The Router offers the **DDNS** (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as www.comexe.cn, www.dyndns.org, or www.no-ip.com. The Dynamic DNS client service provider will give you a password or key.

4.15.1 Comexe.cn DDNS

If the dynamic DNS **Service Provider** you select is www.comexe.cn, the page will appear as shown in Figure 4-72.

Figure 4-72 Comexe.cn DDNS Settings

To set up for DDNS, follow these instructions:

1. Enter the **Tên miền** your dynamic DNS service provider gave.
2. Enter the **Tên đăng nhập** for your DDNS account.
3. Enter the **Mật mã** for your DDNS account.
4. Click the **Đăng nhập** button to login the DDNS service.

Trạng thái kết nối -The status of the DDNS service connection is displayed here.

Click **Đăng xuất** to log out of the DDNS service.

 **Note:**

If you want to login again with another account after a successful login, please click the **Đăng xuất** button, then input your new username and password and click the **Đăng nhập** button.

4.15.2 Dyndns.org DDNS

If the dynamic DNS **Service Provider** you select is www.dyndns.org, the page will appear as shown in Figure 4-73.

DDNS

Nhà cung cấp dịch vụ: Dyndns (www.dyndns.org) [Đăng ký...](#)

Tên đăng nhập: username

Mật mã: ●●●●●●●●●●

Tên miền:

Kích hoạt DDNS

Trạng thái kết nối: DDNS không khởi chạy!

[Đăng nhập](#) [Đăng xuất](#)

[Lưu](#)

Figure 4-73 Dyndns.org DDNS Settings

To set up for DDNS, follow these instructions:

1. Enter the **Tên đăng nhập** for your DDNS account.
2. Enter the **Mật mã** for your DDNS account.
3. Enter the **Tên miền** you received from dynamic DNS service provider.
4. Click the **Đăng nhập** button to login to the DDNS service.

Trạng thái kết nối -The status of the DDNS service connection is displayed here.

Click **Đăng xuất** to logout of the DDNS service.

 **Note:**

If you want to login again with another account after a successful login, please click the **Đăng xuất** button, then input your new username and password and click the **Đăng nhập** button.

4.15.3 No-ip.com DDNS

If the dynamic DNS **Service Provider** you select is www.no-ip.com, the page will appear as shown in Figure 4-74.

DDNS

Nhà cung cấp dịch vụ: No-IP (www.no-ip.com)

Tên đăng nhập:

Mật mã:

Tên miền:

Kích hoạt DDNS

Trạng thái kết nối: DDNS không khởi chạy!

Figure 4-74 No-ip.com DDNS Settings

To set up for DDNS, follow these instructions:

1. Enter the **Tên đăng nhập** for your DDNS account.
2. Enter the **Mật mã** for your DDNS account.
3. Enter the **Tên miền** you received from dynamic DNS service provider.
4. Click the **Đăng nhập** button to login to the DDNS service.

Trạng thái kết nối - The status of the DDNS service connection is displayed here.

Click **Đăng xuất** to log out the DDNS service.

 **Note:**

If you want to login again with another account after a successful login, please click the **Đăng xuất** button, then input your new username and password and click the **Đăng nhập** button.

4.16 Công cụ hệ thống



Figure 4-75 The System Tools menu

Choose menu “**Công cụ hệ thống**”, and you can see the submenus under the main menu: **Cài đặt thời gian**, **Công cụ chẩn đoán**, **Nâng cấp Firmware**, **Cài đặt gốc**, **Sao lưu & Phục hồi**, **Khởi động lại**, **Mật mã**, **Bản ghi hệ thống** and **Thống kê**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.16.1 Cài đặt thời gian

Choose menu “**Công cụ hệ thống**→**Cài đặt thời gian**”, and then you can configure the time on the following screen.

Cài đặt thời gian

Múi giờ: (GMT+08:00) Beijing, Hong Kong, Perth, Singapore ▼

Ngày: (MM/DD/YY)

Giờ: (HH/MM/SS)

Server NTP I: (Tùy chọn)

Server NTP II: (Tùy chọn)

Kích hoạt chế độ Tiết kiệm ánh sáng ngày

Bắt đầu:

Kết thúc:

Trạng thái Tiết kiệm Ánh sáng ngày: tiết kiệm ánh sáng ngày đã tắt

Lưu ý: Bấm “Lấy giờ GMT” để cập nhật thời gian từ Internet với các server được định nghĩa trước

Figure 4-76 Time settings

- **Múi giờ**- Select your local time zone from this pull down list.
- **Ngày** - Enter your local date in MM/DD/YY into the right blanks.
- **Giờ** - Enter your local time in HH/MM/SS into the right blanks.
- **Server NTP I / Server NTP II** - Enter the address or domain of the **Server NTP I** or **Server NTP II**, and then the Router will get the time from the NTP Server preferentially. In addition, the Router built-in some common NTP Servers, so it can get time automatically once it connects the Internet.
- **Kích hoạt chế độ Tiết kiệm ánh sáng ngày** - Check the box to enable the Daylight Saving function.
- **Bắt đầu** - The time to start the Daylight Saving. Select the month in the first field, the week in the second field, the day in the third field and the time in the last field.
- **Kết thúc** - The time to end the Daylight Saving. Select the month in the first field, the week in the second field, the day in the third field and the time in the last field.
- **Trạng thái tiết kiệm ánh sáng ngày** - Displays the status whether the Daylight Saving is in use.

To set time manually:

1. Select your local time zone.
2. Enter the **Ngày** in Month/Day/Year format.
3. Enter the **Giờ** in Hour/Minute/Second format.
4. Click **Lưu**.

To set time automatically:

1. Select your local time zone.
2. Enter the address or domain of the **Server NTP I** or **Server NTP II**.
3. Click the **Lấy GMT** button to get system time from Internet if you have connected to the Internet.

To set Daylight Saving:

1. Check the box to enable Daylight Saving.
2. Select the start time from the drop-down lists in the **Bắt đầu** field.
3. Select the end time from the drop-down lists in the **Kết thúc** field.
4. Click the **Lưu** button to save the settings.

	<input checked="" type="checkbox"/> Kích hoạt chế độ Tiết kiệm ánh sáng ngày			
Bắt đầu:	Th3 ▾	Thứ ba ▾	CN ▾	2 giờ sáng ▾
Kết thúc:	Th11 ▾	Thứ hai ▾	CN ▾	3 giờ sáng ▾
Trạng thái Tiết kiệm Ánh sáng ngày:	tiết kiệm ánh sáng ngày đã tắt.			

Figure 4-77 Time settings

 **Note:**

1. This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, otherwise, these functions will not take effect.
2. The time will be lost if the router is turned off.
3. The Router will automatically obtain GMT from the Internet if it is configured accordingly.
4. The Daylight Saving will take effect one minute after the configurations are completed.

4.16.2 Công cụ chẩn đoán

Choose menu “**Công cụ hệ thống** → **Công cụ chẩn đoán**”, and then you can transact **Ping** or **Traceroute** function to check connectivity of your network in the following screen.

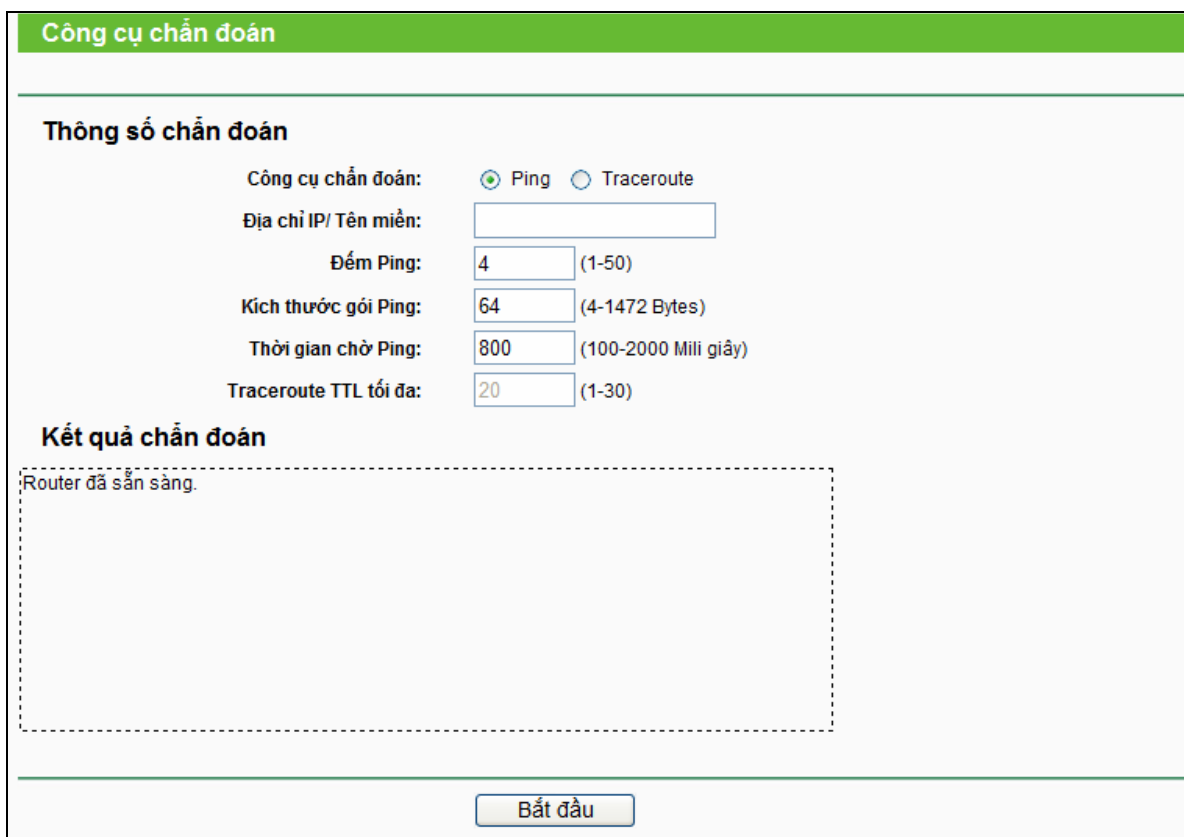


Figure 4-78 Diagnostic Tools

- **Công cụ chẩn đoán** - Check the radio button to select one diagnostic tool.
- **Ping** - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
- **Traceroute** - This diagnostic tool tests the performance of a connection.

 **Note:**

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

- **Địa chỉ IP/Tên miền**- Enter the IP Address or Domain Name of the PC whose connection you

wish to diagnose.

- **Đếm Ping** - Specifies the number of Echo Request messages sent. The default is 4.
- **Kích thước gói Ping** - Specifies the number of data bytes to be sent. The default is 64.
- **Thời gian chờ Ping** - Time to wait for a response, in milliseconds. The default is 800.
- **Traceroute TTL tối đa** - Set the maximum number of hops (max TTL to be reached) in the path to search for the target (destination). The default is 20.

Click **Bắt đầu** to check the connectivity of the Internet.

The **Kết quả chẩn đoán** page displays the result of diagnosis.

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

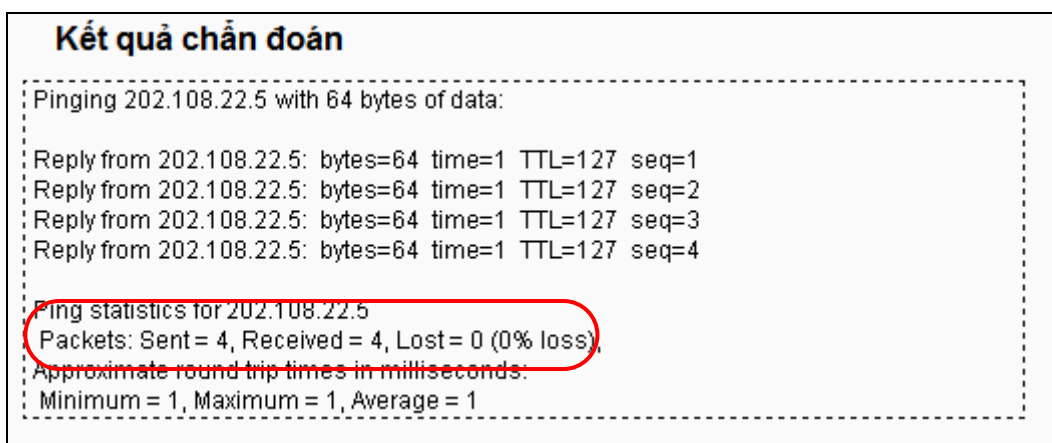


Figure 4-79 Diagnostic Results

Note:

1. Only one user can use the diagnostic tools at one time.
2. "Đếm Ping", "Kích thước gói Ping" and "Thời gian chờ Ping " are Ping Parameters, and "Traceroute TTL tối đa" is Traceroute Parameter.

4.16.3 Nâng cấp Firmware

Choose menu **"Công cụ hệ thống → Nâng cấp Firmware"**, and then you can update the latest version of firmware for the Router on the following screen.



Figure 4-80 Firmware Upgrade

- **Phiên bản Firmware** - Displays the current firmware version.

- **Phiên bản phần cứng** - Displays the current hardware version. The hardware version of the upgrade file must accord with the Router's current hardware version.

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

1. Download a most recent firmware upgrade file from our website (www.tp-link.vn).
2. Enter or select the path name where you save the downloaded file on the computer into the **Tập tin** blank.
3. Click the **Nâng cấp** button.
4. The Router will reboot while the upgrading has been finished.

 **Note:**

- 1) New firmware versions are posted at <http://www.tp-link.vn> and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the Router rather than the configuration, you can try to upgrade the firmware.
- 2) When you upgrade the Router's firmware, you may lose its current configurations, so before upgrading the firmware please write down some of your customized settings to avoid losing important settings.
- 3) Do not turn off the Router or press the Reset button while the firmware is being upgraded. Loss of power during the upgrade could damage the Router.
- 4) The firmware version must correspond to the hardware.
- 5) The upgrade process takes a few moments and the Router restarts automatically when the upgrade is complete.

4.16.4 Cài đặt gốc

Choose menu "**Công cụ hệ thống** → **Cài đặt gốc**", and then and you can restore the configurations of the Router to factory defaults on the following screen

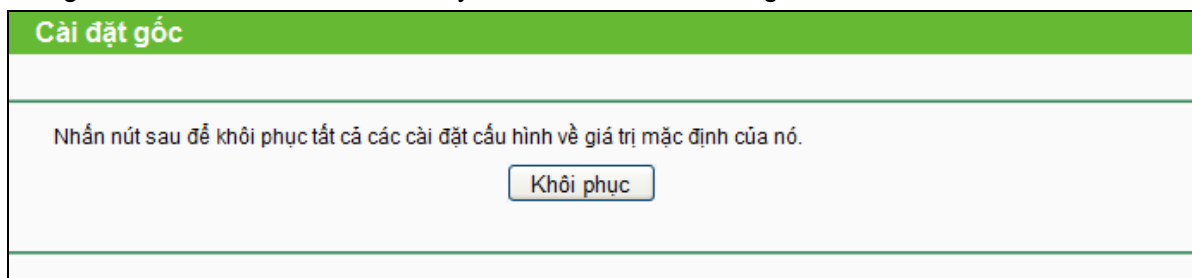


Figure 4-81 Restore Factory Default

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

- The default **Tên đăng nhập**: admin
- The default **Mật mã**: admin
- The default **Địa chỉ IP**: 192.168.0.1
- The default **Subnet Mask**: 255.255.255.0

 **Note:**

All changed settings will be lost when defaults are restored.

4.16.5 Sao lưu & Phục hồi

Choose menu “**Công cụ hệ thống** → **Sao lưu & Phục hồi**”, and then you can save the current configuration of the Router as a backup file and restore the configuration via a backup file as shown in Figure 4-82.



Figure 4-82 Backup & Restore Configuration

- Click the **Sao lưu** button to save all configuration settings as a backup file in your local computer.
- To upgrade the Router's configuration, follow these instructions.
 - Click the **Browse** button to find the configuration file which you want to restore.
 - Click the **Khôi phục** button to update the configuration with the file whose path is the one you have input or selected in the blank.

 **Note:**

The current configuration will be covered with the uploading configuration file. Wrong process will lead the device unmanaged. The restoring process lasts for 20 seconds and the Router will restart automatically then. Keep the power of the Router on during the process, in case of any damage.

4.16.6 Khởi động lại

Choose menu “**Công cụ hệ thống** → **Khởi động lại**”, and then you can click the **Khởi động lại** button to reboot the Router via the next screen.

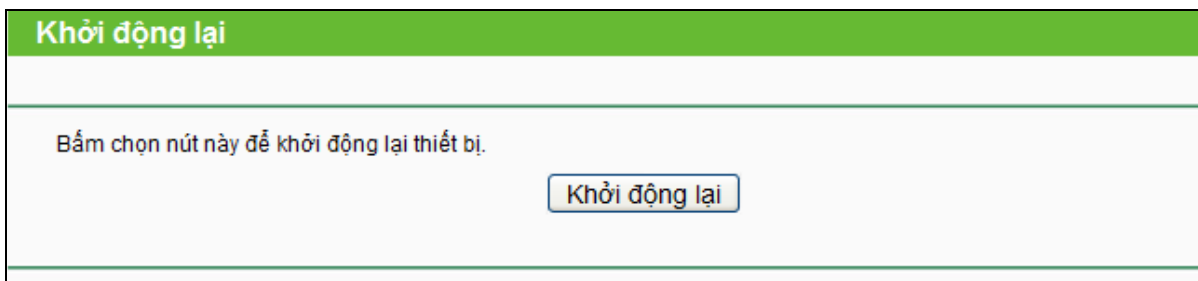


Figure 4-83 Reboot the Router

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

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.

- Change the Wireless configurations.
- Change the Web Management Port.
- Upgrade the firmware of the Router (system will reboot automatically).
- Restore the Router's settings to factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically).

4.16.7 Mật mã

Choose menu “**Công cụ hệ thống** → **Mật mã**”, and then you can change the factory default user name and password of the Router in the next screen as shown in Figure 4-84.

Figure 4-84 Password

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

 **Note:**

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

Click the **Lưu** button when finished.

Click the **Xóa tất cả** button to clear all.

4.16.8 Bản ghi hệ thống

Choose menu “**Công cụ hệ thống** → **Bản ghi hệ thống**”, and then you can view the logs of the Router.

Bản ghi hệ thống

Chức năng thư tự động: **Đã vô hiệu hóa**

Dạng bản ghi: Cấp độ bản ghi:

Chỉ số	Thời gian	Dạng	Cấp độ	Nội dung bản ghi
168	1st day 02:15:34	PPP	Cảnh báo	PPPoE hard line is disconnected, please check the line
167	1st day 02:15:30	PPP	Cảnh báo	PPPoE hard line is disconnected, please check the line
166	1st day 02:15:26	PPP	Cảnh báo	PPPoE hard line is disconnected, please check the line
165	1st day 02:15:22	PPP	Cảnh báo	PPPoE hard line is disconnected, please check the line
164	1st day 02:15:18	PPP	Cảnh báo	PPPoE hard line is disconnected, please check the line
163	1st day 02:15:14	PPP	Cảnh báo	PPPoE hard line is disconnected, please check the line

Time = 1970-01-01 2:15:36 8137s
 H-Ver = WR740N v4 00000000 : S-Ver = 3.12.11 Build 120614 Rel.51047n
 L = 192.168.0.1 : M = 255.255.255.0
 W1 = PPPoE : W = 0.0.0.0 : M = 0.0.0.0 : G = 0.0.0.0

Số thứ tự hiện tại Trang

Figure 4-85 System Log

- **Chức năng thư tự động** - Indicates whether auto mail feature is enabled or not.
- **Cài đặt thư** - Set the receiving and sending mailbox address, server address, validation information as well as the timetable for Auto Mail Feature, as shown in Figure 4-86.

Cài đặt Tài khoản thư

Từ:

Đến:

Server SMTP:

Xác thực

Kích hoạt chức năng thư tự động

Hàng ngày, gửi bản ghi tại :

Gửi bản ghi mỗi giờ

Figure 4-86 Mail Account Settings

- **Từ** - Your mail box address. The Router would connect it to send logs.
- **Đến** - Recipient's address. The destination mailbox where the logs would be received.
- **Server SMTP** - Your smtp server. It corresponds with the mailbox filled in the **From** field.

You can log on the relevant website for help if you are not clear with the address.

- **Xác thực** - Most SMTP Server requires Authentication. It is required by most mailboxes that need User Name and Password to log in.

 **Note:**

Only when you select **Xác thực**, do you have to enter the User Name and Password in the following fields.

- **Tên đăng nhập** - Your mail account name filled in the From field. The part behind @ is excluded.
- **Mật mã** - Your mail account password.
- **Xác nhận mật mã** - Enter the password again to confirm.
- **Kích hoạt chức năng thư tự động** - Select it to mail logs automatically. You could mail the current logs either at a specified time everyday or by intervals, but only one could be the current effective rule. Enter the desired time or intervals in the corresponding field as shown in Figure 4-86.

Click **Lưu** to keep your settings.

Click **Quay lại** to return to the previous page.

- **Dạng bản ghi** - By selecting the log type, only logs of this type will be shown.
- **Cấp độ bản ghi** - By selecting the log level, only logs of this level will be shown.
- **Làm mới** - Refresh the page to show the latest log list.
- **Lưu bản ghi** - Click to save all the logs in a txt file.
- **Bản ghi thư** - Click to send an email of current logs manually according to the address and validation information set in Mail Settings.
- **Xóa bản ghi** - All the logs will be deleted from the Router permanently, not just from the page.

Click the **Tiếp** button to go to the next page, or click the **Trước** button to return to the previous page.

4.16.9 Thống kê

Choose menu “**Công cụ hệ thống** → **Thống kê**”, and then you can view the statistics of the Router, including total traffic and current traffic of the last Packets Statistic Interval.

Thông kê							
Trạng thái thống kê hiện tại:		Đã vô hiệu hóa		Kích hoạt			
Khoảng thời gian thống kê gói tin (5-60):		10	Giây	Làm mới			
		<input type="checkbox"/> Tự động làm mới					
Sắp xếp điều luật:		Sắp xếp theo số Byte hiện tại		Khôi phục tất cả		Xóa tất cả	
	Tổng	Hiện tại					Tùy chỉnh
Địa chỉ IP/ Địa chỉ MAC	Gói tin	Byte	Gói tin	Byte	ICMP Tx	UDP Tx	SYN Tx
Danh sách hiện tại đang trống.							
5	mục trên trang. Số thứ tự hiện tại						1
						trang	
				Trước		Tiếp	

Figure 4-87 Statistics

- **Trạng thái thống kê hiện tại** - Enable or Disable. The default value is disabled. To enable it, click the **Kích hoạt** button. If it is disabled, the function of DoS protection in Security settings will be disabled.
- **Khoảng thời gian thống kê gói tin (5-60)** - The default value is 10. Select a value between 5 and 60 seconds in the drop-down list. The Packets Statistic interval indicates the time section of the packets statistic.
- **Sắp xếp điều luật** - Choose how the displayed statistics are sorted.

Select the **Tự động làm mới** checkbox to refresh automatically.

Click the **Làm mới** button to refresh immediately.

Click **Khôi phục tất cả** to reset the values of all the entries to zero.

Click **Xóa tất cả** to delete all entries in the table.

Bảng thống kê:

Địa chỉ IP/MAC		The IP and MAC address are displayed with related statistics.
Tổng	Gói tin	The total number of packets received and transmitted by the Router.
	Byte	The total number of bytes received and transmitted by the Router.
Hiện tại	Gói tin	The total number of packets received and transmitted in the last Packets Statistic interval seconds.
	Byte	The total number of bytes received and transmitted in the last Packets Statistic interval seconds.
	ICMP Tx	The number of the ICMP packets transmitted to WAN per second at the specified Packets Statistics interval. It is shown like “current transmitting rate / Max transmitting rate”.
	UDP Tx	The number of UDP packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like “current transmitting rate / Max transmitting rate”.
	TCP SYN Tx	The number of TCP SYN packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like “current transmitting rate / Max transmitting rate”.
Tùy chỉnh	Khởi động lại	Reset the value of the entry to zero.
	Xóa	Delete the existing entry in the table.

There would be 5 entries on each page. Click **Trước** to return to the previous page and **Tiếp** to the next page.

Appendix A: FAQ

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

- 1) First, configure the ADSL Modem configured in RFC1483 bridge model.
- 2) Connect the Ethernet cable from your ADSL Modem to the WAN port on the Router. The telephone cord plugs into the Line port of the ADSL Modem.
- 3) Login to the Router, click the “Mạng” menu on the left of your browser, and click "WAN" submenu. On the WAN page, select “PPPoE/Russia PPPoE” for Dạng kết nối WAN. Type user name in the “Tên đăng nhập” field and password in the “Mật mã” field, type password in the “Xác nhận mật mã” field again, finish by clicking “Kết nối”.

The screenshot shows the WAN configuration interface. At the top, there is a dropdown menu for 'Dạng kết nối WAN' set to 'PPPoE/Russia PPPoE' and a 'Phát hiện' button. Below this, there are three input fields: 'Kết nối PPPoE:' (empty), 'Tên đăng nhập:' with the value 'username', and 'Mật mã:' with masked characters. At the bottom, there is another 'Xác nhận mật mã:' field with masked characters.

Figure A-1 PPPoE Connection Type

- 4) If your ADSL lease is in “pay-according-time” mode, select “Kết nối theo yêu cầu” or “Kết nối thủ công” for Chế độ kết nối. Type an appropriate number for Thời gian nghỉ tối đa” to avoid wasting paid time. Otherwise, you can select “Kết nối tự động” for Chế độ kết nối.

The screenshot shows the 'Chế độ kết nối' (Connection Mode) configuration page. It features four radio button options: 'Kết nối theo yêu cầu' (selected), 'Kết nối tự động', 'Kết nối dựa trên thời gian', and 'Kết nối thủ công'. The 'Kết nối theo yêu cầu' option has a 'Thời gian nghỉ tối đa' field set to '15' phút. The 'Kết nối dựa trên thời gian' option has a time range field set from '0 : 0 (HH:MM)' to '23 : 59 (HH:MM)'. At the bottom, there are three buttons: 'Kết nối' (highlighted in blue), 'Ngắt kết nối', and 'Đã ngắt kết nối!'.

Figure A-2 PPPoE Connection Mode

Note:

- i. Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.
- ii. If you are a Cable user, please configure the Router following the above steps.

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

- 1) Login to the Router, click the “Mạng” menu on the left of your browser, and click "WAN" submenu. On the WAN page, select “IP Động” for "Dạng kết nối WAN", finish by clicking “Lưu”.
- 2) Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable/DSL Modem during installation. If your ISP requires MAC register, login to the Router and click the "Mạng" menu link on the left of your browser, and then click "Bản sao MAC" submenu link. On the "Bản sao MAC" page, if your PC's MAC address is proper MAC address, click the "Sao địa chỉ MAC đến" button and your PC's MAC address will fill in the "Địa chỉ MAC WAN" field. Or else, type the MAC Address into the " Địa chỉ MAC WAN " field. The format for the MAC Address is XX-XX-XX-XX-XX-XX. Then click the "Lưu" button. It will take effect after rebooting.

Figure A-3 MAC Clone

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

- 1) If you start Netmeeting as a host, you don't need to do anything with the Router.
- 2) If you start as a response, you need to configure Server ảo or Máy chủ DMZ and make sure the H323 ALG is enabled.
- 3) How to configure Server ảo: Log in to the Router, click the “**Đang chuyển tiếp**” menu on the left of your browser, and click "**Servers ảo**" submenu. On the "**Servers ảo**" page, click **Thêm mới...** Then on the “**Thêm hoặc Tùy chỉnh một mục Server ảo**” page, enter “1720” for the “Cổng dịch vụ” blank, and your IP address for the “Địa chỉ IP” blank, taking 192.168.0.169 for an example, remember to **Kích hoạt** and **Lưu**.

STT	Cổng dịch vụ	Cổng trong	Địa chỉ IP	Giao thức	Trạng thái	Tùy chỉnh
1	21	21	192.168.0.100	Tắt cả	Đã kích hoạt	Tùy chỉnh Xóa

Figure A-4 Virtual Servers

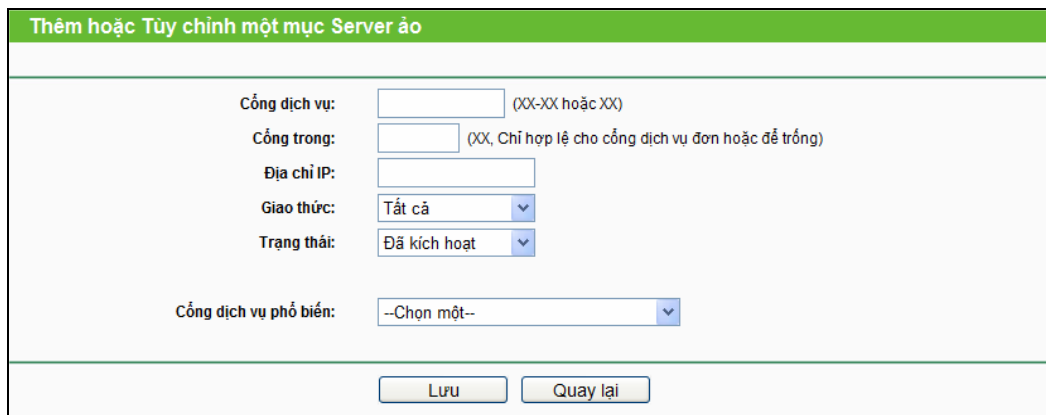


Figure A-5 Add or Modify a Virtual server Entry

 **Note:**

Your opposite side should call your WAN IP, which is displayed on the “Trạng thái” page.

- 4) How to enable DMZ Host: Log in to the Router, click the “**Đang chuyên tiếp**” menu on the left of your browser, and click “**DMZ**” submenu. On the “DMZ” page, click **Kích hoạt** radio button and type your IP address into the “Địa chỉ IP máy chủ DMZ” field, using 192.168.0.169 as an example, remember to click the **Lưu** button.

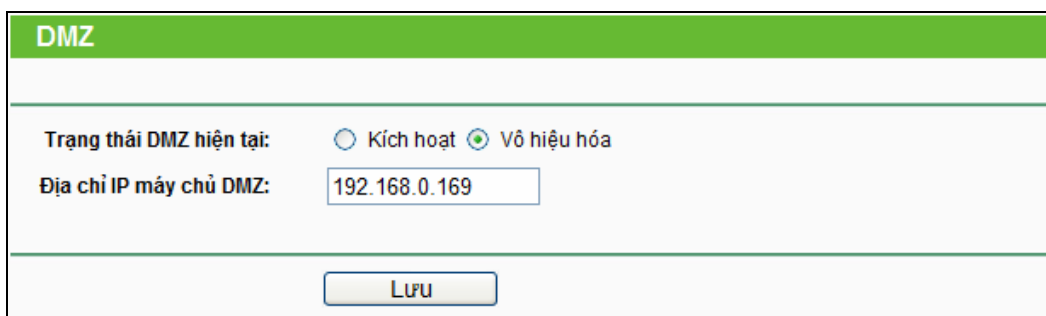


Figure A-6 DMZ

- 5) How to enable H323 ALG: Log in to the Router, click the “**Bảo mật**” menu on the left of your browser, and click “**Bảo mật cơ bản**” submenu. On the “**Bảo mật cơ bản**” page, check the **Kích hoạt** radio button next to **H323 ALG**. Remember to click the **Lưu** button.

Bảo mật cơ bản	
Tường lửa	
Tường lửa SPI:	<input checked="" type="radio"/> Kích hoạt <input type="radio"/> Vô hiệu hóa
VPN (Mạng riêng ảo)	
Truyền qua PPTP:	<input checked="" type="radio"/> Kích hoạt <input type="radio"/> Vô hiệu hóa
Truyền qua L2TP:	<input checked="" type="radio"/> Kích hoạt <input type="radio"/> Vô hiệu hóa
Truyền qua IPSec:	<input checked="" type="radio"/> Kích hoạt <input type="radio"/> Vô hiệu hóa
ALG	
FTP ALG:	<input checked="" type="radio"/> Kích hoạt <input type="radio"/> Vô hiệu hóa
TFTP ALG:	<input checked="" type="radio"/> Kích hoạt <input type="radio"/> Vô hiệu hóa
H323 ALG:	<input checked="" type="radio"/> Kích hoạt <input type="radio"/> Vô hiệu hóa
RTSP ALG:	<input checked="" type="radio"/> Kích hoạt <input type="radio"/> Vô hiệu hóa
<input type="button" value="Lưu"/>	

Figure A-7 Basic Security

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

- 1) 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.
- 2) To change the WEB management port number: Log in to the Router, click the “**Bảo mật**” menu on the left of your browser, and click “**Quản lý từ xa**” submenu. On the “**Quản lý từ xa**” page, type a port number except 80, such as 88, into the “**Cổng quản lý web**” field. Click **Lưu** and reboot the Router.

Quản lý từ xa	
Cổng quản lý web:	<input type="text" value="88"/>
Địa chỉ IP quản lý từ xa:	<input type="text" value="0.0.0.0"/> (Nhập 255.255.255.255 cho tất cả)
<input type="button" value="Lưu"/>	

Figure A-8 Remote Management

 **Note:**

If the above configuration takes effect, you can visit and configure the Router by typing <http://192.168.0.1:88> (the Router's LAN IP address: Web Management Port) in the address field of the Web browser. If the LAN IP of the modem connected with your router is 192.168.1.x, the default LAN IP of the Router will automatically switch from 192.168.0.1 to 192.168.1.1 to avoid IP conflict; in this case, please try <http://192.168.1.1:88>.

- 3) Log in to the Router, click the “**Đăng chuyển tiếp**” menu on the left of your browser, and click the “**Servers ảo**” submenu. On the “**Servers ảo**” page, click **Thêm mới...**, then on

the “**Thêm hoặc tùy chỉnh một mục Server ảo**” page, enter “80” into the blank next to the “**Cổng dịch vụ**”, and your IP address next to the “**Địa chỉ IP**”, assuming 192.168.0.169 for an example, remember to **Kích hoạt** and **Lưu**.

Server ảo						
STT	Cổng dịch vụ	Cổng trong	Địa chỉ IP	Giao thức	Trạng thái	Tùy chỉnh
1	80	80	192.168.0.169	Tất cả	Đã kích hoạt	Tùy chỉnh Xóa

Figure A-9 Virtual Servers

Thêm hoặc Tùy chỉnh một mục Server ảo	
Cổng dịch vụ:	<input type="text" value="80"/> (XX-XX hoặc XX)
Cổng trong:	<input type="text" value="80"/> (XX, Chỉ hợp lệ cho cổng dịch vụ đơn hoặc để trống)
Địa chỉ IP:	<input type="text" value="192.168.0.169"/>
Giao thức:	<input type="text" value="Tất cả"/>
Trạng thái:	<input type="text" value="Đã kích hoạt"/>
Cổng dịch vụ phổ biến:	<input type="text" value="--Chọn một--"/>

Figure A-10 Add or Modify a Virtual server Entry

5. The wireless stations cannot connect to the Router.

- 1) Make sure the "**Vô tuyến không dây**" 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 the 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 XP. 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) Click the **Network and Internet Connections** icon, and then click on the **Network Connections** tab in the appearing window.
- 3) Right click the icon that showed below, select Properties on the prompt page.

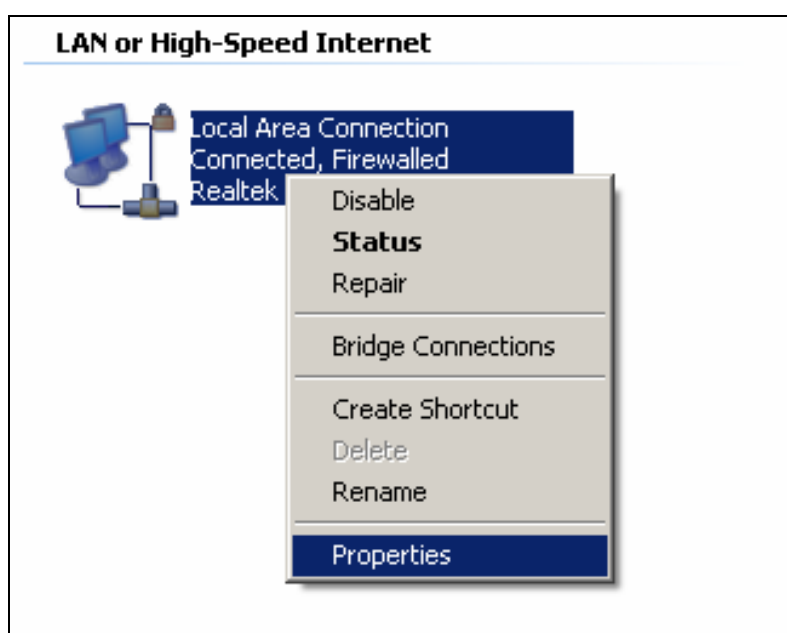


Figure B-1

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

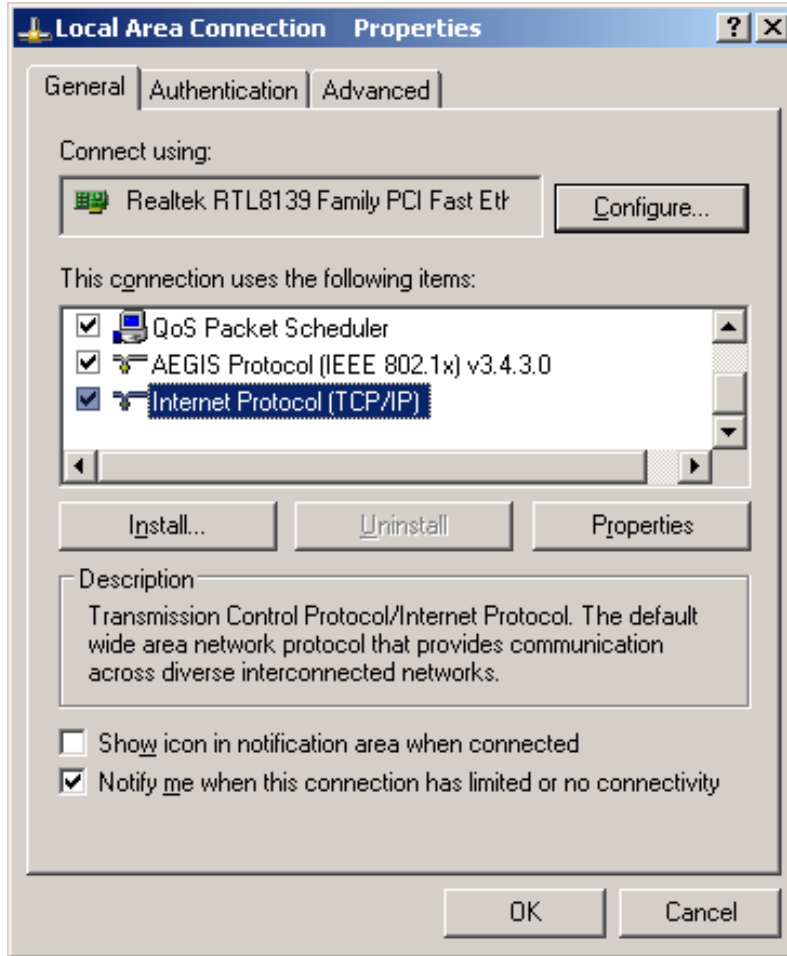


Figure B-2

- 5) The following **TCP/IP Properties** window will display and the **IP Address** tab is open on this window by default.

- 6) Select **Obtain an IP address automatically** and **Obtain DNS server automatically**, as shown in the Figure below:

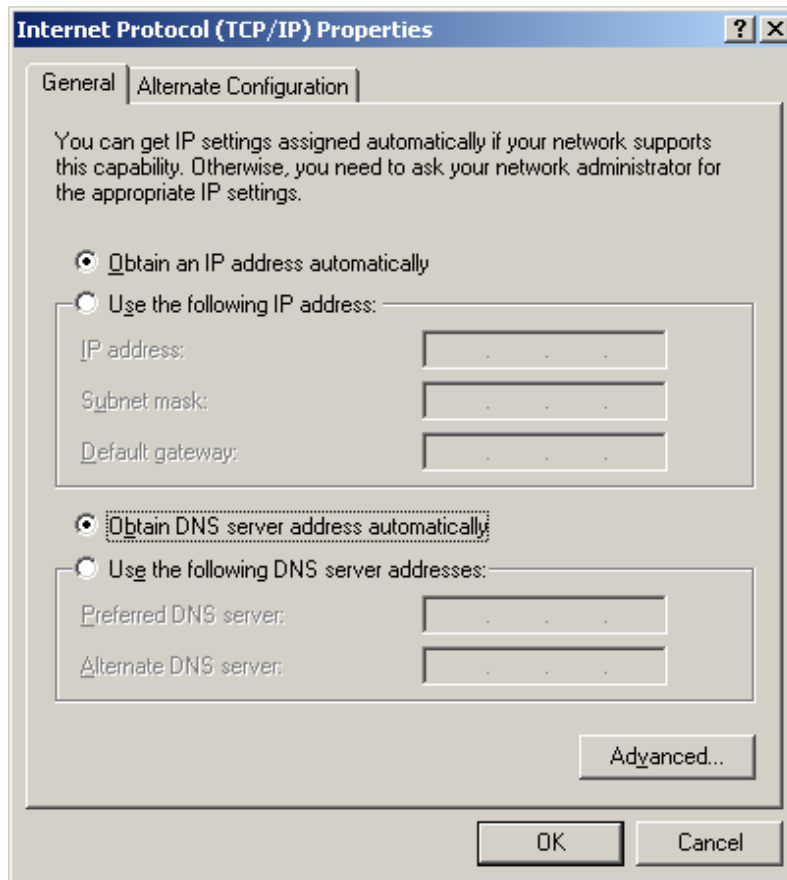


Figure B-3

Appendix C: Specifications

General	
Standards	IEEE 802.3, IEEE 802.3u, IEEE802.11n, IEEE802.11b, IEEE 802.11g
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
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)
LEDs	PWR, SYS, WLAN, WAN, LAN (1-4), QSS
Safety & Emissions	FCC, CE
Wireless	
Frequency Band*	2.4~2.4835GHz
Radio Data Rate	11n: up to 150Mbps (Automatic) 11g: 54/48/36/24/18/12/9/6M (Automatic) 11b: 11/5.5/2/1M (Automatic)
Frequency Expansion	DSSS(Direct Sequence Spread Spectrum)
Modulation	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Security	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK
Sensitivity @PER	130M: -68dBm@10% PER 108M: -68dBm@10% PER; 54M: -68dBm@10% PER 11M: -85dBm@8% PER; 6M: -88dBm@10% PER 1M: -90dBm@8% PER
Antenna Gain	5dBi
Environmental and Physical	
Temperature.	Operating : 0°C~40°C (32°F~104°F)
	Storage: -40°C~70°C(-40°F~158°F)
Humidity	Operating: 10% - 90% RH, Non-condensing
	Storage: 5% - 95% RH, Non-condensing

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

Appendix D: Glossary

- **802.11n** - 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) [3] was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- **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 PC(s) 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 System)** - An Internet Service that translates the names of websites into IP addresses.
- **Domain Name** - A descriptive name for an address or group of addresses on the Internet.
- **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 **S**ervice **S**et **I**dentification 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.

- **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 communicate with each other wirelessly, which network serving users are limited in a local area.