

**Netgear WNR612**  
**Wireless Router User Manual**

**V1.0**

# Contents

1	Safety Precautions .....	3
2	Overview .....	4
	2.1 Product Introduction .....	4
	2.2 Packing list .....	4
3	Hardware Description and Hardware Installation.....	5
	3.1 Front Panel and LED Status.....	5
	3.2 Rear Panel and Interface Description .....	6
	3.3 Hardware Installation.....	7
	3.3.1 System Requirements .....	7
	3.3.2 Before You Begin .....	8
	3.3.3 Connecting the Device .....	8
	3.4 Operation Range .....	9
	3.5 Roaming .....	9
4	TCP/IP Settings and Wireless Connection Introduction.....	11
	4.1 TCP/IP Settings.....	11
	4.2 Wireless Connection Introduction.....	15
5	Logging In to the Web Page.....	19
6	Web Configuration .....	21
	6.1 Language Selection.....	21
	6.2 Setup Wizard .....	21
	6.3 Add WPS Client.....	27
	6.4 Setup .....	29
	6.4.1 Basic Settings.....	29
	6.4.2 Wireless Settings .....	43
	6.4.3 Guest Network.....	48
	6.5 Content Filtering .....	50
	6.5.1 Logs .....	51
	6.5.2 Block Sites.....	51
	6.5.3 Block Services .....	53
	6.5.4 Schedule.....	56
	6.5.5 E-mail.....	58

---

6.6	Maintenance .....	59
6.6.1	Router Status .....	60
6.6.2	Attached Devices .....	64
6.6.3	Backup Settings .....	64
6.6.4	Set Password .....	65
6.6.5	Router Upgrade .....	66
6.7	Advanced Settings .....	67
6.7.1	Advanced Wireless Settings .....	68
6.7.2	Wireless Repeater .....	73
6.7.3	Port Forwarding/Port Triggering .....	74
6.7.4	WAN Setup .....	80
6.7.5	LAN Setup .....	82
6.7.6	QoS Setup .....	85
6.7.7	Dynamic DNS .....	92
6.7.8	Static Routes .....	93
6.7.9	Remote Management .....	95
6.7.10	UPnP .....	96
6.7.11	Traffic Meter .....	98
6.8	Web Support .....	100
6.9	Logout .....	101
7	Troubleshooting .....	102

## About User Manual

This user manual mainly describes how to install and configure the wireless router.

## Organization

This user manual is organized as follows:

Chapter	Description
Chapter 1 : Safety Precautions	Provides safety precaution information.
Chapter 2 : Overview	Provides a general overview of the wireless router, and the packing list.
Chapter 3 : Hardware Description and Hardware Installation	Mainly describes the front and rear panels of the wireless router and the procedure for hardware installation.
Chapter 4 : TCP/IP Settings and Wireless Connection Introduction	Describes how to set the TCP/IP and how to connect the wireless router wirelessly.
Chapter 5 : Logging In to the Web Page	Describes how to log in to the wireless router.
Chapter 6 : Web Configuration	Mainly describes how to navigate through the Web pages and how to configure the parameters.
Chapter 7 : Troubleshooting	Provides the troubleshooting information.

## Features

- Support IEEE802.11b, IEEE802.11b/g, and IEEE802.11b/gn
- Transmission data rate is up to 150 Mbps
- Support WEP and WPA for secure data transmission

- Support DHCP server
- Support manually configuration of static routing
- Support version upgrade through Web page
- Support restoring factory default settings
- Support demilitarized zone (DMZ)
- Support DNS proxy and forwarding
- Support QoS
- Support UPnP
- Support WPS
- Support port mapping
- Support port triggering
- Support wireless repeater
- Support guest network
- Support restricting IP bandwidth
- Support filtering by keyword and domain name
- Support wireless security authentication
- Support 5 types of WAN connection modes, including static IP, dynamic IP, PPPoE, PPTP, and L2TP
- Support remote access control
- Support firewall
- Support system status display
- Support backup and restoration of configuration file

## 1 Safety Precautions

Before operating the wireless router, read the following precaution information carefully:

- Use the type of power that user manual marks.
- Use the power adapter that is packed within the device package.
- Pay attention to the power load of the outlet or the prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid any damage caused by overheating to the device. The long and thin holes on the router are designed for heat dissipation, to ensure that the device works normally. Do not cover these cooling holes.
- Do not put this device close to a place where a heat source exists or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where is over damp or watery. Do not spill any liquid on this device.
- Do not connect this device to any PC or electronic product, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause any power or fire risk.
- Do not place this device on an unstable surface or support.

## 2 Overview

### 2.1 Product Introduction

The wireless router is a high-performance network access device. It is fully compatible with IEEE802.11b, IEEE802.11g and IEEE802.11n standards. It can provide reliable and convenient access service for individual users and SOHO (Small Office, Home Office).

### 2.2 Packing list

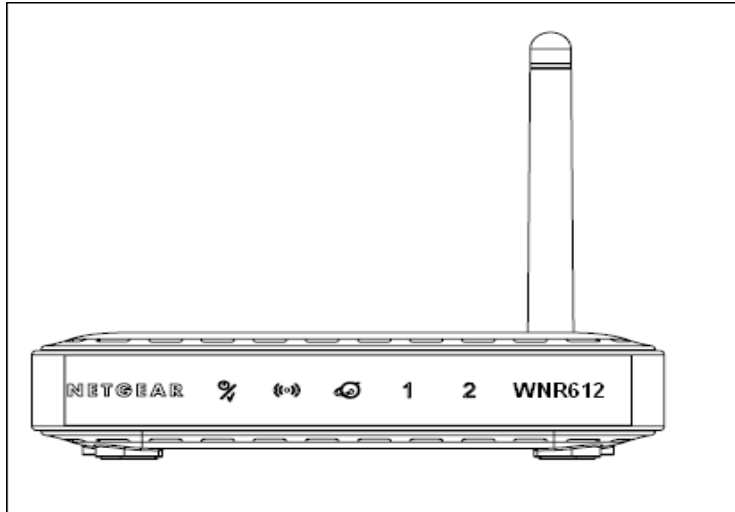
Please check whether your packing list includes the following items:

- Wireless router x 1
- Power adapter (5V DC,1A) x 1
- Network cable x1
- Quick Installation Guide x1
- Warranty card x1 (Optional)



### 3 Hardware Description and Hardware Installation

#### 3.1 Front Panel and LED Status


There are 5 LED indicators on the front panel of the wireless router. By observing their status, you can check whether the device runs normally.



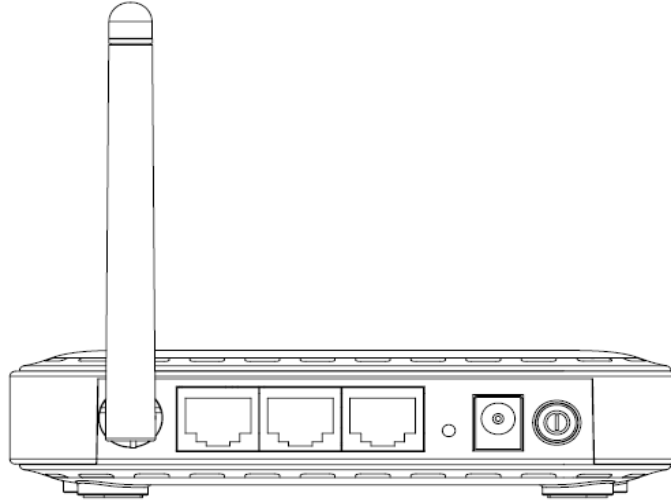
The following table describes the status of LED indicators on the front panel.

Indicator	Color	Status	Description
 Power	Green	On	Power is on.
	-	Off	Power is off or the device is down.
 WLAN	Green	On	Radio switch is turned on.
	Green	Blink	Data is being transmitted.
	-	Off	Radio switch is shut off.

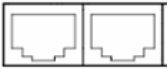






 Internet	Green	On	Connection succeeds.
	Green	Blink	Data is being transmitted.
	-	Off	No WAN connection.
1/2 LAN	Green	On	LAN connection succeeds.
	Green	Blink	Data is being transmitted.
	-	Off	No LAN connection.

### 3.2 Rear Panel and Interface Description



The following table describes interfaces and buttons on the rear panel.

Interface/Button	Description
	The first and second RJ45 interfaces are LAN interfaces, for connecting hub, switch, or computer in a LAN.

	The third RJ45 interface is WAN interface, for connecting WAN or the uplink network devices.
	Reset button. Press this button for 3 seconds and then release it, and then the wireless router reboots and restores to the factory defaults.
	Power socket, for connecting the power adapter (5V DC, 1A).
	Power switch

---

 **Caution:**

**Do not press Reset unless you want to clear the current settings. The Reset button is in a small circular hole on the rear panel. If you want to restore the default settings, please press the Reset button gently for 3 seconds with a fine needle inserted into the hole and then release the button. The system reboots and restores to the factory default settings.**

**The power specification is 5V DC, 1A. If the power adapter does not match the specification, the device may be damaged.**

---

### 3.3 Hardware Installation

#### 3.3.1 System Requirements

Before installing the device, please ensure that the following items are ready:

- At least one Ethernet RJ45 cable (10Base-T/100Base-T)
- One NETGEAR WNR612 wireless router
- A PC is already installed with the TCP/IP protocol and the PC can access the Internet.

### 3.3.2 Before You Begin

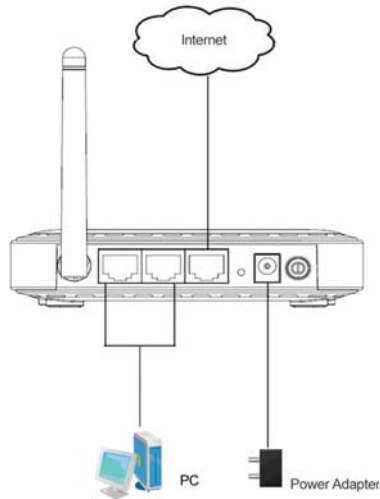
Before you install the device, please pay attention to the following items:

- When the device is connected to a computer, hub, router or switch, the Ethernet cable should be less than 100 meters.
- Do not place this device on an unstable surface or support. Do not put this device on the ground.
- Keep the device clean. Avoid the device from direct sunshine. Avoid any metal in the device.
- Place the device in the center of the area, and try to optimize the wireless coverage.

### 3.3.3 Connecting the Device

To connect the device, do as follows:

- Step 1** Connect one end of the RJ45 cable to the LAN interface of the wireless router.
- Step 2** Connect the other end of the RJ45 cable to your PC.
- Step 3** Connect the power adapter to the power socket of the wireless router.



### 3.4 Operation Range

The operation range of the wireless router depends on the actual environment. The path and effect of signal transmission vary according to the deployment in a house or an office. For example, the outdoor straight transmission distance for a certain device can be 300 meters and the indoor transmission distance can be 100 meters.

### 3.5 Roaming

Suppose that several wireless routers run in the same network. Each wireless router serves as a BSS that has its coverage range. One wireless client (for example, a notebook PC or PDA) can realize roaming from one AP to another AP accurately. In that case, the wireless client can communicate with the other devices within the coverage range of the wireless router.

To realize roaming in the coverage range of the wireless router by a wireless client, you need to set the APs properly as follows:

- Set the same SSID for different APs.
- The SSIDs of all the computers and PDAs should be consistent with that of APs.
- All the BSSs must use the same wireless channel.
- If the encryption function is enabled, all wireless routers must be configured with the same encryption mode and encryption key for establishing connection.
- Wireless routers must keep coverage of uninterrupted wireless signals in the whole operation environment. Hence, please put wireless routers to the appropriate places.

## 4 TCP/IP Settings and Wireless Connection Introduction

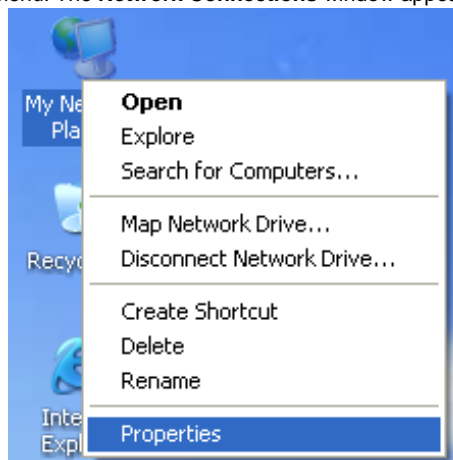
### 4.1 TCP/IP Settings

By default, the LAN IP address of the wireless router is 192.168.1.1, the subnet mask is 255.255.255.0, and the DHCP server is enabled.

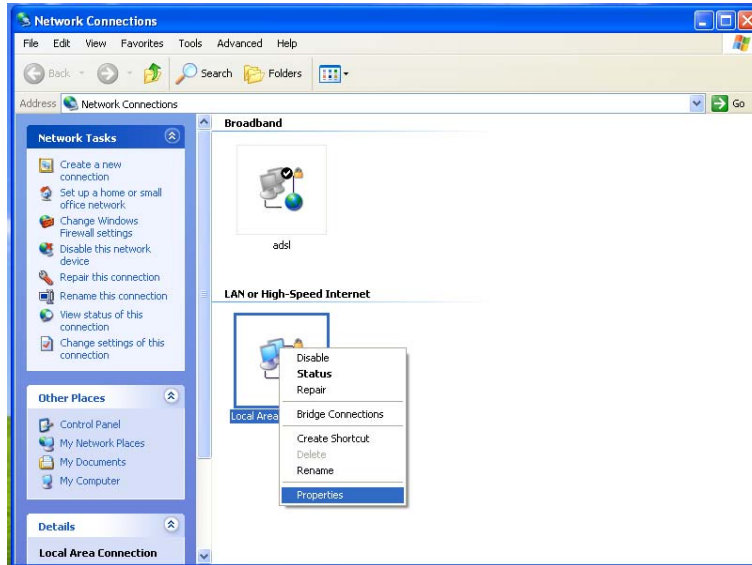
It is recommended to set the network adapter to **Obtain an IP address automatically**. Then, your PC obtains the TCP/IP settings, including the IP address, subnet mask, gateway, and DNS address automatically through the wireless router. If you know the settings of the current LAN interface, you can manually set the TCP/IP properties of the network adapter, so that your PC can communicate with the wireless router.

To manually set the network adapter, do as follows:

**Step 1** Right-click the icon of **My Network Places** and choose **Properties** from the menu. The **Network Connections** window appears.



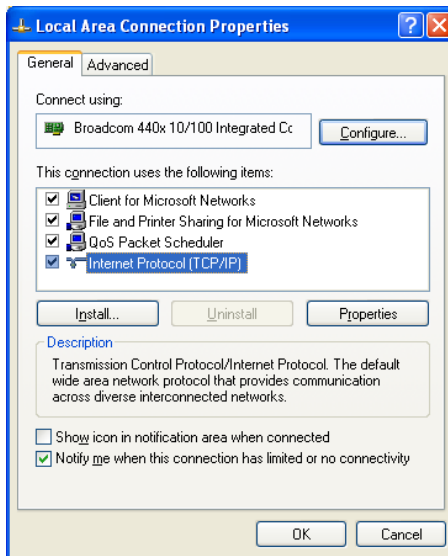
**Step 2** Right-click the network adapter icon and choose **Properties** from the menu. The **Local Area Connections Properties** window appears.



**Note:**

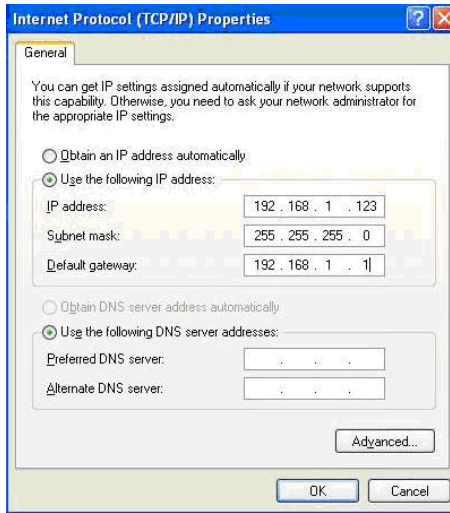
If multiple network cards are installed on your PC, a window other than the **Local Area Connections Properties** window may appear.

**Step 3** Double-click **Internet Protocol (TCP/IP)** and the **Internet Protocol (TCP/IP) Properties** window appears.

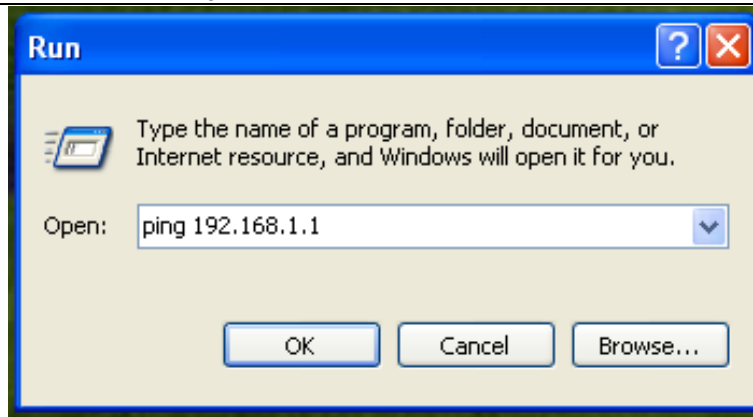


- Step 4** Select **Use the following IP address** and enter the IP address of the network adapter. The IP address must be 192.168. 1.X (X is a number in the range of 2 to 254). If you want to access the Internet through a wireless router, you need to enter the default gateway and IP address of the DNS server correctly.





- Step 5** Set the subnet mask and click **OK**.
- Step 6** After setting, you can ping the default IP address of the wireless router, to check whether the current connection between the PC and the wireless router is normal. Choose **Start > Run** from the desktop and enter **ping 192.168.1.1**. See the following figure:

**Note:**

**192.168.1.1** in the `ping` command is the default IP address of the LAN interface. If the IP address changes, enter the current IP address instead.

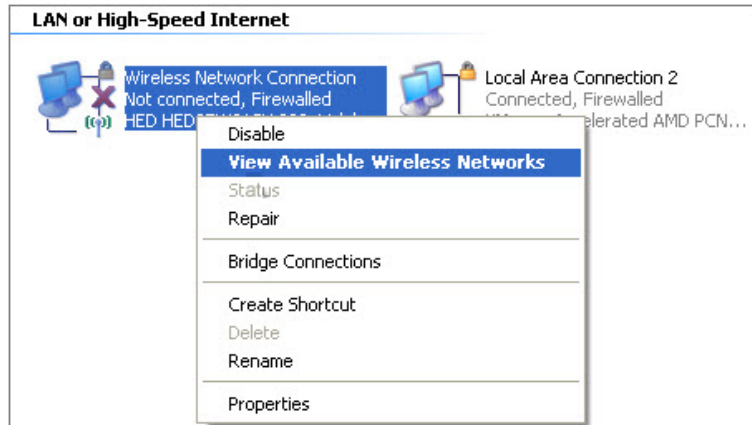
- Step 7** If the PC can ping through the default IP address of the wireless router, the following page appears, indicating that the connection between your PC and the wireless router is normal.

```
c:\WINDOWS\system32\ping.exe
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
```

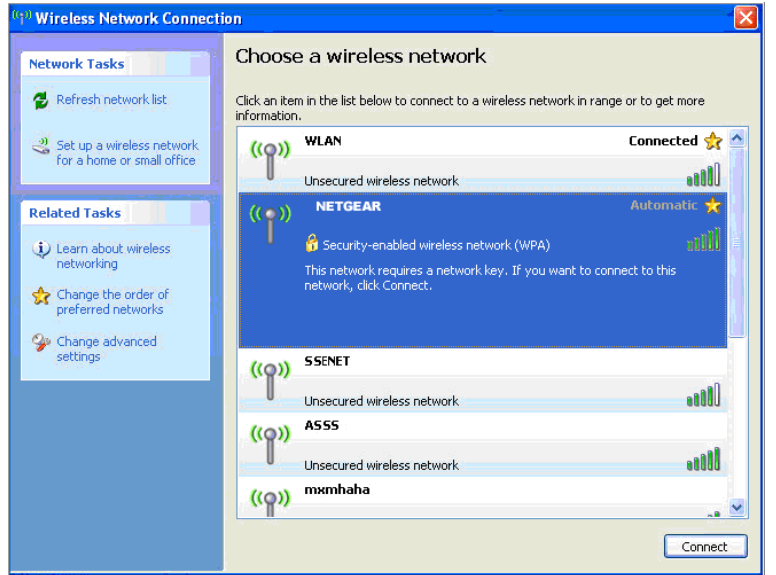
## 4.2 Wireless Connection Introduction

By default, the AP function of the wireless router is enabled. If you use a wireless network adapter, do as follows to establish the connection:

- Step 1** Enable the wireless network adapter on your PC and ensure that the **Wireless Zero Configuration** tool is available. Right-click the **Wireless Network Connection** icon and choose **View Available Wireless Networks** from the menu.



- Step 2** In the **Wireless Network Connection** page, click **Refresh network list** and the network list is refreshed. The default SSID of the wireless router is **NETGEAR**. Select the wireless router that you want to connect and click **Connect**. The default wireless security mode is **None**, and you can connect the wireless router directly without the encryption key in this mode. If the wireless router is encrypted, you need to enter the correct key to connect to the wireless router.



**Step 3** If you are not sure of the available SSID, please log in to the Web page of the wireless router, and view the SSID in the **Wireless Settings** page. For more information about the wireless settings, please refer to 6.4.2 Wireless Settings.

## Wireless Settings

### Region Selection

Region :

### Wireless Network

- Enable SSID Broadcast
- Enable Wireless Isolation

Name(SSID) :

Channel:

Mode :

### Security Options

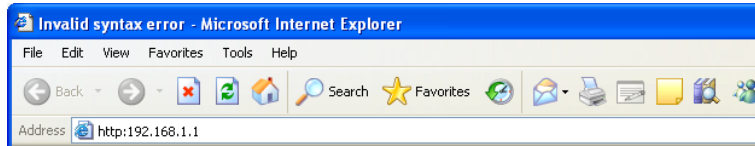
- None
- WEP
- WPA-PSK[TKIP]
- WPA2-PSK[AES]
- WPA-PSK[TKIP]+WPA2-PSK[AES]

### Note:

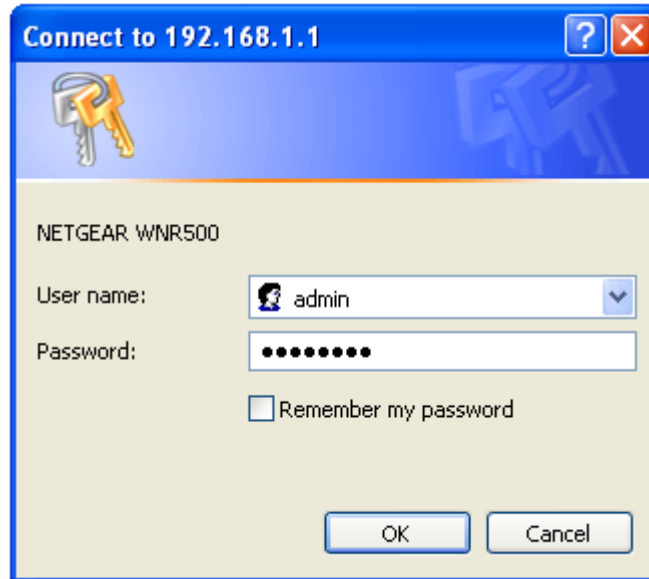
After your wireless network card connects to the wireless router successfully, usually, you should set the network adapter to **Obtain an IP address automatically**. The configuration of wireless connection is now complete.

## 5 Logging In to the Web Page

Run the Internet Explorer (IE), enter **http://192.168.1.1/** (the default IP address of the wireless router) in the address bar, and press **Enter**.



In the window that is displayed as shown in the following figure, enter the user name and password, and click **OK**.



 **Note:**

The default user name and password are **admin** and **admin** respectively.

After logging in to the Web page, you can view, configure and modify the router settings. To make the settings and changes take effect, you need to reboot the wireless router sometimes.

---

 **Caution:**

**If you are managing the wireless router through the Web page, do not cut off the power supply. Otherwise, the device may be damaged.**

---

## 6 Web Configuration

### 6.1 Language Selection

After successful login, you can select the appropriate language in the upper right corner of the page. After selecting a language and clicking **Apply**, the language setting takes effect immediately.



### 6.2 Setup Wizard

You can set the basic network parameters for accessing the Internet by following this wizard.

To configure the setup wizard, do as follows:

**Step 1** After login, click **Setup Wizard** in the navigation bar on the left pane of the page. The **Setup Wizard** page appears.

#### Setup Wizard

The Smart Setup Wizard Can Detect The Type Of Internet Connection That You Have. Do You Want The Smart Setup Wizard To Try And Detect The Connection Type Now?

- Yes.
- No. I Want To Configure The Router Myself.

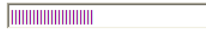
Next

If you are familiar with the router settings, you can select **No. I Want To Configure The Router Myself**. If you want to follow this wizard to configure the router, please select **Yes** and click **Next**. The router automatically detects the WAN connection mode.



## Setup Wizard

---



Detecting Connection Type on Internet Port.

---

Please wait a moment ...

### Note:

If you do not insert the network cable into the WAN interface of the wireless router, the previous page does not appear.

**Step 2** The broadband type can be **Dynamic IP (DHCP)**, **Static IP (Fixed)**, **PPPoE**, or **PPTP**.

- (1) If the detected Internet type is **Dynamic IP (DHCP)**, the following figure appears:

### Dynamic IP (DHCP) detected

---

Successfully detected the type of Internet connection you have.

---

Click **Next** and the following figure appears:

### Dynamic IP Address

---

Account Name (If Required)

---

Enter the account name provided by the Internet service provider (ISP) in the **Account Name** field. If the ISP does not provide it, you need not modify it.

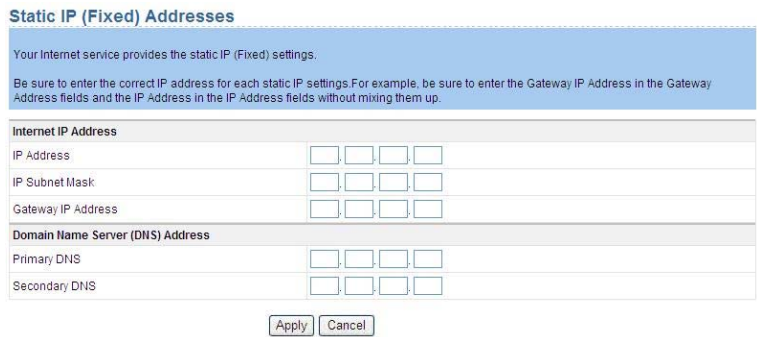
In this mode, the WAN port of the wireless router obtains the network property information, including the IP address, subnet mask, gateway, and IP address of the DNS server, from the connected DHCP server

After setting, click **Apply** to save the settings, and then the **Router Status** page appears. You can view the parameters of WAN connection type in this page. The setup wizard is now complete.

- (2) If the detected Internet type is **Static IP (Fixed)**, the following figure appears:



Click **Next** and the following figure appears:

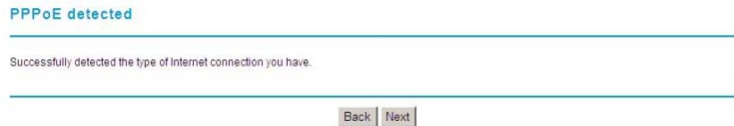


The following table describes parameters in this page:

Field	Description
IP Address	Enter the IP address of the WAN interface.
IP Subnet Mask	Subnet mask of the WAN IP address. It is usually 255.255.255.0.
Gateway IP Address	Enter the IP address of the gateway if necessary.
Primary DNS	Enter the IP address of the primary DNS server if necessary.
Secondary DNS	If the ISP provides another DNS server, enter the IP address of that DNS server.

After setting, click **Apply** to save the settings, and then the **Router Status** page appears. You can view the parameters of WAN connection type in this page. The setup wizard is now complete.

(3) If the detected Internet type is **PPPoE**, the following figure appears:



Click **Next** and the following figure appears:



The following table describes parameters in this page:

Field	Description
Login	Enter the user name provided by the ISP.
Password	Enter the password provided by the ISP.
Service Name (If required)	Enter the service name provided by the ISP. If the ISP does not provide it, you need not enter any information.
Domain Name Server (DNS) Address	Select <b>Use These DNS Servers</b> and enter the IP address information of the DNS server provided by the ISP. If no DNS server information is available, select <b>Get Automatically From ISP</b> .
Primary DNS	Enter the IP address of the primary DNS server if necessary.
Secondary DNS	If the ISP provides another DNS server, enter the IP address of that DNS server.

 **Note:**

The user name and password are case-sensitive. If you have any question about the user name and password, contact your ISP.

After setting, click **Apply** to save the settings, and then the **Router Status** page appears. You can view the parameters of WAN connection type in this page. The setup wizard is now complete.

(4) If the detected Internet type is PPTP, the following figure appears:

**PPTP detected**

---

Successfully detected the type of Internet connection you have.

---

[Back](#) [Next](#)

Click **Next** and the following figure appears:

**PPTP**

---

Username

Password

Idle time(minutes)

My IP Address

Server IP Address

Gateway IP Address

---

The following table describes parameters in this page:

Field	Description
Username	Enter the PPTP user name provided by the ISP.
Password	Enter the PPTP password provided by the ISP.
Idle Timeout (In minutes)	Set the idle timeout. If the system does not detect any Internet access behavior within the set time of idle timeout, the system interrupts the Internet connection.
My IP Address	Enter the IP address provided by the ISP (User needs to manually set this IP address).
Server IP Address	Enter the PPTP server IP address.
Gateway IP Address	Enter the gateway IP address.

After setting, click **Apply** to save the settings, and then the **Router Status** page appears. You can view the parameters of WAN connection type in this page. The setup wizard is now complete.

## 6.3 Add WPS Client

Click **Add WPS Client** on the left pane of the page to display the following page.

### Add WPS Client

---

#### New and easy way to connect to the Wireless Router via WiFi Protected setup (WPS)

A wireless client has to support WPS function in order to use this wizard to add the client to your WPS enabled Wireless Router.

Please check the user manual and gift box of your wireless client to see whether it supports the WPS function. If your wireless client does not support the WPS function, you have to configure your wireless client manually so it has the same SSID and wireless security settings as on this router.

---

Next

WPS refers to Wi-Fi Protected Setup. You can use the WPS setup function to add a wireless client to a network, without setting specific parameters, such as SSID, security mode, and password. To use this function, a wireless client must support WPS. If the wireless client does not support WPS, you must manually configure the wireless client to ensure that it has consistent SSID and wireless security settings with the router. There are two WPS modes: Push Button and PIN.

Click **Next** to select the WPS mode.

- Push Button mode

### Add WPS Client

---


#### Select a setup method:

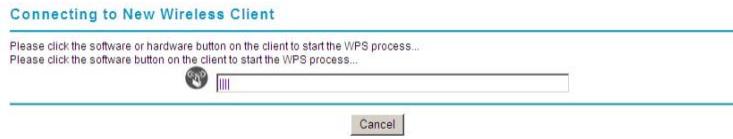
- Push Button (recommended)

You can either press the Push Button physically on the router or press the Button below (soft Push Button).



- PIN (Personal Identification Number)
-

Select **Push Button (recommended)** and click  on the router and the following page appears:



Press the button on the network card or click the button in the software page within two minutes to start WPS connection. After WPS connection is established, the following page appears. The client can now visit the LAN.



● **PIN mode**



Select PIN (Personal Identification Number) and enter the PIN of the network (refer to the client of the network card), then click **Next** to start WPS connection. The following page appears:

Connecting to New Wireless Client

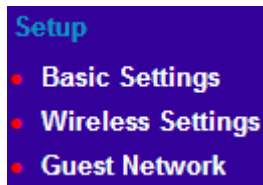


Click the PIN button on the client of the network card within two minutes to start WPS connection. After WPS connection is established, the following page appears. The client can now visit the LAN.



## 6.4 Setup

Click **Setup** and the extended navigation menu is shown as follows:



The submenu contains **Basic Settings**, **Wireless Settings**, and **Cuest Network**.

### 6.4.1 Basic Settings

Click **Basic Settings** on the left pane of the page to display the following page.



**Basic Settings**

Does your Internet Connection Required A Login?

- Yes
- No

Account Name (If Required)

Domain Name (If Required)

**Internet IP Address**

- Get Dynamically From ISP
- Use Static IP Address

IP Address

IP Subnet Mask

Gateway IP Address

**Domain Name Server (DNS) Address**

- Get Automatically From ISP
- Use These DNS Servers

Primary DNS

Secondary DNS

**Router MAC Address**

- Use Default Address
- Use Computer MAC Address
- Use This MAC Address

The router supports 5 modes of Internet connection, including **Dynamic IP (DHCP)**, **Static IP (Fixed)**, **PPPoE**, **PPTP**, and **L2TP**. In this page, you can select the appropriate Internet connection mode and configure the relevant parameters according to the actual requirements.

- Dynamic IP (DHCP)

If you select Dynamic IP (DHCP), the router automatically obtains IP address, subnet mask, and IP address of the gateway from the ISP. If the ISP does not provide any IP network parameters, please select this mode. See the following figure:

**Basic Settings**

---

Does your Internet Connection Required A Login?

Yes

No

---

Account Name (If Required)

Domain Name (If Required)

---

Internet IP Address

Get Dynamically From ISP

Use Static IP Address

IP Address

IP Subnet Mask

Gateway IP Address

---

Domain Name Server (DNS) Address

Get Automatically From ISP

Use These DNS Servers

Primary DNS

Secondary DNS

---

Router MAC Address

Use Default Address

Use Computer MAC Address

Use This MAC Address

---

The following table describes parameters in this page:

Field	Description
-------	-------------

Field	Description
Does your Internet Connection Require A Login?	Select <b>No</b> .
Account Name (If Required)	Enter the account name provided by the ISP. If the ISP does not provide it, you need not modify it.
Domain Name (If Required)	Enter the domain name provided by the ISP. If the ISP does not provide it, you need not modify it.
Internet IP Address	Select <b>Get Dynamically From ISP</b> .
Domain Name Server Address (DNS)	Enter the IP address of the DNS server provided by the ISP. If the ISP does not provide it, select <b>Get Automatically From ISP</b> .
Router MAC Address	Physical address of the router. Normally, you can select <b>Use Default Address</b> . If the ISP requires MAC address authentication, select <b>Use Computer MAC Address</b> or <b>Use This MAC Address</b> . If you select <b>Use Computer MAC Address</b> , the MAC address of the current computer serves as the MAC address of the router. If you select <b>Use This MAC Address</b> , you need to enter the MAC address of another computer. The format of a MAC address is XX:XX:XX:XX:XX:XX.

After setting, click **Apply** to save the settings.

- Static IP (Fixed)

If the ISP provides the information of the IP address, subnet mask, gateway, and DNS server, select **Static IP (Fixed)**. For detailed settings, refer to your ISP.

**Basic Settings**

Does your Internet Connection Require A Login?

- Yes
- No

Account Name (If Required)

Domain Name (If Required)

**Internet IP Address**

- Get Dynamically From ISP
- Use Static IP Address

IP Address

IP Subnet Mask

Gateway IP Address

**Domain Name Server (DNS) Address**

- Get Automatically From ISP
- Use These DNS Servers

Primary DNS

Secondary DNS

**Router MAC Address**

- Use Default Address
- Use Computer MAC Address
- Use This MAC Address

The following table describes parameters in this page:

Field	Description
Does your Internet Connection Require A Login?	Select <b>No</b> .
Account Name (If	Enter the host name provided by the ISP. If the ISP does not

Field	Description
Required)	provide it, you need not modify it.
Domain Name (If Required)	Enter the domain name provided by the ISP. If the ISP does not provide it, you need not modify it.
Internet IP Address	Select <b>Use Static IP Address</b> .
IP Address	Enter the WAN IP address provided by the ISP. It cannot be null.
IP Subnet Mask	Enter the WAN subnet mask provided by the ISP. It varies depending on the network type. It is usually 255.255.255.0 (Class C).
Gateway IP Address	Enter the IP address of the gateway provided by the ISP. It is the IP address used for connecting to the ISP.
Domain Name Server (DNS) Address	Select <b>Use These DNS Servers</b> .
Primary DNS	Enter the IP address of the primary DNS server if necessary.
Secondary DNS	If the ISP provides another DNS server, enter the IP address of that DNS server.
Router MAC Address	Physical address of the router. Normally, you can select <b>Use Default Address</b> . If the ISP requires MAC address authentication, select <b>Use Computer MAC Address</b> or <b>Use This MAC Address</b> . If you select <b>Use Computer MAC Address</b> , the MAC address of the current computer serves as the MAC address of the router. If you select <b>Use This MAC Address</b> , you need to enter the MAC address of another computer. The format of a MAC address is XX:XX:XX:XX:XX:XX.

After setting, click **Apply** to save the settings.

- PPPoE

If the ISP provides the user name and password for PPPoE dialup, select **PPPoE**.

**Basic Settings**

Does your Internet Connection Required A Login?

- Yes
- No

Internet Service Provider

PPPoE

Login

Password

Service Name (If Required)

Connection Mode

Dial On Demand

Idle Timeout (In minutes)

Internet IP Address

- Get Dynamically From ISP
- Use Static IP Address

IP Address

 .  .  . 

Domain Name Server (DNS) Address

- Get Automatically From ISP
- Use These DNS Servers

Primary DNS

 .  .  . 

Secondary DNS

 .  .  . 

Router MAC Address

- Use Default Address
- Use Computer MAC Address
- Use This MAC Address

Apply Cancel

The following table describes parameters in this page:

Field	Description
Does your Internet Connection	Select <b>Yes</b> .

Field	Description
Require A Login?	
Internet Service Provider	Select <b>PPPoE</b> .
Login	Enter the user name for PPPoE dialup provided by the ISP.
Password	Enter the password for PPPoE dialup provided by the ISP.
Service Name (If Required)	If several PPPoE servers are available, specify one in this field.
Connection Mode	<ul style="list-style-type: none"> <li>● <b>Dial On Demand:</b> If you select it, the system automatically establishes a connection when a network access request from the LAN is received. If no network access request is sent from the LAN within the set time of <b>Idle Timeout</b>, the system automatically interrupts the connection. If you pay for Internet access by time, you are recommended to use this connection mode, which effectively saves the expense of Internet access.</li> <li>● <b>Always On:</b> If you select it, the system automatically establishes a connection. If the network is disconnected because of external factors when you are using the Internet access service, the system tries connection every certain time (for example, 10 seconds) until the connection is established. If you pay for Internet access in the monthly fee mode, you are recommended to use this connection mode.</li> <li>● <b>Manually Connect:</b> If you select it, you need to manually set dialup connection after startup.</li> </ul>
Idle Timeout (In minutes)	If the system does not detect any Internet access behavior within the set time of idle timeout, the system interrupts the Internet connection.
Internet IP Address	You may select <b>Get Dynamically From ISP</b> or <b>Use Static IP Address</b> . If you select <b>Use Static IP Address</b> , you need to manually enter the IP address.

Field		Description
Domain Server Address	Name (DNS)	Enter the DNS address provided by the ISP. If the ISP does not provide it, select <b>Get Automatically From ISP</b> .
Router Address	MAC	Physical address of the router. Normally, you can select <b>Use Default Address</b> . If the ISP requires MAC address authentication, select <b>Use Computer MAC Address</b> or <b>Use This MAC Address</b> . If you select <b>Use Computer MAC Address</b> , the MAC address of the current computer serves as the MAC address of the router. If you select <b>Use This MAC Address</b> , you need to enter the MAC address of another computer. The format of a MAC address is XX:XX:XX:XX:XX:XX.

After setting, click **Apply** to save the settings.

- PPTP

If the ISP provides the user name and password for PPTP dialup, select **PPTP**.



**Basic Settings**

Does your Internet Connection Required A Login?

- Yes
- No

Internet Service Provider

PPTP

Login

Password

Connection Mode

Dial On Demand

Idle Timeout (In minutes)

5

My IP Address

 .  .  . 

Subnet Mask

 .  .  . 

Server Address

Gateway IP Address

 .  .  . 

Connection ID/Name

Domain Name Server (DNS) Address

- Get Automatically From ISP
- Use These DNS Servers

Primary DNS

 .  .  . 

Secondary DNS

 .  .  . 

Router MAC Address

- Use Default Address
- Use Computer MAC Address
- Use This MAC Address

00:1E:E3:DA:95:B0

Apply Cancel

The following table describes parameters in this page:

Field	Description
Does your Internet Connection Require A Login?	Select <b>Yes</b> .
Internet Service Provider	Select <b>PPTP</b> .
Login	Enter the user name for PPTP dialup provided by the ISP.
Password	Enter the password for PPTP dialup provided by the ISP.
Service Name	If several PPPoE servers are available, specify one in this field.
Connection Mode	<ul style="list-style-type: none"> <li>● <b>Dial On Demand:</b> If you select it, the system automatically establishes a connection when a network access request from the LAN is received. If no network access request is sent from the LAN within the set time of <b>Idle Timeout</b>, the system automatically interrupts the connection. If you pay for Internet access by time, you are recommended to use this connection mode, which effectively saves the expense of Internet access.</li> <li>● <b>Always On:</b> If you select it, the system automatically establishes a connection. If the network is disconnected because of external factors when you are using the Internet access service, the system tries connection every certain time (for example, 10 seconds) until the connection is established. If you pay for Internet access in the monthly fee mode, you are recommended to use this connection mode.</li> <li>● <b>Manually Connect:</b> If you select it, you need to manually set dialup connection after startup.</li> </ul>
Idle Timeout (In minutes)	If the system does not detect any Internet access behavior within the set time of idle timeout, the system interrupts the Internet connection.
My IP Address	Enter the IP address provided by the ISP (User needs to

Field	Description
	manually set this IP address).
Subnet Mask	Enter the subnet mask of the IP address provided by the ISP.
Server Address	Enter the PPTP server address.
Gateway IP Address	Enter the gateway IP address.
Connection ID/Name	Specify the connection name.
Domain Name Server Address	Enter the DNS address provided by the ISP. If the ISP does not provide it, select <b>Get Automatically From ISP</b> .
Router MAC Address	Physical address of the router. Normally, you can select <b>Use Default Address</b> . If the ISP requires MAC address authentication, select <b>Use Computer MAC Address</b> or <b>Use This MAC Address</b> . If you select <b>Use Computer MAC Address</b> , the MAC address of the current computer serves as the MAC address of the router. If you select <b>Use This MAC Address</b> , you need to enter the MAC address of another computer. The format of a MAC address is XX:XX:XX:XX:XX:XX.

After setting, click **Apply** to save the settings.

- L2TP

If the ISP provides the user name and password for L2TP dialup, select **L2TP**.

**Basic Settings**

Does your Internet Connection Required A Login?

- Yes
- No

Internet Service Provider

L2TP

Login

Password

Connection Mode

Dial On Demand

Idle Timeout (In minutes)

My IP Address

 .  .  . 

Subnet Mask

 .  .  . 

Server Address

Gateway IP Address

 .  .  . 

Domain Name Server (DNS) Address

- Get Automatically From ISP
- Use These DNS Servers

Primary DNS

 .  .  . 

Secondary DNS

 .  .  . 

Router MAC Address

- Use Default Address
- Use Computer MAC Address
- Use This MAC Address

Apply Cancel

The following table describes parameters in this page:

Field	Description
Does your Internet Connection	Select <b>Yes</b> .

Field	Description
Require A Login?	
Internet Service Provider	Select <b>PPTP</b> .
Login	Enter the user name for PPTP dialup provided by the ISP.
Password	Enter the password for PPTP dialup provided by the ISP.
Connection Mode	<ul style="list-style-type: none"> <li>● <b>Dial On Demand:</b> If you select it, the system automatically establishes a connection when a network access request from the LAN is received. If no network access request is sent from the LAN within the set time of <b>Idle Timeout</b>, the system automatically interrupts the connection. If you pay for Internet access by time, you are recommended to use this connection mode, which effectively saves the expense of Internet access.</li> <li>● <b>Always On:</b> If you select it, the system automatically establishes a connection. If the network is disconnected because of external factors when you are using the Internet access service, the system tries connection every certain time (for example, 10 seconds) until the connection is established. If you pay for Internet access in the monthly fee mode, you are recommended to use this connection mode.</li> <li>● <b>Manually Connect:</b> If you select it, you need to manually set dialup connection after startup.</li> </ul>
Idle Timeout (In minutes)	If the system does not detect any Internet access behavior within the set time of idle timeout, the system interrupts the Internet connection.
My IP Address	Enter the IP address provided by the ISP (User needs to manually set this IP address).
Subnet Mask	Enter the subnet mask of the IP address provided by the ISP.
Server Address	Enter the L2TP server address.

Field		Description
Gateway Address	IP	Enter the gateway IP address.
Domain Server Address	Name (DNS)	Enter the DNS address provided by the ISP. If the ISP does not provide it, select <b>Get Automatically From ISP</b> .
Router Address	MAC	Physical address of the router. Normally, you can select <b>Use Default Address</b> . If the ISP requires MAC address authentication, select <b>Use Computer MAC Address</b> or <b>Use This MAC Address</b> . If you select <b>Use Computer MAC Address</b> , the MAC address of the current computer serves as the MAC address of the router. If you select <b>Use This MAC Address</b> , you need to enter the MAC address of another computer. The format of a MAC address is XX:XX:XX:XX:XX:XX.

After setting, click **Apply** to save the settings.

#### 6.4.2 Wireless Settings

Click **Wireless Settings** on the left pane of the page to display the following page.

**Wireless Settings**

---

**Region Selection**  
 Region :

---

**Wireless Network**  
 Enable SSID Broadcast  
 Enable Wireless Isolation  
 Name(SSID) :   
 Channel:   
 Mode :

---

**Security Options**  
 None  
 WEP  
 WPA-PSK[TKIP]  
 WPA2-PSK[AES]  
 WPA-PSK[TKIP]+WPA2-PSK[AES]

---

In this page, you can configure the basic wireless parameters.

The following table describes parameters in this page:

Field	Description
Region	Select the region where you are in from the drop-down list.
Enable SSID Broadcast	Enable or disable SSID broadcast. If it is enabled, the router broadcasts its SSID in the wireless network. In this way, wireless clients can find the SSID after scanning and join the corresponding wireless network.
Enable Wireless Isolation	Enable or disable wireless isolation. If it is selected, wireless clients that use this SSID can access the Internet, but cannot communicate with other wireless clients, Ethernet clients, or other devices.
Name (SSID)	Network name. The SSID can contain up to 32 characters and can be letters, numerals, underlines, and any

Field	Description
	combinations of them. The SSID is case-sensitive.
Channel	Select the working channel of the wireless network. The default is <b>Auto</b> , which indicates that the wireless router automatically searches for the best channel in the available channels.
Mode	The drop-down list displays all the supported data rate. Please select one as the maximum transmission data rate.
Security Options	Set the security encryption of the wireless network, to prevent unauthorized access and listening. You can select <b>None</b> , <b>WEP</b> , <b>WPA-PSK (TKIP)</b> , <b>WPA2-PSK (AES)</b> , or <b>WPA-PSK (TKIP) + WPA2-PSK (AES)</b> . The following describes the settings in detail.

### Security Options

- None: Data encryption is not adopted and the network is not secure. Any station can access the network. This option is not recommended.

#### Security Options

- None  
 WEP  
 WPA-PSK[TKIP]  
 WPA2-PSK[AES]  
 WPA-PSK[TKIP]+WPA2-PSK[AES]

Apply Cancel

- WEP: Wired equivalent privacy. You can encrypt the data with WEP 64 bits or 128 bits.



**Security Encryption(WEP)**

Authentication Type:

Encryption Strength:

---

**Security Encryption(WEP) Key**

Passphrase:

Key 1:

Key 2:

Key 3:

Key 4:

---

The following table describes parameters related to the WEP mode:

Field	Description
Authentication Type	You can select <b>Automatic</b> or <b>Shared Keys</b> . The default is <b>Automatic</b> .
Encryption Strength	Select the encryption strength of WEP. You can select <b>64-bit</b> or <b>128-bit</b> .
Passphrase	Enter a word or a string of printable characters, and click <b>Generate</b> button. The wireless router automatically generates four WEP keys. User may select one as the encryption key of wireless network.
Key 1/2/3/4	Select one from the four keys and enter the corresponding WEP key in the field. If the <b>Encryption Strength</b> is set to <b>64-bit</b> , enter 10 hexadecimal digits. The key can be any combination of 0-9 and A-F. If the <b>Encryption Strength</b> is set to <b>128-bit</b> , enter 26 hexadecimal digits. The key can be any combination of 0-9 and A-F.

- WPA-PSK (TKIP): Preshared key Wi-Fi protection access. It uses WPA-PSK standard encryption and Temporal Key Integrity Protocol (TKIP). TKIP has stronger encryption mechanism and integrates message integrity code (MIC) to protect against attacks of hackers.

Security Options

- None
- WEP
- WPA-PSK[TKIP]
- WPA2-PSK[AES]
- WPA-PSK[TKIP]+WPA2-PSK[AES]

Security Options(WPA-PSK)

PassPhrase :  (8-63 characters or 64 hex digits)

The following table describes parameters related to the WPA-PSK (TKIP) mode:

Field	Description
PassPhrase	Enter 8-63 characters or 64 hexadecimal digits.

- WPA2-PSK (AES): Preshared key Wi-Fi protection access version 2. It uses WPA2-PSK standard encryption and Advanced Encryption Standard (AES). AES uses symmetric 128 bits block data to encrypt.

Security Options

- None
- WEP
- WPA-PSK[TKIP]
- WPA2-PSK[AES]
- WPA-PSK[TKIP]+WPA2-PSK[AES]

Security Options(WPA2-PSK)

PassPhrase :  (8-63 characters or 64 hex digits)

The following table describes parameters related to the WPA2-PSK (AES) mode:

Field	Description
PassPhrase	Enter 8-63 characters or 64 hexadecimal digits.

- WPA-PSK (TKIP) + WPA2-PSK (AES): It allows the client to use WPA-PSK (TKIP) or WPA2-PSK (AES).

Security Options--Profile 1

- None
- WEP
- WPA-PSK[TKIP]
- WPA2-PSK[AES]
- WPA-PSK[TKIP]+WPA2-PSK[AES]

Security Options(WPA-PSK+WPA2-PSK)

PassPhrase :  (8-63 characters or 64 hexdigits)

The following table describes parameters related to the WPA-PSK (TKIP) + WPA2-PSK (AES) mode:

Field	Description
PassPhrase	Enter 8-63 characters or 64 hexadecimal digits.

**Note:**

After wireless setting is complete on the router, a host in the wireless network must have consistent wireless settings, including the SSID, with the router if the host wants to connect to the router. If the router has security settings, the host in the wireless network must have consistent security settings. For example, the passwords set on the host and the router must be the same. Otherwise, the host cannot connect to the router.

### 6.4.3 Guest Network

If you enable guest network, a visitor can use Internet connection in your home without knowing your wireless password.

Click **Guest Network** on the left pane of the page to display the following page.

**Guest Network Settings**

---

**Network Profiles**

	Scheme	SSID	Security	Apply	SSID Broadcast
<input checked="" type="radio"/>	1	NetGear-002	None	NO	YES
<input type="radio"/>	2	NetGear-003	None	NO	YES
<input type="radio"/>	3	NetGear-004	None	NO	YES
<input type="radio"/>	4	NetGear-005	None	NO	YES

---

**Wireless Settings--Profile 1**

Enable Guest Network

Enable SSID Broadcast

Allow Guest to access My Local Network

Enable Wireless Isolation

Guest Wireless Network Name(SSID):

---

**Security Options--Profile 1**

None

WEP

WPA-PSK[TKIP]

WPA2-PSK[AES]

WPA-PSK[TKIP]+WPA2-PSK[AES]

---

The following table describes parameters in this page:

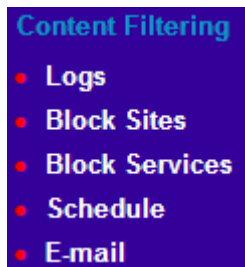
Field	Description
Network Profiles	Brief description of the created guest network. You can create up to four guest networks. A network profile contains the information of a guest network, including the number, SSID, encryption mode, whether the guest network is enabled, and whether to broadcast SSID. You can select the radio button of a profile to view the detailed information or modify the settings.
Enable Guest	Enable or disable a guest network. After it is enabled, you and

Field	Description
Network	the visitor can connect to the network through the SSID of the guest network.
Enable SSID Broadcast	Enable or disable SSID broadcast. After it is enabled, the wireless router broadcasts its SSID to all wireless stations.
Allow Guest to access My Local network	If it is enabled, users connected to the network of this SSID can access not only the Internet but also the LAN of the wireless router, like users connected to the network of the primary SSID. If this option is disabled, users connected to the network of this SSID cannot access the LAN of the wireless router.
Enable Wireless Isolation	Enable or disable wireless isolation. If it is enabled, wireless clients connected to the network of this SSID can access the Internet, but cannot communicate with other wireless clients or Ethernet clients.
Guest Wireless Network Name (SSID)	Name of the guest network. The SSID can contain up to 32 characters and can be any combination of letter, numerals, and underlines. It is case-sensitive.
Security Options	Refer to descriptions and setting methods of <b>Security Options</b> in section 6.4.2 "Wireless Settings".

After setting, click **Apply** to save the settings.

## 6.5 Content Filtering

Click **Content Filtering** and the extended navigation menu is shown as follows:



The submenu contains **Logs**, **Block Sites**, **Block Services**, **Schedule**, and **E-mail**.

### 6.5.1 Logs

Click **Guest Network** on the left pane of the page to display the following page.

#### Logs

Enable Log

Current time: Saturday, Jan 01, 2011 20:28:16

```
[5] syslog: [AUTH] 192.168.1.136 login
success, Sat Jan 1 20:28:13 2011
[5] syslog: [AUTH] User admin session
timeout and auto logout
[5] syslog: [AUTH] 192.168.1.136 login
success, Sat Jan 1 20:22:22 2011
[5] syslog: [AUTH] User admin session
timeout and auto logout
[4] kernel: wlan0: A STA is rejected by
802.1x daemon - 00:26:5A:80:87:48
[4] kernel: wlan0: A wireless client is
associated - 00:26:5A:80:87:48
[4] kernel: wlan0: A wireless client is
associated - 00:26:5A:80:87:48
[4] kernel: wlan0: A STA is rejected by
```

Apply Refresh Clear Log Send Log

In this page, you can view the system events.

Enable log function and click the **Apply** button to activate the log function.

Click the **Refresh** button to refresh the system log.

Click the **Clear Log** button to clear the system events.

Click the **Send Log** button to send the system events to your local PC.

### 6.5.2 Block Sites

Click **Block Sites** on the left pane of the page to display the following page.

**Block Sites**

---

**Keyword Blocking**

Never  
 Per Schedule  
 Always

---

Type Keyword or Domain Name Here.

Add Keyword

---

Block Sites Containing these Keywords or Domain Names:

Delete Keyword    Clear List

---

Allow Trusted IP Address To Visit Blocked Sites

Trusted IP Address   

---

Apply    Cancel

In this page, you can add or delete a filter rule of domain name or keyword, to block LAN users from accessing certain websites in the WAN.

The following table describes parameters and buttons in this page:

Field	Description
Keyword Blocking	Select the mode of blocking. You can select <b>Never</b> , <b>Per Schedule</b> , or <b>Always</b> . <ul style="list-style-type: none"> <li>● <b>Never</b>: Website blocking is disabled.</li> <li>● <b>Per Schedule</b>: After you select it and set in <b>Schedules</b> page, website blocking is enabled according to the settings in the <b>Schedules</b> page.</li> <li>● <b>Always</b>: Website blocking is always enabled.</li> </ul>
Type Keyword or Domain	Enter the keyword or domain name that you want to block. Domain name: For example, <i>www.badstuff.com/xxx</i> ( <i>bad stuff</i>

Field	Description
Name Here	indicates improper information. Keyword: Enter certain words, for example, blasphemy or erotic readings, included in a link.
Add Keyword	Click the button to add the keyword or domain name you entered to the list under the button.
Block Sites containing these Keywords or Domain Names	The list displays the blocked entries. It can contain up to 32 entries.
Delete Keyword	Select a keyword or domain name in the above list and click the button to delete it from the list.
Clear List	Click the button and all keywords and domain names are deleted from the list.
Allow Trusted IP Address To Visit Blocked Sites	After it is selected, the specified computer has the full authority for accessing the Internet.
Trusted IP Address	Specify the IP address of a computer. You need to enter only a numeral in the fourth field.

After setting, click **Apply** to save the settings.

### 6.5.3 Block Services

Click **Block Services** on the left pane of the page to display the following page.



**Block Services**

---

Services Blocking

Never

Per Schedule

Always

---

Block Service Rules Table

#	Service Name	Port	IP

---

In this page, you can set rules of service blocking, to block users from Internet access.

The following table describes parameters and buttons in this page:

Field	Description
Services Blocking	<p>Select the mode of service blocking. You can select <b>Never</b>, <b>Per Schedule</b>, or <b>Always</b>.</p> <ul style="list-style-type: none"> <li>● <b>Never</b>: Service blocking is disabled.</li> <li>● <b>Per Schedule</b>: After you select it and set in the <b>Schedules</b> page, service blocking is enabled according to the settings in the <b>Schedules</b> page.</li> <li>● <b>Always</b>: Service blocking is always enabled.</li> </ul>
Block Service Rules Table	The table lists all services to be blocked. You can add, edit, or delete a service entry according to your requirement.
Add	Click the button to add a rule of service blocking in the <b>Block Services Setup</b> page that is displayed.
Edit	Select a rule of service blocking in the <b>Block Service Rules Table</b> and click the button to edit the rule in the <b>Block Services Setup</b> page that is displayed.
Delete	Select a rule of service blocking in the <b>Block Service Rules Table</b> and click the button to delete it.

Click **Add** and the **Block Services Setup** page appears:

**Block Services Setup**

---

Service Type

Protocol

Starting Port

Ending Port

Service Type/User Defined

---

Filter Service For:

Only This IP Address:

IP Address Range:

to

All IP Address:

---

The following table describes parameters in this page:

Field	Description
Service Type	Select a service type from the drop-down list. If your desired type is not in the list, select <b>User defined</b> . Then, you need to select the protocol, enter the service name, and specify the port range. For services that exist in the drop-down list, the corresponding information is already preset.
Protocol	Indicate the protocol that is used at the service ports. You can select <b>TCP/UDP</b> , <b>TCP</b> , or <b>UDP</b> .
Starting Port	The first port to which an application sends a connection request. All relevant ports can be open only after connection is established at this starting port. Otherwise, other relevant ports are not open.
Ending Port	Set the end port of the service port range.
Service Type/User	Enter the service name.

Field	Description
Defined	
Filter Service For	<p>It determines the computers to be blocked.</p> <ul style="list-style-type: none"> <li>● <b>Only This IP Address:</b> Only one network card on a computer is blocked. You need to enter the IP address of a network card on a computer.</li> <li>● <b>IP Address Range:</b> Network cards that corresponding to a range of IP addresses are blocked. You need to enter the starting and ending addresses of the IP address range.</li> <li>● <b>All IP Address:</b> Network cards of all computers are blocked.</li> </ul>

After setting, click **Add** to add a new rule. Then, click **Apply** to save the settings in the **Block Services** page.

#### 6.5.4 Schedule

Click **Schedule** on the left pane of the page to display the following page.

**Schedule**

---

**Days to Block:**

- Every Day
- Sunday
- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday

---

**Time of day to Block:(use 24-hour clock)**

All Day

Start Blocking                       Hour  Minute

End Blocking                         Hour  Minute

---

**Time Zone**

▾

Automatically adjust for daylight savings time

Current time: Saturday, Jan01, 2011 20:16:53

---

If you already set content filtering in the **Block Sites** page or set service filtering in the **Block Services** page, you can set a schedule to specify the time and mode of restricting Internet access.

The following table describes parameters in this page:

Field	Description
Days to Block	Select every day, one day, or several days.
Time of Day to Block	If you want to fully restrict access every day, select <b>All Day</b> . If you want to restrict access in a specific time during certain days, select the days and enter the starting time and ending time.

Field	Description
	Note that the system uses 24-hour clock.
Time Zone	Select the proper local time zone. After selecting the time zone, the time schedule can work properly. You may select <b>Automatically adjust for daylight savings time</b> according to your location.

After setting, click **Apply** to save the settings.

### 6.5.5 E-mail

Click **E-mail** on the left pane of the page to display the following page.

#### E-mail

---

Turn E-mail Notification On

---

**Send Alerts and Logs Via E-mail**

Your Outgoing Mail Server:

Send To This E-mail Address:

Your Mail Server requires authentication

User Name

Password

---

**Send Alert Immediately**  
When Someone Attempts To Visit A Blocked Site.

---

**Send Logs According to this Schedule**

None

Day

Time   a.m.  p.m.

---

The wireless router can send the alarm information to you if someone tries to access the blocked sites. The log information lists all the accessed URL addresses.

If you hope that the wireless router sends you the alarm and log information by E-mail, please set the relevant parameters in this page.

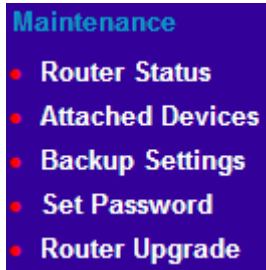
The following table describes parameters in this page:

Field	Description
Turn E-mail Notification On	Enable or disable E-mail notification function.
Your Outgoing Mail Server	Enter SMTP outgoing mail server of ISP.
Send To This E-mail Address	Enter an E-mail address. The alarm and log information can be sent to this E-mail address.
Your Mail Server requires authentication	If your mail server requires authentication for sending an E-mail, please select this option and enter the correct username and password.
User Name	Enter the user name of your E-mail server.
Password	Enter the password of your E-mail server.
Send Alert Immediately	Enable or disable the function of sending alarm information immediately to your e-mail.
Send Logs According to this Schedule	Set the regular time for sending the log information to your E-mail.

After setting, click **Apply** to save the settings.

## 6.6 Maintenance

Click **Maintenance** and the extended navigation menu is shown as follows:



The submenu contains **Router Status**, **Attached Devices**, **Backup Settings**, **Set Password**, and **Router Upgrade**.

### **6.6.1 Router Status**

Click **Router Status** on the left pane of the page to display the following page.

Router Status

System Info

Hardware Version	WNR612
Firmware Version	1.0.7.1
Time and Date	2011-01-01 21:44:16

Internet Port

MAC Address	00:1E:E3:DA:95:B0
Internet	Disconnected(DHCP)
IP address	0.0.0.0
IP Subnet mask	0.0.0.0
Default Gateway	0.0.0.0
Domain Name Server	0.0.0.0

LAN Port

MAC Address	00:1E:E3:DA:95:AF
IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0

Wireless Port

Wireless Network Name (SSID)	NETGEAR
Region	Asia
Wireless Channel	2.442GHz- CH7
802.11 Mode	Up to 150Mbps
Wireless Radio	Enabled
Broadcast Name	ON
Wireless Isolation	OFF
Wi-Fi Protected Setup	ON
Wireless Security Mode	None

Show Statistics

Connection Status

This page displays the information of the current running status of the device, including system information, connection status of the Internet port, LAN port, and wireless port.

Click **Show Statistics** to display the following page.



System Up Time: 00:02:06

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	LinkDown	0	0	0	0	0	00:00:00
LAN1	100M Full	783	607	0	572287	80889	00:01:56
LAN2	LinkDown						00:00:00
WLAN	150Mbps	144	2298	0	56448	378835	00:01:48

Poll Interval:  (1~86400 secs)

This page displays the performance statistics information of the router, including the numbers of sent and received packets at each port.

The following table describes parameters in this page:

Field	Description
System Up Time	Display the time period that the router is running.
Set Interval	Set the interval for refreshing this page. Its value range is 1 to 86400 seconds. Enter a value in the field and click <b>Set Interval</b> . The settings take effect immediately. If you click <b>Stop</b> , this page displays the statistics information when the page is refreshed for the last time and it is not refreshed any more.

Click **Connection Status** in the **Router Status** page, and the **Connection Status** page appears. This page displays the information of current connection on the router.

If the WAN connection is set to **Dynamic IP (DHCP)**, the **Connection Status** page is as shown in the following figure:

## Connection Status

IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
DHCP Server	0.0.0.0
DNS Server	0.0.0.0
Lease Obtained	0Day,0Hour,0Minute
Lease Expires	0Day,0Hour,0Minute




The following table describes buttons in this page:

Button	Description
Release	Click the button to release the IP address of the WAN interface.
Renew	Click the button to refresh the parameters in this page.

If the WAN connection is set to any other mode, you can view the information, the parameters in the **Connection Status** page varies according to the Internet connection mode.

For detailed descriptions of the WAN connection modes, refer to the section [错误! 未找到引用源。](#)

### 6.6.2 Attached Devices

Click **Attached Devices** on the left pane of the page to display the following page.

#### Attached Devices

##### Wired Devices

#	IP Address	Device Name	MAC Address
1	192.168.1.136	GJ544D	00:22:19:04:FE:26

##### Wireless Devices(Wireless intruders also show up here)

#	IP Address	Device Name	MAC Address
---	------------	-------------	-------------

Refresh

This page displays the information of computers connected to the router, including the IP address, device name, and MAC address of each computer.

Click **Refresh** to refresh the information of the connected computers.

### 6.6.3 Backup Settings

Click **Backup Settings** on the left pane of the page to display the following page.

#### Backup Settings

Save a Copy of Current Settings	Backup
Restore Saved Setting from a File	Browse... Restore
Revert to Factory Default Settings	Erase
Reboot Device	Reboot

In this page, you can export the configuration information of the router in a file to the computer for later use, import a previously saved or a new configuration file, restore the factory default settings of the router, and reboot the router.

- **Backup**  
Click **Backup** and select the path to save the configuration of the router as a local file.
- **Restore**  
Click **Browse...** to select the configuration file in your computer and click **Restore** to load the selected file to the router.
- **Erase**  
Click **Erase** to restore the factory default settings of the router. This operation has the same effect of pressing the **Reset** button on the rear panel for 3 seconds.
- **Reboot**  
Click **Reboot** to reboot the router.

---

 **Caution:**

**After a new configuration file is imported, the original configuration information of the router is lost. Hence, it is recommended to back up the configuration before importing a new configuration file. If the new configuration file is incorrect, you can import the previous backup file. During a configuration file is loading, do not power off the router. Otherwise, the router may be damaged and fail to work.**

---

#### 6.6.4 Set Password

Click **Set Password** on the left pane of the page to display the following page.

**Set Password**

---

Old Password

Set Password

Repeat New Password

---

In this page, you can change the password of the administrator.

The following table describes parameters in this page:

Field	Description
Old Password	Enter the password for logging in to the router.
Set Password	Enter a new password.
Repeat New Password	Enter the new password again.

**Note:**

For security measures, it is strongly recommended to change the default password of the administrator. If you forget the password, you can restore the router to the default settings. The default user name and password are **admin** and **password** respectively.

**6.6.5 Router Upgrade**

Click **Router Upgrade** on the left pane of the page to display the following page.

## Router Upgrade

---

Locate and select the upgrade file from your hard disk:

In this page, you can upgrade the software of the router in the following steps:

**Step 1** Click **Browse...** to navigate to the latest software.

**Step 2** Select the correct upgrade file.

**Step 3** Click **Upload** to start upgrading.

After the upgrade is complete, the router automatically reboots.

---

 **Caution:**

**To avoid losing previous configuration of the router, save the configuration before upgrade.**

**During upgrade, do not power off the router or press the Reset button.**

---

## 6.7 Advanced Settings

Click **Advanced** and the extended navigation menu is shown as follows:



The submenu of advanced settings contains **Advanced Wireless Settings**, **Wireless Repeating Function**, **Port Forwarding/Port Triggering**, **WAN Setup**, **LAN Setup**, **QoS Setup**, **Dynamic DNS**, **Static Routes**, **Remote Management**, **UPnP**, and **Traffic Meter**.

### 6.7.1 Advanced Wireless Settings

Click **Advanced Wireless Settings** on the left pane of the page to display the following page..

**Advanced Wireless Settings**

---

**Wireless Advanced Setting**

Enable Wireless Router Radio

Fragmentation Length (256-2346)

CTS/RTS Threshold (1-2347)

Preamble Mode

Transmit Power Control

---

**WPS Settings**

Router's PIN: 87682830

Enable WPS

Disable Router's PIN

Keep Existing Wireless Settings

Wireless Card Access List

---

The following table describes parameters in this page:

Field	Description
Enable Wireless Router Radio	After it is selected, the WLAN indicator on the front panel of the router blinks. The client can now connect to the router wirelessly.
Fragmentation Length (256-2346)	Set the threshold of fragmentation length. If the length of a packet is greater than the value, the packet is automatically fragmented into several packets. Because too many packets lead to low performance of the wireless network, the value of <b>Fragmentation Length</b> cannot be too small. The default value is 2346.
CTS/RTS Threshold (1-2347)	Set the CTS/RTS threshold. If the length of a packet is greater than the value, the router sends an RTS frame to the destination station to negotiate. After receiving the RTS frame, the wireless station responds with a Clear to



Field	Description
	Send (CTS) frame to the router, indicating that they can communicate with each other. The default value is 2346.
Preamble Mode	Set the preamble mode. You may select <b>Long preamble</b> or <b>Short preamble</b> . The default is <b>Short preamble</b> . A preamble (especially the <b>802.11b High Rate/DSSS PHY</b> field; 56 digits synchronized field for short preamble) defines the length of the CRC correction block for communication between wireless devices. Shorter settings should be applied in a network of intense traffics. Short preamble is mainly used to improve the efficiency of a wireless network for applications that have high requirement of real-time, such as streaming video and voice-over-IP telephony.
Transmit Power Control	Set the transmit power of the router. The default is <b>100%</b> , which indicates to transmit full power.
Router's PIN	To configure wireless settings of the router through WPS, you need to enter PIN on the wireless client.
Enable WPS	Enable or disable WPS.
Disable Router's PIN	Enable or disable routeris PIN mode.
Keep Existing Wireless Settings	It determines whether WPS is configured on the router. If this option is not selected, newly added wireless clients changes the wireless settings of the router into random SSID and security key that are automatically generated.
Wireless Card Access List	You can set to allow only network cards of specific PCs to access your wireless network according to the MAC address of the network card of a PC. Click <b>Setup Access List</b> to add, edit, or delete entries in the <b>Wireless Card Access List</b> page.

Click **Setup Access list** button and the **Wireless Card Access List** page appears:

Wireless Card Access List

---

Turn Access Control On

Device Name	Mac Address

---

---

The following table describes parameters and buttons in this page:

Field	Description
Turn Access Control On	Enable or disable wireless access control. If it is selected, you can restrict wireless network cards according to their MAC addresses.
Add	Click the button to add an entry of wireless network card in the <b>Wireless Card Access Setup</b> page that is displayed.
Edit	Select an entry of wireless network card and click the button to modify the device name or MAC address in the <b>Wireless Card Access Setup</b> page that is displayed.
Delete	Select an entry of wireless network card and click the button to delete it.

Click the **Add** button and the **Wireless Card Access Setup** page appears:

Wireless Card Access Setup

Available Wireless Cards

	Device Name	Mac Address
<input type="radio"/>	--	04:0C:CE:E0:B8:60
<input type="radio"/>	ANDROID_3188850087525FA6	78:D6:F0:33:59:C1
<input type="radio"/>	--	00:22:66:E2:37:41
<input type="radio"/>	GJ1461D	00:26:5A:80:87:48
<input type="radio"/>	ALVIN	00:22:FA:F5:5F:08
<input type="radio"/>	ARTHUR	00:1C:B3:61:D1:1B

Wireless Card Entry

Device Name

Mac Address

The following table describes parameters in this page:

Field	Description
Available Wireless Cards	It displays all the available wireless network cards of PCs and their MAC addresses. Click the radio button of a network card to select its MAC address. If the list does not contain your desired wireless network card, you can manually enter the MAC address of the wireless network card.
Device Name	Name of the device. You can customize one.
Mac Address	Physical address of the network card. It is a string of 12 characters.

After setting, click **Add** to add a wireless card entry. Then, click **Apply** to save the settings in the **Advanced Wireless Settings** page.

## 6.7.2 Wireless Repeater

Wireless distribution system (WDS) enables interconnection between APs in an IEEE 802.11 wireless network. It extends the wireless network through several APs, without connection of wired backbone network. This function is also called wireless repeating or bridging.

Click **Wireless Repeating Function** on the left pane of the page to display the following page.

### Wireless Repeater

---

Enable Wireless Repeating Function

Wireless MAC of this router: 00:1E:E3:DA:95:AF

Wireless Repeater

Disable Wireless Clients Association

Repeater IP Address:  .  .  .

Basic Station MAC Address:  :  :  :  :  :

Wireless Basic Station

Disable Wireless Clients Association

Repeater MAC Address 1:  :  :  :  :  :

Repeater MAC Address 2:  :  :  :  :  :

Repeater MAC Address 3:  :  :  :  :  :

Repeater MAC Address 4:  :  :  :  :  :

---

The following table describes parameters in this page:

Field	Description
Enable Wireless Repeating Function	Enable or disable wireless repeating. If the channel is set to <b>Auto</b> , this function cannot be enabled. If you try enabling the function when the channel is set to <b>Auto</b> , the system automatically

Field	Description
	switches to the <b>Wireless Settings</b> page, where you can change the channel.
Wireless Repeater	In this mode, the router serves as a repeater to communicate with the central base station.
Disable Wireless Clients Association	If it is selected, clients cannot access the LAN.
Repeater IP Address	Enter the IP address of the repeater. It must be in the same network segment as the IP address of the central base station.
Basic Station MAC Address	Enter the physical address of the central base station.
Wireless Basic Station	In this mode, the router serves as the central base station to communicate with repeaters. You can add up to four repeaters. The central base station forwards the data of communication between repeaters to the destination repeaters. Repeaters should be configured accordingly.
Repeater MAC Address 1/2/3/4	Enter the physical address of the repeater.

After setting, click **Apply** to save the settings.

### 6.7.3 Port Forwarding/Port Triggering

Click **Port Forwarding/Port Triggering** on the left pane of the page to display the following page.

Port Forwarding / Port Triggering

Please select the service type

Port Forwarding  
 Port Triggering

Service Name: 
 Service IP Address:  .  .  .

#	Server Name	Start Port	End Port	Server IP Address

● **Port Forwarding**

By default, the firewall function of the router hides your LAN. As a result, other users on the Internet can detect only the router, but cannot access a certain PC in the LAN directly. If you want to access a PC in a LAN, you need to configure port forwarding on the router and map the desired port to the corresponding PC in the LAN. After setting, after receiving an access request from the Internet, the router forwards the packets to the PC according to the rule of port mapping. In this way, communication is successfully established between the Internet and the PC in the LAN.

Choose **Port Forwarding** in the **Port Forwarding/Port Triggering** page to display the following page.

Port Forwarding / Port Triggering

Please select the service type

Port Forwarding  
 Port Triggering

Service Name:  Service IP Address:

#	Server Name	Start Port	End Port	Server IP Address

The following table describes parameters and buttons in this page:

Field	Description
Service Name	Select a service type from the drop-down list.
Service IP Address	Enter the IP address of the computer on which the service is to be provided.
Add	Click the button to add a service.
Edit Service	Click the button to edit a service entry in the <b>Ports - Custom Service</b> page that is displayed.
Delete Service	Delete a service entry.
Add Custom Service	If the list does not contain your desired service, click the button to add a service in the <b>Ports - Custom Service</b> page that is displayed.

Click the **Add Custom Service** button and the **Ports - Custom Service** page appears:

**Ports - Custom Service**

---

Service Name:

Protocol:

Starting Port:  (1~65535)

Ending Port:  (1~65535)

Server IP Address:  .  .  .

---

The following table describes parameters in this page:

Field	Description
Service Name	Select a service type from the drop-down list.
Protocol	Indicate the protocol that is used at the mapping port. You can select <b>TCP/UDP</b> , <b>TCP</b> , or <b>UDP</b> .
Starting Port	After the connection to the mapping port is established, the corresponding port is open and the application can initiate consequent connection requests to the open port.
Ending Port	Set the end port of the mapping port range.
Server IP Address	Enter the IP address of the computer on which the service is to be provided.

After setting, click **Apply** to save the settings.

● **Port Triggering**

Certain applications, such as WAN network games, video conferences, and network calls, require multiple connections. Because of the firewall setting, these applications cannot work on a simple NAT router. However, certain special applications enable the applications to work on a NAT router. When an application sends a connection request to a trigger port, the corresponding ports are open, for later connection and service provision.



Choose **Port Triggering** in the **Port Forwarding/Port Triggering** page to display the following page.

**Port Triggering**

Please select the service type

Port Forwarding  
 Port Triggering  
 Enable Port Triggering

Port Triggering Timeout(in minutes)  (1-9999)

#	Enable	Server Name	Service Type	Required Inbound Connection	Service User
<input type="button" value="Add Service"/> <input type="button" value="Edit Service"/> <input type="button" value="Delete Service"/>					
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					

The following table describes parameters in this page:

Field	Description
Enable Port Triggering	Enable or disable port triggering.
Port Triggering Timeout (in minutes)	Enter a value not greater than 9999. The timeout value controls the inactive timer at the specified ingress port. Upon timeout of the inactive timer, the ingress port is disabled.
Add Service	Click the button to add a rule in the <b>Port Triggering – Services</b> page that is displayed.
Edit Service	Click the button to edit a selected rule in the <b>Port Triggering – Services</b> page that is displayed.
Delete Service	Click the button to delete a selected rule.

Click the **Add Service** button and the **Port Triggering – Services** page appears:

Port Triggering - Services

---

Service Name

Service User

Service Type

Triggering Port  (1~65535)

Required Inbound Connection

Connection Type

Starting Port  (1~65535)

Ending Port  (1~65535)

---

The following table describes parameters in this page:

Field	Description
Service Name	Enter the service name.
Service User	You can select <b>Any</b> or <b>Single address</b> . <ul style="list-style-type: none"> <li>● <b>Any</b>: Allow everybody in the user network to use the service.</li> <li>● <b>Single address</b>: Enter the IP address of the network card on the PC. Then, the service is applied only on the specific network card of the PC.</li> </ul>
Service Type	Indicate the protocol used at the triggering port. You can select <b>TCP/UDP</b> , <b>TCP</b> , or <b>UDP</b> .
Triggering Port	Unless this port generates the traffic, the input connection service cannot be triggered.
Connection Type	You can select <b>TCP/UDP</b> , <b>TCP</b> , or <b>UDP</b> .
Starting Port	When the connection to the triggering port is successful, the corresponding ports are open and the application can send consequent connection request to the open ports.

Field	Description
Ending Port	Set the end port of the triggering port range.

After setting, click **Apply** to add the rule of port triggering.

### 6.7.4 WAN Setup

Click **WAN Setup** on the left pane of the page to display the following page.

#### WAN Setup

---

Disable Port Scan and DOS Protection

---

Default DMZ Server

---

Respond to Ping on Internet Port

---

Disable IGMP Proxying

---

MTU Size(in bytes)

---

NAT Filtering  Secured  Open

Disable SIP ALG

Enable IPv6 Pass-Through

---

In this page, you can set a default DMZ server and allow the router to respond to the **ping** command from the Internet. Do not use the two functions unless it is necessary because they lead to security risks. DMZ allows all ports of a PC in your LAN to be exposed to the WAN. Enter the IP address of a PC to set the PC to a DMZ host, which is not restricted by the firewall any more. In this way, the DMZ

host can have mutually unrestricted communication with a user or server on the WAN.

The following table describes parameters in this page:

Field	Description
Disable Port Scan and DOS Protection	This function protects your LAN against DoS attack. Do not disable this firewall function unless a special situation occurs.
Default DMZ Server	Enter the IP address of a computer or server that serves as a DMZ server.
Respond to Ping on Internet Port	If you want the router to respond to ping commands from the Internet, select the check box. The ping command can be used for diagnosis. Like a DMZ server, this function also leads to security risks. Hence, do not select the check box unless it is necessary.
Disable IGMP Proxying	IGMP proxy allows a PC in the LAN to receive certain multicast traffics from the Internet. If you do not want to use IGMP proxy, select the check box to disable IGMP proxy.
MTU Size (in bytes)	The maximum transmission unit. Normally, it is 1500 bytes for most Ethernet networks, 1492 bytes for PPPoE connection, and 1436 bytes for PPTP connection. Certain ISPs may require smaller MTU, but this is a rare case. Do not modify the value of MTU size unless it is necessary for your ISP connection.
NAT Filtering	Determines the mode of the router to handle the input traffics. <ul style="list-style-type: none"> <li>● <b>Secured:</b> It provides a secure firewall that protects personal computers in a LAN against attacks from the Internet. However, it causes malfunction of certain network games, point-to-point (P2P) applications, and multimedia applications.</li> <li>● <b>Open:</b> It provides firewall settings of a lower security level. It allows running of almost all network applications.</li> </ul>
Disable SIP ALG	Certain SIP applications have special mechanisms of passing through the NAT firewall and SIP ALG may have conflicts with these mechanisms. In most cases, you should not disable SIP ALG.

Field	Description
Enable IPv6 Pass-Through	By default, IPv6 pass-through is disabled. If your configuration contains IPv6 devices and you want to replace IPv4 with IPv6, you can select the check box to enable IPv6 pass-through.

After setting, click **Apply** to save the settings.

### 6.7.5 LAN Setup

Click **LAN setup** on the left pane of the page to display the following page.

#### LAN IP Setup

---

Device Name

---

**LAN TCP/IP Setup**

IP Address

IP Subnet Mask

RIP Direction

RIP Version

Use Router as DHCP Server

Starting IP Address

Ending IP Address

DHCP Lease Time( 1 - 160 hours)

---

**Address Reservation**

#	IP Address	Device Name	MAC Address
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

---

In this page, you can configure the parameters of the LAN port. You can modify the IP address of the LAN port according to the actual network environment.

The following table describes parameters and buttons in this page:

Field	Description
IP Address	Set the IP address that a LAN user uses to access the router. The default IP is 192.168.1.1. You can change it if necessary.
IP Subnet Mask	Subnet mask of the LAN port. You can enter a different subnet mask according to the actual network status.
RIP Direction	The mode in which the router sends and receives RIP packets. If it is set to <b>Both</b> or <b>Out Only</b> , the router periodically broadcasts its routing table. If it is set to <b>Both</b> or <b>In Only</b> , the router integrates the received routing tables.
RIP Version	The format of the RIP packets and broadcast mode that the router sends them. RIP-1 is universally supported. Routing data sent by using RIP-2B or RIP-2M is in RIP-2 format. RIP-2B uses subnet broadcast and RIP-2M uses multicast.
Use Router as DHCP Server	If it is selected, the router serves as the DHCP server and automatically assigns IP addresses for all connected computers.
Starting IP Address	The first address in a consecutive IP address pool.
Ending IP Address	The last address in a consecutive IP address pool.
DHCP Lease Time (1 – 160 hours)	After the DHCP lease time elapsed, the router automatically assigns new IP addresses for all connected computers.
Address Reservation	If an IP address is reserved for the network card of a PC in a LAN, the network card obtains the same IP address every time the network card accesses the DHCP server.
Add	Click the button to add an entry in the <b>Address Reservation</b> page that is displayed.
Edit	Select an entry of reserved address and click the button to modify the IP address, MAC address, or device name in the <b>Address Reservation</b> page that is displayed.
Delete	Select an entry of reserved address and click the button to delete it.

Click the **Add** button in the **LAN IP Setup** page, and the **Address Reservation** page is as follows:

**Address Reservation**

Address Reservation Table

	#	IP Address	Device Name	MAC Address
	1	192.168.1.136	GJ544D	00:22:19:04:fe:26

IP Address

MAC Address

Device Name

The following table describes parameters and buttons in this page:

Field	Description
Address Reservation Table	Display entries of reserved addresses. You can select the information of the local computer, or enter the IP address, MAC address, and device name of a computer, and then click <b>Add</b> to add an entry to the <b>Address Reservation Table</b> .
IP Address	Enter the IP address to be reserved. It must be within the IP address pool.
MAC Address	Enter the MAC address of a computer whose IP address is to be reserved.
Device Name	Enter the device name of a computer whose IP address is to be reserved.
Add	Click the button to add the entry to the <b>Address Reservation Table</b> .
Cancel	Click the button to cancel the entry just set.
Refresh	Click the button to refresh the page.

After setting, click **Add** to add an entry to the **Address Reservation Table**.

**Note:**

- If your IP address is changed, you must use the new IP address to log in to the Web configuration page of the router and the default gateway of all hosts in the LAN must be set to the new IP address for Internet access.
- The subnet mask of all hosts in the LAN must be consistent with the subnet mask specified in the **LAN IP Setup** page.

### 6.7.6 QoS Setup

Click **QoS Setup** on the left pane of the page to display the following page.

**QoS Setup**

---

Enable WMM (Wi-Fi multi-media) Settings

---

Turn Internet QoS Access On

---

Turn Bandwidth Control On

    Uplink bandwidth: maximum

---

QoS Priority Rule list   

---

The QoS function sets priority policies on applications, online games, Ethernet LAN ports, and MAC addresses, sets an order for various network traffics, and thus optimizes your network performance.

The following table describes parameters in the **QoS Setup** page:

Field	Description
Enable WMM (Wi-Fi)	Enable or disable WMM. Wireless Multimedia (WMM) is a subset of the 802.11e standard. It supports setting priorities of



Field	Description
multi-media) Settings	wireless traffics according to data types within a certain range. Time-related information such as audio and video has higher priority than normal data. To ensure proper performance of WMM, wireless clients must support WMM.
Turn Internet QoS Access On	Enable or disable QoS. After it is enabled, you can optimize the network access traffics according to the settings in the <b>QoS Priority Table</b> page.
Turn Bandwidth Control On	Set the maximum uplink bandwidth at the WAN port. If the value is in units of <b>Kbps</b> , the maximum value is <b>1000</b> . If the value is in units of <b>Mbps</b> , the maximum value is <b>100</b> .
Setup QoS rule	Click the button and the <b>QoS Setup</b> page is displayed
Enable Trusted IP Address	After it is enabled, you can reserve half egress bandwidth for a specified computer, to avoid impact to the computer because of Internet access behaviors by other users in the network.
Trusted IP Address	Specify the IP address of a computer. You need to enter only a numeral in the fourth field.

Click **Setup QoS Rule** and the **QoS Setup** page appears:

QoS Setup

	#	QoS Policy	Priority	Description
<input type="radio"/>	1	MSN Messenger	High	MSN_messenger Applications
<input type="radio"/>	2	Yahoo Messenger	High	Yahoo_Messenger Applications
<input type="radio"/>	3	IP Phone	Highest	IP_Phone Applications
<input type="radio"/>	4	Vonage IP Phone	Highest	Vonage_IP_Phone Applications
<input type="radio"/>	5	Net Meeting	High	NetMeeting Applications
<input type="radio"/>	6	AIM	High	AIM Applications
<input type="radio"/>	7	Google Talk	Highest	Google_Talk Applications
<input type="radio"/>	8	Netgear EVA	Highest	Netgear_EVA Applications
<input type="radio"/>	9	SSH	High	SSH Applications
<input type="radio"/>	10	Telnet	High	Telnet Applications
<input type="radio"/>	11	VPN	High	VPN Applications
<input type="radio"/>	12	FTP	Normal	FTP Applications
<input type="radio"/>	13	SMTP	Normal	SMTP Applications
<input type="radio"/>	14	WWW	Normal	WWW Applications
<input type="radio"/>	15	DNS	Normal	DNS Applications
<input type="radio"/>	16	ICMP	Normal	ICMP Applications
<input type="radio"/>	17	eMule/eDonkey	Low	eMule/eDonkey Applications
<input type="radio"/>	18	Kazaa	Low	Kazaa Applications
<input type="radio"/>	19	Gnutella	Low	Gnutella Applications
<input type="radio"/>	20	BT/Azureus	Low	BT/Azureus Applications
<input type="radio"/>	21	Counter Strike	High	On-line Gaming Counter-Strike
<input type="radio"/>	22	Age of Empires	High	On-line Gaming Age-of-Empires
<input type="radio"/>	23	Everquest	High	On-line Gaming Everquest
<input type="radio"/>	24	Quake 2	High	On-line Gaming Quake-2
<input type="radio"/>	25	Quake 3	High	On-line Gaming Quake-3
<input type="radio"/>	26	Unreal Tourment	High	On-line Gaming Unreal-Tourment
<input type="radio"/>	27	Warcraft	High	On-line Gaming Warcraft

The following table describes buttons in this page:

Field	Description
Edit	Click the button to change the priorities of the applications, LAN ports, online games, and MAC addresses in the <b>QoS Priority Table</b> .
Delete	Click the button to delete a rule in the <b>QoS Priority Table</b> .
Add Priority Rule	Click the button to set priority policy for an online game, an application, an Ethernet LAN port, or the MAC address of a computer in the <b>QoS – Priority Rules</b> page that is displayed.

Click the **Add Priority Rule** button and the **QoS – Priority Rules** page for an application appears:

**QoS - Priority Rules**

---

Priority

QoS Policy For

Priority Category

Applications

Priority

---

Specified Port Range

Connection Type

Starting Port  (1 - 65535)

Ending Port  (1 - 65535)

---

The following table describes parameters in this page:

Field	Description
QoS Policy For	Enter the name of the QoS policy.
Priority Category	Select <b>Applications</b> .

Field	Description
Applications	Select an application that you want to set. If your desired application is not in the drop-down list, select <b>Add A New Application</b> .
Priority	You can select <b>Highest, High, Normal, or Low</b> .
Connection Type	Indicates the protocol that is used at the port. You can select <b>TCP/UDP, TCP, or UDP</b> .
Starting Port	The first port to which an application sends a connection request. All relevant ports can be open only after connection is established at this starting port. Otherwise, other relevant ports are not open.
Ending Port	Set the end port of the port range.

The **QoS - Priority Rules** page for an online game is as follows:

**QoS - Priority Rules**

---

**Priority**

QoS Policy For

Priority Category

On-line Gaming

Priority

---

**Specified Port Range**

Connection Type

Starting Port  (1 - 65535)

Ending Port  (1 - 65535)

---

The following table describes parameters in this page:

Field	Description
QoS Policy For	Enter the name of the QoS policy.
Priority Category	Select <b>On-line Gaming</b> .
On-line Gaming	Select an online game that you want to set. If your desired online game is not in the drop-down list, select <b>Add a new Game</b> .
Priority	You can select <b>Highest, High, Normal</b> , or <b>Low</b> .
Connection Type	Indicates the protocol that is used at the port. You can select <b>TCP/UDP, TCP</b> , or <b>UDP</b> .
Starting Port	The first port to which an application sends a connection request. All relevant ports can be open only after connection is established at this starting port. Otherwise, other relevant ports are not open.
Ending Port	Set the end port of the port range.

The **QoS – Priority Rules** page for a LAN port is as follows:

**QoS - Priority Rules**

---

Priority

QoS Policy For

Priority Category

Ethernet LAN Port

Priority

---

The following table describes parameters in this page:

Field	Description
QoS Policy For	Enter the name of the QoS policy.

Field	Description
Priority Category	Select <b>Ethernet LAN Port</b> .
Ethernet LAN Port	Select the LAN port that you want to set.
Priority	You can select <b>Highest, High, Normal, or Low</b> .

The **QoS - Priority Rules** page for an MAC address is as follows:

**QoS - Priority Rules**

---

Priority

QoS Policy For

Priority Category

---

**MAC Device List**

	QoS Policy	Priority	Device Name	MAC Address
<input type="checkbox"/>	Pri_MAC_104E88	Normal	WANLI	00:03:7F:10:4E:88
<input type="checkbox"/>	Pri_MAC_04FE26	Normal	GJ544D	00:22:19:04:FE:26

MAC Address

Device Name

Priority

---

---

The following table describes parameters in this page:

Field	Description
QoS Policy For	Enter the name of the QoS policy.
Priority Category	Select MAC Address.
MAC Device List	Display the existing priority rules of computers that have higher priorities according to MAC addresses.

Field	Description
	Enter the MAC address and device name of a computer for which you want to set high priority, and then click <b>Add</b> to add the rule to the list.
MAC Address	Enter the MAC address of a computer for which you want to set high priority.
Device Name	Enter the device name of a computer for which you want to set high priority.
Priority	You can select <b>Highest, High, Normal</b> , or <b>Low</b> .
Add	Click the button to add a priority rule to the <b>MAC Device List</b> .
Edit	Select a priority rule in the <b>MAC Device List</b> and click the button to modify the priority rule.
Delete	Select a priority rule in the <b>MAC Device List</b> and click the button to delete the priority rule from the list.
Refresh	Click the button to update the priority rules in the <b>MAC Device List</b> .

After setting, click **Apply** to save the settings. Then, click **Apply** to save the settings in the **QoS Setup** page.

### 6.7.7 Dynamic DNS

Dynamic DNS (DDNS) is mainly used to realize resolution between fixed domain names and dynamic IP addresses. For a user that uses a dynamic IP address, after the user obtains a new IP address when accessing to the Internet, the dynamic domain name software installed in the host sends the IP address to the dynamic domain name resolution server provided by the DDNS service provider and updates the domain name resolution database. When another user on the Internet tries accessing the domain name, the dynamic domain name resolution server returns the correct IP address.

Click **Dynamic DNS** on the left pane of the page to display the following page.

**Dynamic DNS**

---

Use a Dynamic DNS Service

---

Service Provider DynDNS.org ▾

Host Name

User Name

Password

---

In this page, you can configure the DDNS parameters.  
 The following table describes parameters in this page:

Field	Description
User Dynamic DNS Service <sup>a</sup>	Enable this function if you already register to the DDNS service provider.
Service Provider	You can only select <b>Dyndns.org</b> .
Host Name	Enter the host name or domain name provided by the DDNS service provider.
User Name	Enter the user name of the DDNS account.
Password	Enter the password of the DDNS account.

After setting, click **Apply** to save the settings.

**6.7.8 Static Routes**

Static routing is a special type of routing that can be applied properly in a network to reduce the problem of routing selection and overload of data flow because of routing selection and to improve the forwarding speed of packets. You can set the



destination IP address, subnet mask, and gateway to specify a routing rule. The destination IP address and subnet mask are used to determine a destination network or host. Then, the router sends packets to the specified destination network or host through the gateway.

Click **Static Routes** on the left pane of the page to display the following page.

**Static Routes**

Max of rules: 32

#	Active	Name	Destination	Gateway
---	--------	------	-------------	---------

In this page, you can add, edit, and delete a static routing rule, and view the current static routing table in the router.

Click **Add** and the following page appears:

**Static Routes**

---

Route Name

Active

Destination IP Address  .  .  .

IP Subnet Mask  .  .  .

Gateway IP Address  .  .  .

Metric

---

The following table describes parameters of adding a routing rule:

Field	Description
Router Name	Enter the name of the static route.
Active	Enable it to apply the routing rule.
Destination IP Address	Indicate the destination address or network that you want to access.

Field	Description
IP Subnet Mask	Subnet mask of the destination IP address.
Gateway IP Address	IP address of the router or host to which packets are sent.
Metric	Indicate the number of other routers in the user network. Its value range is 2 to 15. Usually, the value of 2 or 3 leads to the best performance. If the route is direct connection, set the <b>Metric to 2</b> .

After setting, click **Apply** to save the settings.

### 6.7.9 Remote Management

Click **Remote Management** on the left pane of the page to display the following page.

#### Remote Management

Turn Remote Management On

Remote Management Address :  
http://0.0.0.0:8080

Allow Remote Access By :

Only This Computer :

IP Address Range :

Everyone

From	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
To	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Port Number :

The remote management function allows you to configure the router in the WAN through the Web browser. In this way, you can manage the router from a remote host.

The following table describes parameters in this page:

Field	Description
Turn Remote Management On	Enable or disable remote Web management.
Remote Management Address	IP address that is used to access the router from the Internet. The default is http://0.0.0.0:8080. When accessing the router, you need to enter the WAN IP address of the router, along with : and the port number in the address bar (of IE) or the location bar (of Netscape).
Allow Remote Access By	Set the IP address of the computer on which remote Web management is carried out to access the router. <ul style="list-style-type: none"> <li>● <b>Only This Computer:</b> Only the specified IP address can access the router. You need to enter an IP address.</li> <li>● <b>IP Address Range:</b> A number of IP addresses on the Internet can access the router. You need to enter the starting and ending IP addresses to specify the range.</li> <li>● <b>Everyone:</b> Everyone on the Internet can access the router.</li> </ul>
Port Number	Specify the port of Web management for accessing the broadband router.

After setting, click **Apply** to save the settings.

### 6.7.10 UPnP

By using the Universal Plug and Play (UPnP) protocol, a host at the LAN side can ask the router to realize specific port conversion, so that an external host can access resources on the internal host when necessary. For example, if MSN Messenger is installed on Windows ME and Windows XP operating systems, UPnP can be used for audio and video conversations. In this way, functions restricted by NAT can work properly.

Click **UPnP** on the left pane of the page to display the following page.

UPnP

Turn UPnP On

Advertisement Period(in minutes)

Advertisement Time To Live(in hops)

UPnP Portable Table

Active	Protocol	Int. Port	Ext. Port	IP Address	Description
--------	----------	-----------	-----------	------------	-------------

The following table describes parameters in this page:

Field	Description
Turn UPnP On	Enable or disable UPnP.
Advertisement Period (in minutes)	Set the broadcast interval. It indicates the interval for broadcasting the UPnP information by the router. The value should be in the range of 1 to 1440 minutes and the default is 30 minutes.
Advertisement Time To live (in hops)	The time for the broadcast to live. It is the number of hops after each UPnP packet is sent. The number of hops is the times that each packet can be broadcast before it vanishes. The value should be in the range of 1 to 255 hops and the default is 4 hops.
UPnP Portable Table	This table shows the IP addresses of UPnP devices that are connected to the router and open (internal and external) ports on the devices. It also lists the types and status of the open ports.

 **Note:**

Only applications that support UPnP can use the function.  
 The functionality of UPnP requires support by the application and operating systems such as Windows ME, Windows XP, and Windows Vista.

### 6.7.11 Traffic Meter

Choose **System Tools > Traffic Meter** and the **Traffic Meter** page appears.

#### Traffic Meter

##### Internet Traffic Meter

Enable Traffic Meter

Traffic volume control by No limit

Monthly limit  MBytes

Round up data volume for each connection by  MBytes

Connection time control

Monthly limit  Hours

##### Traffic Counter

Restart traffic counter at  :   On the  day of each month

##### Traffic Control

Pop up a warning message

MBytes/Minutes before the monthly limit is reached

When the monthly limit is reached

Disconnect and disable the Internet connection

##### Internet Traffic Statistics

Start Date / Time: 2011-01-01 Saturday 20:00:17  
 Current Date / Time: 2011-01-01 Saturday 21:45:40  
 Traffic Volume Left: No limit

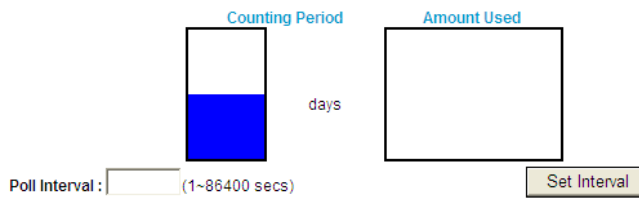
Counting Period	Connection Time (hh:mm)	Traffic Volume (MBytes)		
		Upload/Avg	Download/Avg	Total/Avg
Today	0:0	0	0	0
Yesterday	0:0	0	0	0
This week	0:0	0/0	0/0	0/0
This month	0:0	0/0	0/0	0/0
Last month	0:0	0/0	0/0	0/0

This page records and restricts the traffics that pass through the Internet port of the router. The following table describes parameters and buttons in this page:

Field	Description
Enable Traffic Meter	Enable or disable traffic statistics and control.
Traffic volume control by	Select the object of traffic control. <ul style="list-style-type: none"> <li>● <b>No limit:</b> No limit to the Internet traffics.</li> <li>● <b>Download only:</b> Restrict downlink traffics only.</li> <li>● <b>Both directions:</b> Restrict both uplink and downlink traffics.</li> </ul> <b>Monthly limit:</b> Enter the allowed amount of traffics for each month. <b>Round up data volume for each connection by:</b> Certain ISPs counts extra traffics when a user establishes a new connection. In this case, set the extra data volume.
Connection time control	Enter the allowed connection time for each month. It takes effect only in PPPoE dialup mode.
Restart traffic counter at	Set the time and date when the traffic statistics is started again. Click <b>Restart Counter Now</b> to start traffic statistics again immediately.
Traffic Control	Enter a number other than 0 as the threshold. If the available traffic or available connection time reaches the threshold, a warning message appears on the router and you can view the warning message in the <b>Traffic Status</b> page. If you select this option, all Internet access behaviors are blocked after the monthly traffic amount reaches the threshold.
Internet Traffic Statistics	Display the detailed statistics information of traffics at the Internet port.
Refresh	Click the button to update the information of traffics at the Internet port.
Traffic Status	Click the button and the <b>Traffic Status</b> page appears. You can view the utilization of Internet traffics in real time in this page.

Click the **Traffic Status** button to display the following page.

**Traffic Status**

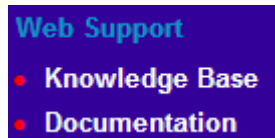


The following table describes parameters in this page:

Field	Description
Poll Interval	Set the poll interval. Its value range is 1 to 86400 seconds. The page is refreshed periodically according to the set interval.
Set Interval	Click the button and the poll interval setting takes effect.

## 6.8 Web Support

Click **Web Support** and the extended navigation menu is shown as follows:



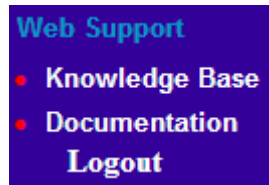
The submenu contains **Knowledge Base** and **Documentation**.

Click **Knowledge Base**, and then you can visit the Web site of the Netgear Company, to get useful information.

Click **Documentation**, and then you can download the user manual, finish product registration, and obtain Web support.

## 6.9 Logout

The Logout control is under the navigation bar on the left pane of the page. See the following figure:



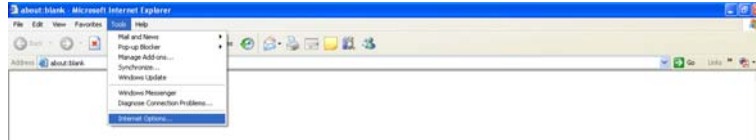
The logout function is used to log out the current login status. After logout, you need to log in again before accessing the configuration page of the router. For the method of login, refer to chapter 5 "Logging In to the Web Page".



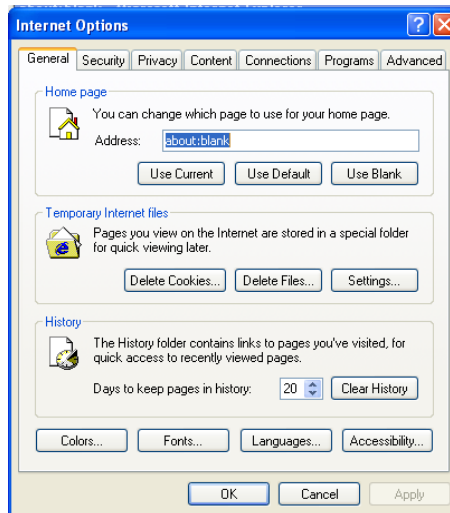
## 7 Troubleshooting

### Failure to configure the router through a web browser

- (1) Open the Web browser (for example, IE) and choose **Tools > Internet Options** from the main menu.



- (2) Click **Delete Cookies...** and **Delete Files...**



### Failure to establish wireless network connection

- Because the router is beyond the wireless coverage.
  - (1) Place the router near the customer premises equipment (CPE).
  - (2) Try modifying the channel setting.
- Because of authentication problems.
  - (1) Use a computer of wired connection to connect the router.
  - (2) Check the network security settings.
  - (3) Try hard reset on the router.
- Because the router cannot be detected.
  - (1) Try hard reset on the router and test again.
  - (2) Check the settings of the wireless network.
  - (3) Check the settings of SSID and encryption.

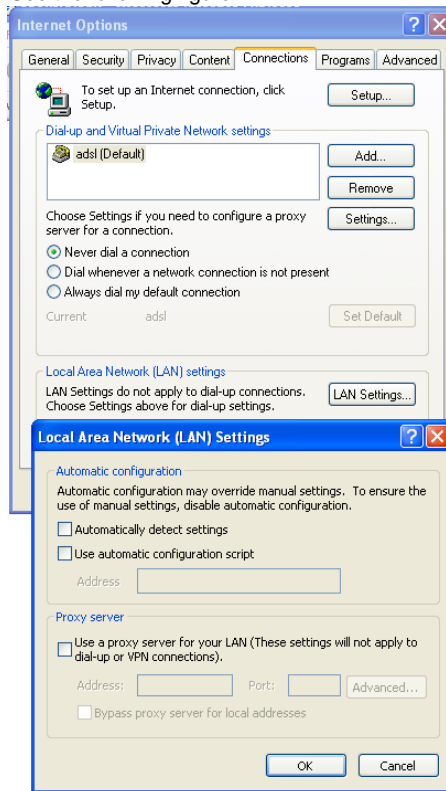
#### **Failure to connect to the Internet through the wireless router**

- (1) Place the router to the wireless area where the CPE can connect.
- (2) Check whether the wireless network card connects to the correct AP (base station).
- (3) Check whether the wireless channel accords with the channel specified in your country or region.
- (4) Check the encryption settings.
- (5) Check whether your ADSL cable is connected to the correct network interfaces.
- (6) Replace with a new network cable to connect to the router.

#### **Failure to access the Internet**

- (1) Check whether the status of indicators on the ADSL modem and the wireless router is normal.
- (2) Check whether the **WAN** indicator is on. If the WAN indicator is off, check whether the cable connected to the **WAN** interface is loose.
- (3) When the **Link** indicator keeps on but does not blink, the router is connected to the Internet.
- (4) Reboot your computer.
- (5) Set the AP again.
- (6) Check whether the WAN indicator is on.
- (7) Check the encryption settings of the wireless network.

- (8) Check whether the PC that connects to the router can obtain the IP address through either the wireless network or the cable network.
- (9) Check the LAN settings of your Internet options, and do not use a proxy server for your LAN. See the following figure:



## FCC Statement

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

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.