

ADDON Magic r9000
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	7
3.3.3	Connecting the Device	8
3.4	Operation Range	8
3.5	Roaming	8
4	TCP/IP Settings and Wireless Connection Introduction	10
4.1	TCP/IP Settings	10
4.2	Wireless Connection Introduction	14
5	Logging In to the Web Page	18
6	Web Configuration	20
6.1	Setup Wizard	20
6.2	Running Status	24
6.2.1	Router Status	24
6.2.2	Clients List	28
6.3	Network Settings	29
6.3.1	LAN Interface Settings	29
6.3.2	WAN Interface Settings	33
6.4	Wireless Settings	40
6.4.1	Wireless Basic Settings	40
6.4.2	Guest Network	45
6.4.3	WPS Setup	47
6.4.4	Wireless Advanced Settings	49
6.4.5	Wireless Repeater	53

6.5	Forwarding Rule	55
6.5.1	Port Forwarding	55
6.5.2	Port Triggering	58
6.5.3	UPnP	60
6.6	Access Control	61
6.6.1	Block Sites	61
6.6.2	Block Services	63
6.6.3	QoS Setup	66
6.7	Dynamic DNS	72
6.8	Static Routing	73
6.9	Security Options	75
6.9.1	Remote Management	75
6.9.2	WAN Setup	77
6.10	System Tools	79
6.10.1	Schedules	79
6.10.2	SNTP	81
6.10.3	Backup Settings	82
6.10.4	Set Password	83
6.10.5	Router Upgrade	85
6.11	Logout	86
7	Troubleshooting	87

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	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	Describes how to navigate through Web pages and how to configure parameters.
	Provides the troubleshooting information.

Features

- Support IEEE802.11b, IEEE802.11g, IEEE802.11n, IEEE802.3, IEEE802.3u, IEEE802.11i, and IEEE802.11e
- 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 3 types of WAN connection modes, that is, static IP, dynamic IP, and PPPoE
- 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 exits 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 services for individual users and SOHO (Small Office, Home Office).

2.2 Packing list

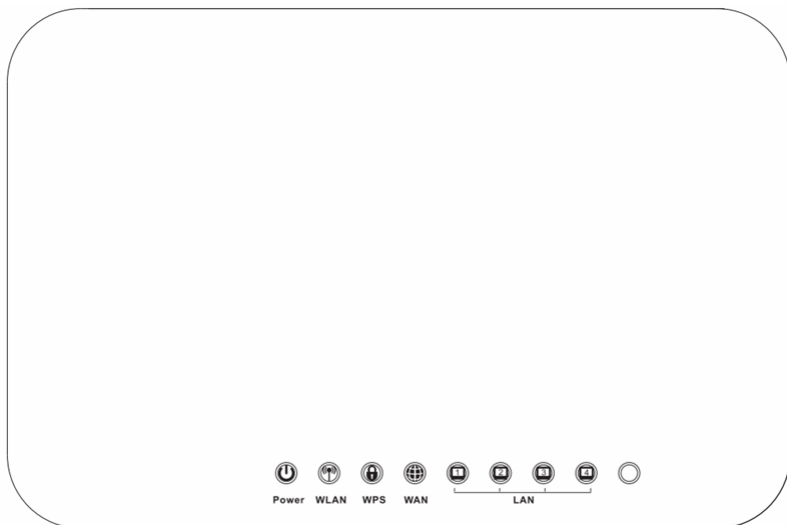
Please check whether your packing list includes the following items:

- Wireless router x 1
- Power adapter (12V DC,500mA) x 1
- Ethernet cable (RJ45) x 1
- Quick installation guide x 1
- CD x 1

3 Hardware Description and Hardware Installation

3.1 Front Panel and LED Status

There are 8 LED indicators on the front panel of the wireless router. By observing their status, you can check whether the device runs normally.

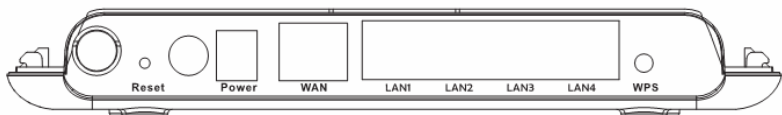


The following table describes the status of LED indicators on the front panel.

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.

WPS	Green	On	Connection succeeds under Wi-Fi Protected Setup.
	Green	Blink	Negotiation is in progress under Wi-Fi Protected Setup.
	-	Off	Wi-Fi Protected Setup is disabled.
WAN	Green	On	Connection succeeds.
	Green	Blink	Data is being transmitted.
	-	Off	No WAN connection.
LAN1/LAN2/LAN3/LAN4	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
Reset	Use a fine needle to press Reset gently for 3 seconds and then release the button. The system reboots and restores to the factory defaults.
Power	Power socket, for connecting the power adapter.
WAN	RJ45 WAN interface, for connecting WAN or the uplink network devices.
LAN1/LAN2/ LAN3/LAN4	RJ45 LAN interfaces, for connecting hubs, switches, or computers in a LAN.
WPS	This button is used for enabling the WPS PBC mode. When WPS is enabled, press this button, and the AP starts to accept

**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 Reset 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 12V, 500 mA. 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 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

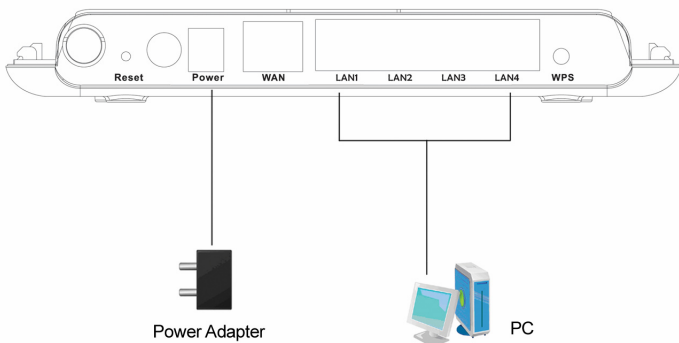
Before you install the device, please pay attention to the following items:

- 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

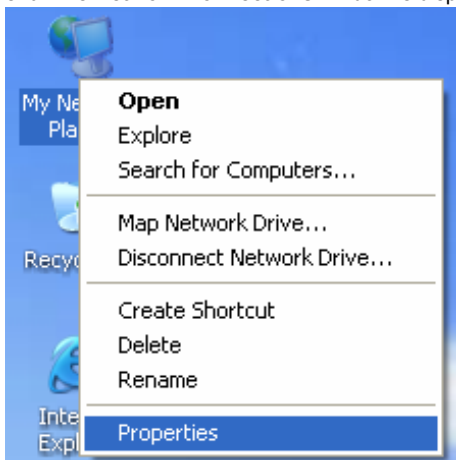
4.1 TCP/IP Settings

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.

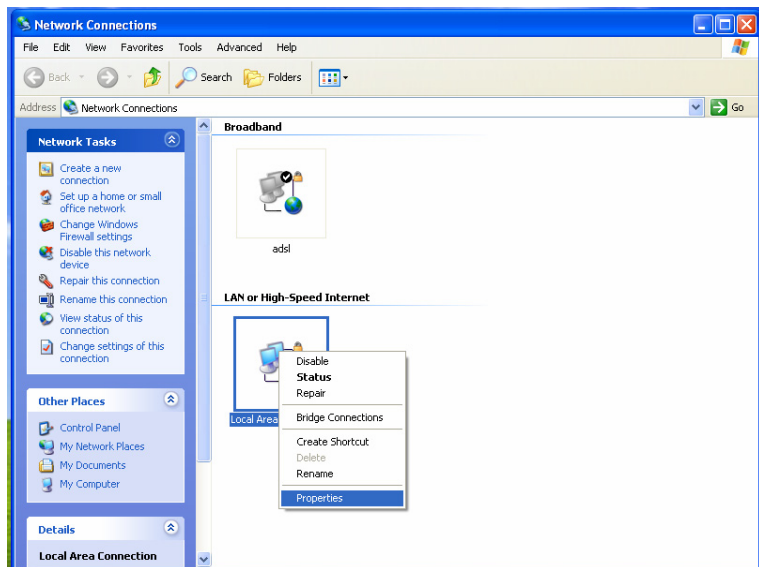
It is recommended to set the network adapter to **Obtain an IP address automatically**. Then, your PC obtains the TCP/IP settings, including the IP address, subnet mask, gateway, and DNS address automatically through the wireless router. If you know the settings of the current LAN interface, you can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



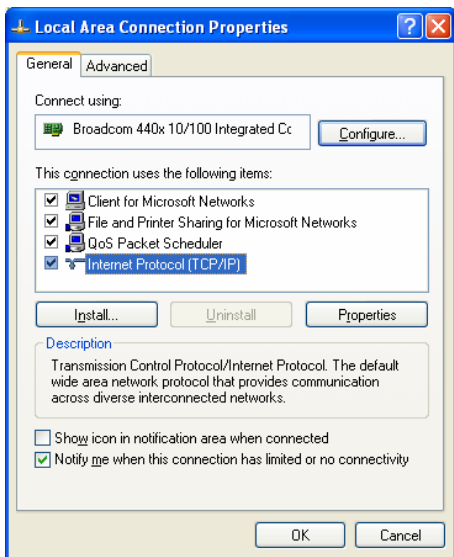
Step 2 Right-click the network adapter icon and choose **Properties** from the menu. The **Local Area Connections Properties** window is displayed.



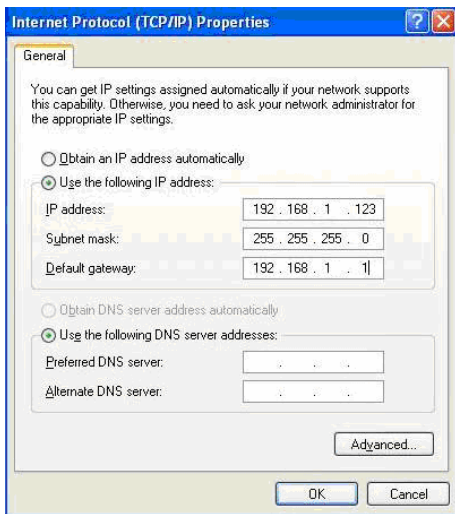
Note:

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

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

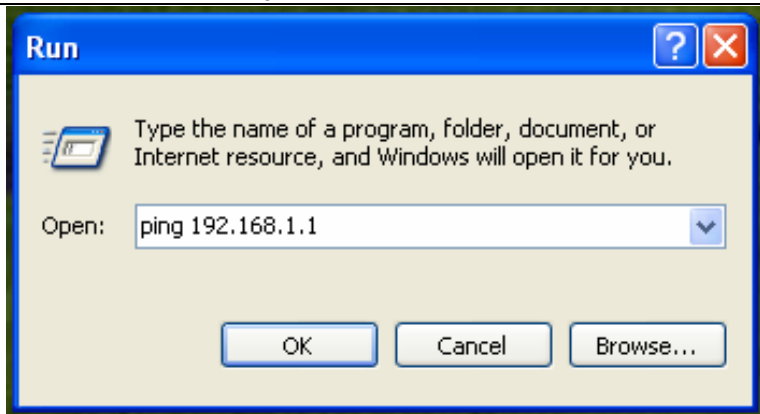


- Step 4** Select **Use the following IP address** and enter the IP address of the network adapter. The IP address must be 192.168. 1.X (X is a number in the range of 2 to 254). If you want to access the Internet through a wireless router, you need to enter the default gateway and IP address of the DNS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

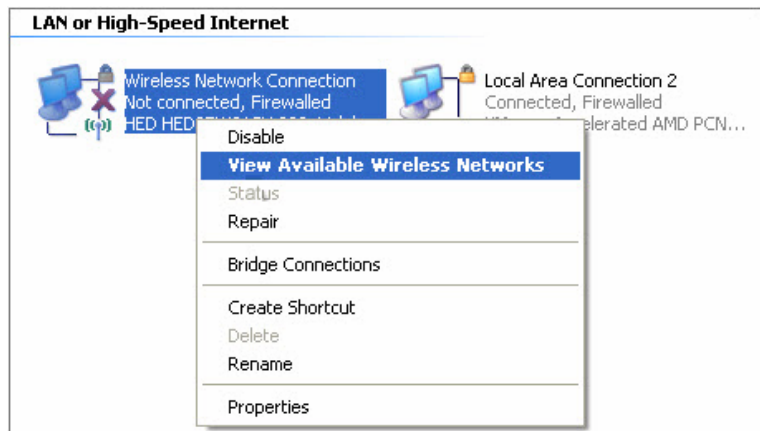
- Step 7** If the PC can ping through the default IP address of the wireless router, the following page is displayed, indicating that the connection between your PC and the wireless router is normal.

```
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
```

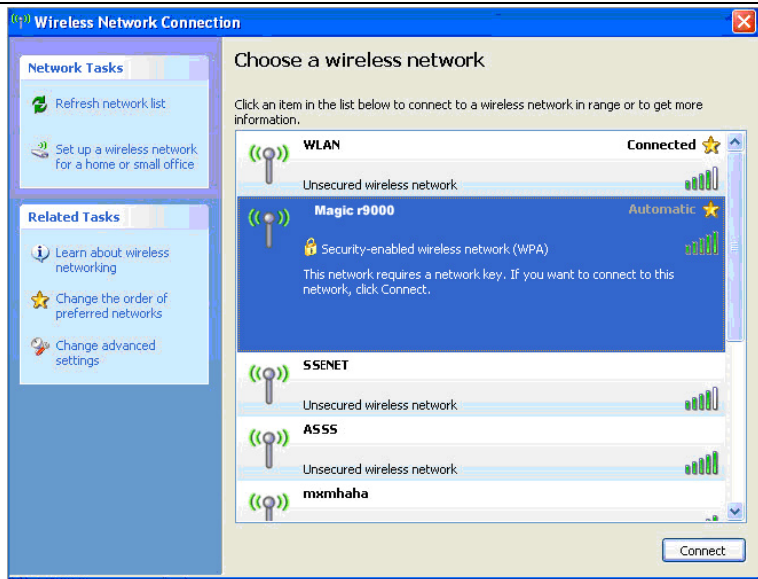
4.2 Wireless Connection Introduction

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 **Magic r9000**. 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 Basic Settings** page of the wireless settings. For more information about the wireless settings, please refer to 6.4 "Wireless Settings".

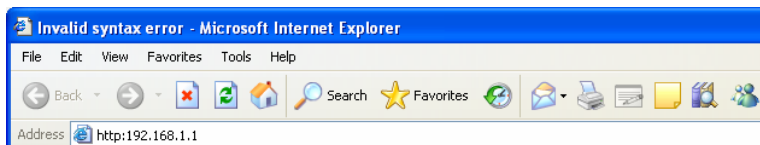
Region Selection	
Region :	Europe ▼
Wireless Network	
<input checked="" type="checkbox"/> Enable SSID Broadcast	
<input type="checkbox"/> Enable Wireless Isolation	
Name(SSID) :	Magic r9000
Mode :	Mixed 802.11b/g/n ▼
Channel:	Auto ▼
Band Width :	40M ▼
Max Transmission Rate :	Auto ▼ Mbps
Security Options	
Security Options :	WPA-PSK[AES] ▼
Security Options(WPA-PSK)	
PassPhrase :	<input type="text"/> (8-63 characters or 64 hex digits)

Note:

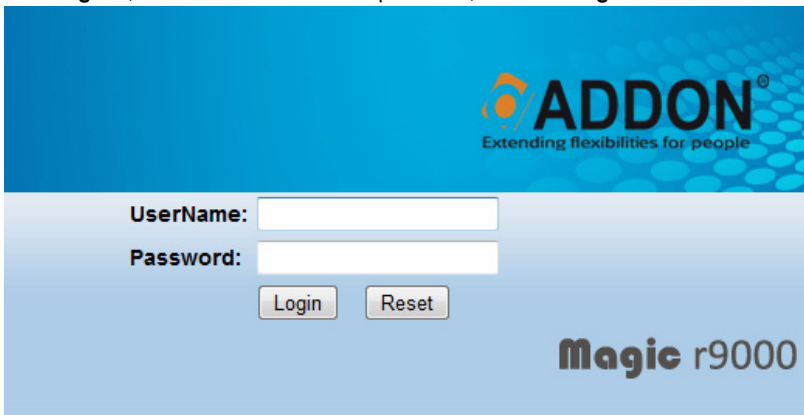
After your wireless network card connects to the wireless router successfully, usually, you should set the network adapter to **Obtain an IP address automatically**. The configuration of wireless connection is now complete.

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, set the **Language** to **English**, enter the user name and password, and click **Login**.



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 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 is displayed.

Setting up your internet


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)**, or **PPPoE**.

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

Setup Wizard

Dynamic IP (DHCP) detected

Successfully detected the type of Internet connection you have.

Back Next

Click **Next** and the following figure is displayed:

Dynamic IP Address

Account Name (If Required)

Apply Cancel

Enter the host 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** and the settings take effect immediately. The setup wizard is now complete.

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

Setup Wizard

Static IP (Fixed) detected

Successfully detected the type of Internet connection you have.

If you believe you have received this message in error, please power cycle your modem (unplug the modem and plug it back in). Then close this screen, and reopen a new Web browser (e.g., Internet Explorer)

Back Next

Click **Next** and the following figure is displayed:

Static IP (Fixed) Addresses

Your Internet service provides the static IP (Fixed) settings.

Be sure to enter the correct IP address for each static IP settings. For example, be sure to enter the Gateway IP Address in the Gateway Address fields and the IP Address in the IP Address fields without mixing them up.

Internet IP Address	
IP Address	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
IP Subnet Mask	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Gateway IP Address	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Domain Name Server (DNS) Address	
Primary DNS	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Secondary DNS	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>

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** and the settings take effect immediately. The setup wizard is now complete.

- (3) If the detected broadband type is **PPPoE**, the following figure is displayed:

Setup Wizard**PPPoE detected**

Successfully detected the type of Internet connection you have.

Click **Next** and the following figure is displayed:

PPPoE	
Password Setting	
Login :	<input type="text"/>
Password :	<input type="password"/>
Service Name (if required) :	<input type="text"/>
Domain Name Server(DNS) Address	
<input checked="" type="radio"/> Get Automatically From ISP	
<input type="radio"/> Use These DNS Servers	
Primary DNS :	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Secondary DNS :	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>

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	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 Use These DNS Servers and enter the IP address information of the DNS server provided by the ISP. If no DNS server information is available, select Get Automatically From ISP .
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.

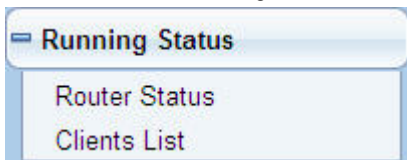
 **Note:**

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** and the settings take effect immediately. The setup wizard is now complete.

6.2 Running Status

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



The submenu contains **Router Status** and **Clients List**.

6.2.1 Router Status

Choose **Running Status** > **Router Status** and the **Router Status** page is displayed.

Device Info

System Info	
Hardware Version	V1.0
Firmware Version	V1.0
Product Name	Magic r9000
Time and Date	1971-01-01 08:18:38
Internet Port	
MAC Address	00:1E:E3:E2:A8:70
Internet Access Mode	Disconnected(PPPOE)
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:E2:A8:6F
IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
Wireless Port	
Wireless Network Name (SSID)	Magic r9000
Region	Europe
Wireless Channel	Auto
802.11 Mode	Mixed 802.11b/g/n
Wireless Radio	Enabled
Broadcast Name	ON
Wireless Isolation	OFF
Wi-Fi Protected Setup	ON
Wireless Security Mode	None

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, and traffic statistics of each port.

Click **Show Statistics** and the displayed **Statistic Information** page is as follows:

Statistic Information

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	LinkDown	0	0	0	0	0	00:00:00
LAN 1	LinkDown						00:00:00
LAN 2	LinkDown						00:00:00
LAN 3	LinkDown	1778	2032	0	579909	345491	00:00:00
LAN 4	100M Full						01:49:55
WLAN	135Mbps	6669	82009	0	2489730	20136247	01:49:48
System Up Time		01:50:03					
Poll Interval							
5		(1~86400 secs) <input type="button" value="Set Interval"/> <input type="button" value="Stop"/>					

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 Set Interval . The settings take effect immediately. If you click Stop , 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 is displayed. This page displays the information of current connection on the router.

If the WAN connection is set to **PPPoE (Manually Connect)**, the displayed **Connection Status** page is as follows:

Connection Status

Connection Time	00:00:09
Connecting to Server	Connected
Negotiation	----
Authentication	----
IP Address	10.188.0.241
IP Subnet Mask	255.255.255.255

The following table describes buttons in this page:

Button	Description
Connect	Click the button to interrupt the WAN connection.
Disconnect	Click the button to start a new WAN connection.

If the WAN connection is set to **DHCP**, the displayed **Connection Status** page is as follows:

Connection Status

IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
DHCP Server	
DNS Server	0.0.0.0
Lease Obtained	NaNDay,NaNHour,NaNMinute
Lease Expires	NaNDay,NaNHour,NaNMinute

The following table describes buttons in this page:

Button	Description
Release	Click the button to release the IP address.
Renew	Click the button to obtain a new IP address.

If the WAN connection is set to any other mode, you can view the information, but not perform any settings, in the **Connection Status** page.

For detailed descriptions of the WAN connection modes, refer to section 6.3.2 “WAN Interface Settings”.

6.2.2 Clients List

Choose **Running Status** > **Clients List** and the **Clients List** page is displayed.

Clients List

Wired Devices			
#	IP Address	MAC Address	Device Name
1	192.168.1.12	00:1D:0F:19:72:F0	unknown
Wireless Devices(Wireless intruders also show up here)			
#	IP Address	MAC Address	Device Name

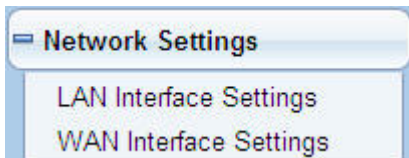
Refresh

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.

6.3 Network Settings

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



The submenu contains **LAN Interface Settings** and **WAN Interface Settings**.

6.3.1 LAN Interface Settings

Choose **Network Settings** > **LAN Interface Settings** and the **LAN Interface Settings** page is displayed.

LAN Interface Settings

LAN TCP/IP Setup					
IP Address		192	168	1	1
IP Subnet Mask		255	255	255	0
RIP Direction		Both ▼			
RIP Version		Disable ▼			
<input checked="" type="checkbox"/> Use Router as DHCP Server					
Starting IP Address		192	168	1	2
Ending IP Address		192	168	1	100
DHCP Lease Time(1 - 160 hours)		24			
Address Reservation					
#	IP Address	Device Name	MAC Address		
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>					
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					

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 Both or Out Only , the router periodically broadcasts its routing table. If it is set to Both or In Only , 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

Field	Description
	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 Address Reservation 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 Address Reservation 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 Interface Settings** page, and the **Address Reservation** page is as follows:

Address Reservation

Address Reservation Table				
	#	IP Address	Device Name	MAC Address
<input type="radio"/>	1	192.168.1.12	unknown	00:1D:0F:19:72:F0
IP Address		<input type="text"/>	<input type="text"/>	<input type="text"/>
MAC Address		<input type="text"/>		
Device Name		<input type="text"/>		

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 Add to add an entry to the Address Reservation Table .
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 Address Reservation Table .
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 Interface Settings** page.

6.3.2 WAN Interface Settings

Choose **Network Settings** > **WAN Interface Settings** and the **WAN Interface Settings** page is displayed.

WAN Interface Settings

Does your Internet Connection Require A Login? <input checked="" type="radio"/> Yes <input type="radio"/> No	
Account Name (If Required)	<input type="text" value="Hostname"/>
Internet IP Address	
<input type="radio"/> Get Dynamically From ISP	
<input checked="" type="radio"/> Use Static IP Address	
IP Address	<input type="text" value="100"/> . <input type="text" value="100"/> . <input type="text" value="100"/> . <input type="text" value="100"/>
IP Subnet Mask	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
Gateway IP Address	<input type="text" value="100"/> . <input type="text" value="100"/> . <input type="text" value="100"/> . <input type="text" value="1"/>
Domain Name Server (DNS) Address	
<input type="radio"/> Get Automatically From ISP	
<input checked="" type="radio"/> Use These DNS Servers	
Primary DNS	<input type="text" value="100"/> . <input type="text" value="100"/> . <input type="text" value="100"/> . <input type="text" value="109"/>
Secondary DNS	<input type="text" value="100"/> . <input type="text" value="100"/> . <input type="text" value="100"/> . <input type="text" value="110"/>
Router MAC Address	
<input checked="" type="radio"/> Use Default Address	
<input type="radio"/> Use Computer MAC Address	
<input type="radio"/> Use This MAC Address	<input type="text" value="00:1E:E3:AC:73:3A"/>

The router supports 3 modes of WAN connection, including **Dynamic IP (DHCP)**, **Static IP (Fixed)**, or **PPPoE**. In this page, you can select the appropriate WAN connection and configure the relevant parameters according to the actual requirements.

- **Static IP (DHCP)**

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

WAN Interface Settings

Does your Internet Connection Require A Login?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Account Name (If Required)	Hostname <input type="text"/>
Internet IP Address	
<input checked="" type="radio"/> Get Dynamically From ISP	
<input type="radio"/> Use Static IP Address	
IP Address	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
IP Subnet Mask	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Gateway IP Address	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Domain Name Server (DNS) Address	
<input checked="" type="radio"/> Get Automatically From ISP	
<input type="radio"/> Use These DNS Servers	
Primary DNS	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Secondary DNS	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Router MAC Address	
<input checked="" type="radio"/> Use Default Address	
<input type="radio"/> Use Computer MAC Address	
<input type="radio"/> Use This MAC Address	<input type="text" value="00:1E:E3:6A:31:F8"/>

The following table describes parameters in this page:

Field	Description
Does your Internet Connection Require A Login?	Select No .
Account Name	Enter the host name provided by the ISP. If the ISP does not provide it, you need not modify it.
Internet IP Address	Select Get Dynamically From ISP .
Domain Name Service (DNS) Address	Enter the IP address of the DNS server provided by the ISP. If the ISP does not provide it, select Get Automatically From ISP .
Router MAC Address	Physical address of the router. Normally, you can select Use Default Address . If the ISP requires MAC address authentication, select Use Computer MAC Address or Use This MAC Address . If you select Use Computer MAC

Field	Description
	Address , the MAC address of the current computer serves as the MAC address of the router. If you select Use This MAC Address , 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.

WAN Interface Settings

Does your Internet Connection Require A Login?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Account Name (If Required)	Hostname <input type="text"/>
Internet IP Address	
<input type="radio"/> Get Dynamically From ISP	
<input checked="" type="radio"/> Use Static IP Address	
IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
IP Subnet Mask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Gateway IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Domain Name Server (DNS) Address	
<input type="radio"/> Get Automatically From ISP	
<input checked="" type="radio"/> Use These DNS Servers	
Primary DNS	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Secondary DNS	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Router MAC Address	
<input checked="" type="radio"/> Use Default Address	
<input type="radio"/> Use Computer MAC Address	
<input type="radio"/> Use This MAC Address	<input type="text" value="00:1E:E3:6A:31:F8"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

The following table describes parameters in this page:

Field	Description
Does your Internet Connection Require	Select No .

Field	Description
A Login?	
Account Name	Enter the host name provided by the ISP. If the ISP does not provide it, you need not modify it.
Internet IP Address	Select Use Static IP Address .
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 Service Address (DNS)	Select Use These DNS Servers .
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 Use Default Address . If the ISP requires MAC address authentication, select Use Computer MAC Address or Use This MAC Address . If you select Use Computer MAC Address , the MAC address of the current computer serves as the MAC address of the router. If you select Use This MAC Address , 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**.

WAN Interface Settings

Does your Internet Connection Require A Login?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Internet Service Provider	PPPoE ▾
Login	<input type="text"/>
Password	<input type="text"/>
Service Name (If Required)	<input type="text"/>
Connection Mode	Always On ▾
Idle Timeout (In minutes)	5 <input type="text"/>
Domain Name Server (DNS) Address	
<input type="radio"/> Get Automatically From ISP	
<input checked="" type="radio"/> Use These DNS Servers	
Primary DNS	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Secondary DNS	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Router MAC Address	
<input checked="" type="radio"/> Use Default Address	
<input type="radio"/> Use Computer MAC Address	
<input type="radio"/> Use This MAC Address	<input type="text" value="00:1E:E3:6A:31:F8"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

The following table describes parameters in this page:

Field	Description
Does your Internet Connection Require A Login?	Select Yes .
Internet Service Provider	Select PPPoE .
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 several PPPoE servers are available, specify one in this field.

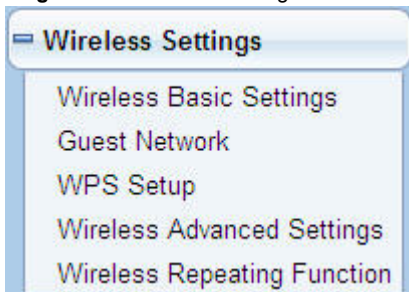
Field	Description
Connection Mode	<ul style="list-style-type: none"> ● Dial On Demand: If you select it, the system automatically establishes a connection when a network access request from the LAN is received. If no network access request is sent from the LAN within the set time of Idle Timeout, the 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. ● Always On: 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. ● Manually Connect: If you select it, you need to manually set dialup connection after startup.
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.
Domain Name Server (DNS) Address	Enter the DNS address provided by the ISP. If the ISP does not provide it, select Get Automatically From ISP .
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 Use Default Address . If the ISP requires MAC address authentication, select Use Computer MAC Address or Use This MAC Address . If you select Use Computer MAC Address , the MAC address of the current computer serves as the MAC address of the router. If you select Use This MAC Address , you

Field	Description
	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 Wireless Settings

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



The submenu contains **Wireless Basic Settings**, **Guest Network**, **WPS Setup**, **Wireless Advanced Settings**, and **Wireless Repeating Function**.

6.4.1 Wireless Basic Settings

Choose **Wireless Settings** > **Wireless Basic Settings** and the **Wireless Basic Settings** page is displayed. In this page, you can configure the basic wireless parameters.

Wireless Basic Settings

Region Selection	
Region :	Europe ▼
Wireless Network	
<input checked="" type="checkbox"/> Enable SSID Broadcast	
<input type="checkbox"/> Enable Wireless Isolation	
Name(SSID) :	Magic r9000
Mode :	Mixed 802.11b/g/n ▼
Channel:	Auto ▼
Band Width :	40M ▼
Max Transmission Rate :	Auto ▼ Mbps
Security Options	
Security Options :	None ▼

Apply Cancel

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 combinations of them. The SSID is case-sensitive.

Field	Description
Mode	<p>Select the appropriate wireless mode. The default is Mixed 802.11b/g/n.</p> <ul style="list-style-type: none"> ● 802.11b only: The maximum rate is 11 Mbps. ● 802.11g only: The maximum rate is 54 Mbps. ● 802.11n only: For 20M bandwidth, the maximum rate is 130 Mbps (150 Mbps in short preamble); for 40M bandwidth, the maximum rate is 270 Mbps (300 Mbps in short preamble). You can select Long preamble or Short Preamble in the Wireless Advanced Settings page. For details, refer to section 6.4.4 “Wireless Advanced Settings”. ● Mixed 802.11b/g: It is compatible with 802.11b and 802.11g. ● Mixed 802.11n/g: It is compatible with 802.11n and 802.11g. ● Mixed 802.11b/g/n: It is compatible with 802.11b, 802.11n, and 802.11g.
Channel	<p>Select the working channel of the wireless network. The default is Auto, which indicates that the wireless router automatically searches for the best channel in the available channels.</p>
Band Width	<p>Select the bandwidth. For 20M bandwidth, the maximum rate is 130 Mbps (150 Mbps in short preamble); for 40M bandwidth, the maximum rate is 270 Mbps (300 Mbps in short preamble).</p>
Max Transmission Rate	<p>Select one from the drop-down list that displays all rates that the system supports.</p>
Security Options	<p>Set the security encryption of the wireless network to prevent unauthorized access and listening. You can select None, Wep, WPA-PSK(AES), WPA2-PSK(AES), or WPA-PSK(TKIP)+WPA2-PSK(AES). The following describes the settings in detail.</p>

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	
Security Options :	None <input type="button" value="v"/>

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

Security Options	
Security Options :	Wep <input type="button" value="v"/>
Security Encryption(WEP)	
Authentication Type	Automatic <input type="button" value="v"/>
Encryption Strength	64 bits <input type="button" value="v"/>
Security Encryption(WEP) Key	
Key 1: <input checked="" type="radio"/>	<input type="text" value="1111111111"/>
Key 2: <input type="radio"/>	<input type="text" value="2222222222"/>
Key 3: <input type="radio"/>	<input type="text" value="3333333333"/>
Key 4: <input type="radio"/>	<input type="text" value="4444444444"/>

The following table describes parameters related to the WEP mode:

Field	Description
Authentication Type	You can select Automatic or Shared Keys . The default is Automatic .
Encryption Strength	Select the encryption strength of WEP. You can select 64 bits or 128 bits .
Key 1/2/3/4	Select one from the four keys and enter the corresponding WEP key in the field. If the Encryption Strength is set to 64 bits , enter 10 hexadecimal digits. The key can be any combination of 0-9 and A-F. If the Encryption Strength is set to 128 bits , enter 26

Field	Description
	hexadecimal digits. The key can be any combination of 0-9 and A-F.

- WPA-PSK (AES): Preshared key Wi-Fi protection access. It uses WPA-PSK standard encryption and Advanced Encryption Standard (AES).

Security Options	
Security Options :	WPA-PSK[AES]
Security Options(WPA-PSK)	
PassPhrase :	<input type="text"/> (8-63 characters or 64 hex digits)

The following table describes parameters related to the WPA-PSK (AES) 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	
Security Options :	WPA2-PSK[AES]
Security Options(WPA2-PSK)	
PassPhrase :	<input type="text"/> (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	
Security Options :	WPA-PSK[TKIP]+WPA2-PSK[AES] ▼
Security Options(WPA-PSK+WPA2-PSK)	
PassPhrase :	<input type="text"/> (8-63 characters or 64 hex digits)

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.

6.4.2 Guest Network

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

Choose **Wireless Settings > Guest Network** and the **Guest Network** page is displayed.

Guest Network

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

Security Options :

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 Network	Enable or disable a guest network. After it is enabled, you and 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 AP broadcasts its SSID to all wireless stations.

Field	Description
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 Security Options in section 6.4.1 “Wireless Basic Settings”.

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

6.4.3 WPS Setup

Choose **Wireless Settings > WPS Setup** and the **WPS Setup** page is displayed.

WPS Setup

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 **Start PBC** or press the **WPS** button on the router and the following page is displayed:

Connecting to New Wireless Client

Please click the software or hardware button on the client to start the WPS process.

Connecting[||||]

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 is displayed. The client can now visit the LAN.

Success

The wireless client has been added to the network successfully.
Click OK to go back to the Wi-Fi Protected Setup page...

- PIN mode

Add WPS Client

Select a setup method:	
<input type="radio"/> Push Button (recommended)	
<input checked="" type="radio"/> PIN (Personal Identification Number)	
If your Adapter supports WPS, please click on 'Generate a client Security Pin to input on the AP/Router/Gateway' and put the generated client PIN number here.	Enter Client's PIN: <input type="text"/> <input type="button" value="Start PIN"/>

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

Connecting to New Wireless Client

The client's PIN is **58650431**.

Connecting[|||||]

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 is displayed. The client can now visit the LAN.

Success

The wireless client has been added to the network successfully.
Click OK to go back to the Wi-Fi Protected Setup page...

6.4.4 Wireless Advanced Settings

Choose **Wireless Settings > Wireless Advanced Settings** and the **Wireless Advanced Settings** page is displayed.

Wireless Advanced Settings

Wireless Advanced Setting	
<input checked="" type="checkbox"/> Enable Wireless Router Radio	
Fragmentation Length (256-2346)	<input type="text" value="2346"/>
CTS/RTS Threshold (1-2347)	<input type="text" value="2346"/>
Preamble Mode	<input type="text" value="Long preamble"/> ▾
Transmit Power Control	<input type="text" value="100%"/> ▾
WPS Settings	
Router's PIN:	<input type="text" value="12345670"/>
<input checked="" type="checkbox"/> Enable WPS <input type="checkbox"/> Disable Router's PIN <input checked="" type="checkbox"/> Keep Existing Wireless Settings	
Wireless Card Access List	
<input type="button" value="Setup Access List"/>	

The following table describes parameters in this page:

Field	Description
Enable Wireless Router Radio	After it is selected, the WPS indicator on the rear 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 Fragmentation Length 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 Send (CTS) frame to the router,

Field	Description
	indicating that they can communicate with each other. The default value is 2346.
Preamble Mode	Set the preamble mode. The default is Long preamble . A preamble (especially the 802.11b High Rate/DSSS PHY 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 100% , 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	Functions in the WPS Setup page are available only after this option is selected. If this option is not selected, the WPS Setup menu item is greyed out.
Disable Router's PIN	The PIN mode function in the WPS Setup page is available only after this option is selected. If this option is not selected, the PIN mode option is greyed out.
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. You can select this option in the Wireless Basic Settings page.
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 Setup Access List to add, edit, or delete entries in the Wireless Card Access List page.

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

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 Wireless Card Access Setup 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 Wireless Card Access Setup 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 is displayed:

Wireless Card Access Setup

Available Wireless Cards	
Device Name	Mac Address
<input type="radio"/> unknown	00-1D-0F-19-72-F0

Wireless Card Entry(Max of terms:16)	
Device Name	<input type="text"/>
Mac Address	<input type="text"/>

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. You can enter up to 16 entries of MAC addresses.
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 **Wireless Advanced Settings** page.

6.4.5 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.

Choose **Wireless Settings** > **Wireless Repeating Function** and the **Wireless Repeater** page is displayed.

Wireless Repeater

<input type="checkbox"/> Enable Wireless Repeating Function	
<input type="checkbox"/> Disable Wireless Clients Association	
Wireless MAC of this router: 00:1E:E3:AC:73:40	
<input checked="" type="radio"/> Wireless Repeater	
Repeater IP Address:	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="1"/> <input type="text"/>
Basic Station MAC Address:	<input type="text"/>
<input type="radio"/> Wireless Basic Station	
Repeater MAC Address 1:	<input type="text"/>
Repeater MAC Address 2:	<input type="text"/>
Repeater MAC Address 3:	<input type="text"/>
Repeater MAC Address 4:	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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 Auto , this function cannot be enabled. If you try enabling the function when the channel is set to Auto , the system automatically switches to the Wireless Basic Settings page, where you can change the channel.
Disable Wireless Clients Association	If it is selected, clients cannot access the LAN.
Wireless Repeater	In this mode, the router serves as a repeater to communicate with the central base station.

Field	Description
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.

6.5 Forwarding Rule

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



The submenu contains **Port Forwarding**, **Port Triggering**, and **UPnP**.

6.5.1 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 **Forwarding Rule > Port Forwarding** and the **Port Forwarding** page is displayed.

Port Forwarding

Service Name
FTP

Service IP Address
192 . 168 . 1 . Add

Service List
Max of rules: 32

#	Server Name	Start Port	End Port	Server IP Address
---	-------------	------------	----------	-------------------

Edit Service Delete Service

Add Custom Service

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.
Service List	Display the information of configured services, including the service name, start port, end port, and server IP address.
Edit Service	Click the button to edit a service entry in the Ports - Custom Service page that is displayed.
Delete Service	Delete a service entry.
Add Custom	If the list does not contain your desired service, click the button to

Field	Description
Service	add a service in the Ports - Custom Service page that is displayed.

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

Ports - Custom Service

Service Name:	<input type="text"/>
Protocol :	TCP <input type="button" value="v"/>
Starting Port	<input type="text"/> (1~65535)
Ending Port	<input type="text"/> (1~65535)
Server IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

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 TCP/UDP , TCP , or UDP .
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.

6.5.2 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 **Forwarding Rule > Port Triggering** and the **Port Triggering** page is displayed.

Port Triggering

Enable Port Triggering

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

Max of rules: 32

#	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"/>				

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 Port Triggering – Services page that is displayed.
Edit Service	Click the button to edit a selected rule in the Port Triggering – Services page that is displayed.
Delete	Click the button to delete a selected rule.

Field	Description
Service	

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

Port Triggering - Services

Service Name	<input type="text"/>
Service User	Any <input type="button" value="v"/>
	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Service Type	TCP <input type="button" value="v"/>
Triggering Starting Port	<input type="text"/> (1~65535)
Triggering Ending Port	<input type="text"/> (1~65535)
Required Inbound Connection	
Connection Type	TCP <input type="button" value="v"/>
Starting Port	<input type="text"/> (1~65535)
Ending Port	<input type="text"/> (1~65535)

The following table describes parameters in this page:

Field	Description
Service Name	Enter the service name.
Service User	<p>You can select Any or Single address.</p> <ul style="list-style-type: none"> ● Any: Allow everybody in the user network to use the service. ● Single address: 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.
Service Type	Indicate the protocol used at the triggering port. You can select TCP/UDP , TCP , or UDP .
Triggering 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.

Field	Description
Triggering Ending Port	Set the end port of the triggering port range.
Connection Type	You can select TCP/UDP , TCP , or UDP .
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.
Ending Port	Set the end port of the triggering port range.

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

6.5.3 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.

Choose **Forwarding Rule > UPnP** and the **UPnP** page is displayed.

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	Enable or disable UPnP.

Field	Description
On	
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.

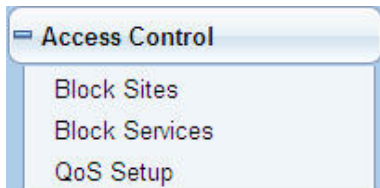
Note:

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.

6.6 Access Control

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



The submenu contains **Block Sites**, **Block Services**, and **QoS Setup**.

6.6.1 Block Sites

Choose **Access Control** > **Block Sites** and the **Block Sites** page is displayed.

Block Sites

Keyword Blocking

Never
 Per Schedule
 Always

Type Keyword or Domain Name Here.

Add Keyword

Block Sites Containing these Keywords or Domain Names(Max of terms: 32) :

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. When a user tries accessing a restricted website, a message is displayed, indicating that the firewall restricts access to the website.

The following table describes parameters and buttons in this page:

Field	Description
Keyword Blocking	Select the mode of blocking. You can select Never , Per Schedule , or Always . <ul style="list-style-type: none"> ● Never: Website blocking is disabled. ● Per Schedule: After you select it and set in System Tools > Schedules page, website blocking is enabled according to

Field	Description
	<p>the settings in the Schedules page.</p> <ul style="list-style-type: none"> ● Always: Website blocking is always enabled.
Type Keyword or Domain Name Here	<p>Enter the keyword or domain name that you want to block.</p> <p>Domain name: For example, <i>www.badstuff.com/xxx</i> (<i>bad stuff</i> indicates improper information).</p> <p>Keyword: Enter certain words, for example, blasphemy or erotic readings, included in a link.</p>
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 of 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.

6.6.2 Block Services

Choose **Access Control > Block Services** and the **Block Services** page is displayed.

Block Services

Services Blocking				
<input checked="" type="radio"/>	Never			
<input type="radio"/>	Per Schedule			
<input type="radio"/>	Always			
Block Service Rules Table				
Max of rules: 32				
	#	Service Name	Port	IP
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

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 Never, Per Schedule, or Always.</p> <ul style="list-style-type: none"> ● Never: Service blocking is disabled. ● Per Schedule: After you select it and set in System Tools > Schedules page, service blocking is enabled according to the settings in the Schedules page. ● Always: Service blocking is always enabled.
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 Block Services Setup page that is displayed.
Edit	Select a rule of service blocking in the Block Service Rules Table and click the button to edit the rule in the Block Services Setup page that is displayed.
Delete	Select a rule of service blocking in the Block Service Rules Table and click the button to delete it.

Click **Add** and the **Block Services Setup** page is displayed:

Block Services Setup

Service Type	User Defined
Protocol	TCP
Starting Port	<input type="text"/> (1~65535)
Ending Port	<input type="text"/> (1~65535)
Service Type/User Defined	<input type="text"/>
Filter Service For:	
<input type="radio"/> Only This IP Address:	<input type="text"/> 192 . <input type="text"/> 168 . <input type="text"/> 1 . <input type="text"/>
<input type="radio"/> IP Address Range:	<input type="text"/> 192 . <input type="text"/> 168 . <input type="text"/> 1 . <input type="text"/>
	to <input type="text"/> 192 . <input type="text"/> 168 . <input type="text"/> 1 . <input type="text"/>
<input checked="" type="radio"/> All IP Address:	

Add

Cancel

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 User defined . 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 TCP/UDP , TCP , or UDP .
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"> ● Only This IP Address: Only one network card on a computer is blocked. You need to enter the IP address of a network card on a computer. ● IP Address Range: 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. ● All IP Address: Network cards of all computers are blocked.

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

6.6.3 QoS Setup

Choose **Access Control > QoS Setup** and the **QoS Setup** page is displayed.

QoS Setup

QoS Control

Enable WMM (Wi-Fi multi-media) Settings

Turn Internet QoS Access On

Turn Bandwidth Control On

Uplink bandwidth: maximum Mbps

QoS Priority Rule list

Trust IP Control

Enable Trusted IP Address

Trusted IP Address

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 multi-media) Settings	Enable or disable WMM. Wireless Multimedia (WMM) is a subset of the 802.11e standard. It supports setting priorities of 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 QoS Priority Table page.
Turn Bandwidth Control On	Set the maximum uplink bandwidth at the WAN port. If the value is in units of Kbps , the maximum value is 1000 . If the value is in units of Mbps , the maximum value is 100 .
Setup QoS rule	Click the button and the QoS Setup 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 is displayed:

QoS Setup

#	QoS Policy	Priority	Description
<input type="button" value="Edit"/> <input type="button" value="Delete"/>			
<input type="button" value="Add Priority Rule"/>			
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

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 QoS Priority Table .
Delete	Click the button to delete a rule in the QoS Priority Table .
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 QoS – Priority Rules page that is displayed.

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

QoS - Priority Rules

Priority	
QoS Policy For	<input type="text"/>
Priority Category	Applications <input type="button" value="v"/>
Applications	Add A New Application <input type="button" value="v"/>
Priority	High <input type="button" value="v"/>
Specified Port Range	
Connection Type	TCP/UDP <input type="button" value="v"/>
Starting Port	<input type="text"/> (1 - 65535)
Ending Port	<input type="text"/> (1 - 65535)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

The following table describes parameters in this page:

Field	Description
QoS Policy For	Enter the name of the QoS policy.
Priority Category	Select Applications .
Applications	Select an application that you want to set. If your desired

Field	Description
	application is not in the drop-down list, select Add A New Application .
Priority	You can select Highest, High, Normal , or Low .
Connection Type	Indicates the protocol that is used at the port. You can select TCP/UDP, TCP , or UDP .
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	<input type="text"/>
Priority Category	On-line Gaming ▾
On-line Gaming	Add a new Game ▾
Priority	High ▾
Specified Port Range	
Connection Type	TCP/UDP ▾
Starting Port	<input type="text"/> (1 - 65535)
Ending Port	<input type="text"/> (1 - 65535)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

The following table describes parameters in this page:

Field	Description
QoS Policy For	Enter the name of the QoS policy.
Priority Category	Select On-line Gaming .

Field	Description
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 Add a new Game .
Priority	You can select Highest, High, Normal , or Low .
Connection Type	Indicates the protocol that is used at the port. You can select TCP/UDP, TCP , or UDP .
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	LAN Port 1
Priority Category	Ethernet LAN Port ▼
Ethernet LAN Port	1 ▼
Priority	High ▼

The following table describes parameters in this page:

Field	Description
QoS Policy For	Enter the name of the QoS policy.
Priority Category	Select Ethernet LAN Port .
Ethernet LAN Port	Select the LAN port that you want to set. You can select 1, 2, 3 , or 4 .

Field	Description
Priority	You can select Highest , High , Normal , or Low .

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

QoS - Priority Rules

Priority				
QoS Policy For	<input type="text"/>			
Priority Category	MAC Address <input type="button" value="v"/>			
MAC Device Example List				
	QoS Policy	Priority	Device Name	MAC Address
<input type="radio"/>	Pri_MAC_23C538	Normal	unknown	00:19:E0:23:C5:38
MAC Device Add List				
	QoS Policy	Priority	Device Name	MAC Address
MAC Address	<input type="text"/>			
Device Name	<input type="text"/>			
Priority	High <input type="button" value="v"/>			

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 Example List	Give an example of a priority rule of a computer.
MAC Device Add List	Display the existing priority rules of computers that have higher priorities according to MAC addresses. Enter the MAC address and device name of a computer for which you want to set high priority, and then click Add to add the rule to the list.

Field	Description
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 Highest, High, Normal , or Low .
Add	Click the button to add a priority rule to the MAC Device Add List .
Edit	Select a priority rule in the MAC Device Add List and click the button to modify the priority rule.
Delete	Select a priority rule in the MAC Device Add List and click the button to delete the priority rule from the list.
Cancel	Click the button to cancel configurations.

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

6.7 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** and the **Dynamic DNS** page is displayed. In this page, you can configure the DDNS parameters.

Dynamic DNS

<input type="checkbox"/> Use a Dynamic DNS Service	
Service Provider	DynDNS.org
Host Name	myhostname
User Name	User
Password	••••

The following table describes parameters in this page:

Field	Description
User a Dynamic DNS Service	Enable this function if you already register to the DDNS service provider.
Service Provider	Select a server from the drop-down list. You can select Dyndns.org , 3322.org , or DtDNS.com .
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.

6.8 Static Routing

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

Static Routes

Max of rules: 32					
#	Active	Name	Destination	Gateway	

Click **Add** and the following figure is displayed:

Static Routes

Active	<input type="checkbox"/>
Route Name	<input type="text"/>
Destination IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
IP Subnet Mask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Gateway IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Metric	<input type="text"/>

The following table describes parameters of adding a routing rule:

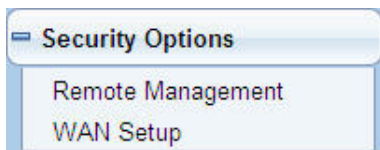
Field	Description
Active	Enable it to apply the routing rule.
Router Name	Enter the name of the static route.
Destination IP Address	Indicate the destination address or network that you want to access.

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. The parameter value ranges from 2 to 15. Usually, the value of 2 or 3 leads to the best performance. If the route is direction connection, set the Metric to 2 .

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

6.9 Security Options

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



The submenu contains **Remote Management** and **WAN Setup**.

6.9.1 Remote Management

Choose **Security Options** > **Remote Management** and the **Remote Management** page is displayed.

Remote Management

<input type="checkbox"/> Turn Remote Management On	
Remote Management Address :	http://0.0.0.0:8080
Port Number :	<input type="text" value="8080"/>
Allow Remote Access By :	
<input type="radio"/>	Only This Computer : <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
<input type="radio"/>	IP Address Range : 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"/>
<input checked="" type="radio"/>	Everyone

The remote management function allows you to configure the router in the WAN using 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).
Port Number	Specify the port of Web management for accessing a broadband router.
Allow Remote Access By	Set the IP address of a computer on which remote Web management is performed to access the router. <ul style="list-style-type: none"> ● Only This Computer: Enter an IP address. Only the specified IP address can access the router. ● IP Address Range: Enter the starting and ending IP addresses to specify the range. IP addresses within the range

Field	Description
	can access the router. ● Everyone: Everyone on the Internet can access the router.

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

6.9.2 WAN Setup

Choose **Security Options** > **WAN Setup** and the **WAN Setup** page is displayed.

WAN Setup

<input checked="" type="checkbox"/>	Disable Port Scan and DOS Protection
<input type="checkbox"/>	Respond to Ping on Internet Port
<input checked="" type="checkbox"/>	Disable IGMP Proxying
<input type="checkbox"/>	Default DMZ Server
	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="1"/> <input type="text"/>
MTU Size(616~1500 bytes)	<input type="text" value="1500"/>
NAT Filtering	
<input checked="" type="radio"/>	Secured
<input type="radio"/>	Open
<input checked="" type="checkbox"/>	Disable SIP ALG
<input type="checkbox"/>	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:

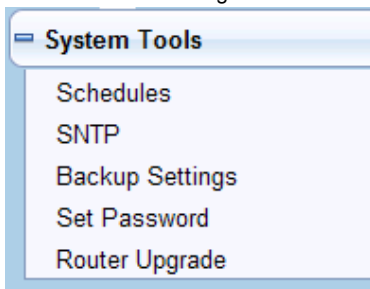
Field	Description
-------	-------------

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.
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.
Default DMZ Server	Enter the IP address of a computer or server that serves as a DMZ server.
MTU Size (616~1500 bytes)	The maximum transmission unit. Generally, the parameter value is set to 1500 bytes for most Ethernet networks, 1492 bytes for PPPoE connection, and 1436 bytes for PPTP connection. In some cases, ISPs may require smaller MTU. Do not modify the value of MTU size unless required.
NAT Filtering	<p>Determines the mode of the router to handle the input traffics.</p> <ul style="list-style-type: none"> ● Secured: 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. ● Open: It provides firewall settings of a lower security level. It allows running of almost all network applications.
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.
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.

6.10 System Tools

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



The submenu contains **Schedules**, **SNTP**, **Backup Settings**, **Set Password**, and **Router Upgrade**.

6.10.1 Schedules

Choose **System Tools** > **Schedules** and the **Schedules** page is displayed.

Schedule

Days to Block:	
<input checked="" type="checkbox"/>	Every Day
<input checked="" type="checkbox"/>	Sunday
<input checked="" type="checkbox"/>	Monday
<input checked="" type="checkbox"/>	Tuesday
<input checked="" type="checkbox"/>	Wednesday
<input checked="" type="checkbox"/>	Thursday
<input checked="" type="checkbox"/>	Friday
<input checked="" type="checkbox"/>	Saturday
Time of day to Block:(use 24-hour clock)	
<input checked="" type="checkbox"/>	All Day
Start Blocking	<input type="text" value="00"/> Hour <input type="text" value="00"/> Minute
End Blocking	<input type="text" value="23"/> Hour <input type="text" value="59"/> Minute
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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	<p>If you want to fully restrict access every day, select All Day.</p> <p>If you want to restrict access in a specific time during certain days, select the days and enter the starting and ending time.</p> <p>Note that the system uses 24-hour clock.</p>

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

6.10.2 SNTP

Choose **System Tools** > **SNTP** and the **SNTP** page is displayed.

SNTP

Time Setting				
<input type="checkbox"/> Automatically synchronize with Internet time servers				
First NTP time server :	<input type="text" value="210.72.145.44"/>			
Second NTP time server :	<input type="text"/>			
Time Configuration				
Current Router Time :	1971-01-01 09:43:17			
Time Zone :	(GMT-00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▾			
<input type="checkbox"/> Enable Daylight Saving				
Daylight Saving Offset :	<input type="text" value="0:00"/> ▾			
Daylight Saving Dates : (Time interval must be greater than the days of start month)		Month	Week	Day
	Start	<input type="text" value="Apr"/> ▾	<input type="text" value="2nd"/> ▾	<input type="text" value="Sun"/> ▾
	End	<input type="text" value="Sep"/> ▾	<input type="text" value="2nd"/> ▾	<input type="text" value="Sun"/> ▾
		<input type="button" value="Apply"/>	<input type="button" value="Cancel"/>	

In this page, you can set the time information of your router. It is strongly recommended to set the correct time on the router first. This ensures proper functioning of log, site blocking, and schedule, because these functions are based on the time setting in this page.

The following table describes parameters in this page:

Field	Description
Time Setting	<p>Automatically synchronize with Internet time servers: Enable or disable automatic synchronization with the network time server.</p> <ul style="list-style-type: none"> ● First NTP time server: Enter the URL of the primary network time server. ● Second NTP time server: Enter the URL of the secondary

Field	Description
	time server.
Time Configuration	<ul style="list-style-type: none"> ● Current Router Time: Display the current system time of the router. ● Time Zone: Select the time zone that the router is in from the drop-down list.
Enable Daylight Saving	Enable or disable daylight saving time (DST), which is a practice of temporarily advancing clocks during the summertime so that afternoons have more daylight and mornings have less. It helps saving the lighting power.
Daylight Saving Offset	Select a proper offset. If it is set to +1:00, 10:00 in the morning in standard time becomes 11:00 in the morning in DST.
Daylight Saving Dates	Set the starting time and ending time of DST.

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

6.10.3 Backup Settings

Choose **System Tools** > **Backup Settings** and the **Backup Settings** page is displayed.

Backup Settings

Save a Copy of Current Settings	<input type="button" value="Backup"/>
Restore Saved Setting from a File	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Restore"/>
Revert to Factory Default Settings	<input type="button" value="Erase"/>
Reboot Device	<input type="button" value="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 action 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.

6.10.4 Set Password

Choose **System Tools > Set Password** and the **Set Password** page is displayed.

Set Password

Set Password	
Old Password	<input type="text"/>
Set Password	<input type="text"/>
Repeat New Password	<input type="text"/>

Web Idle Time Out Settings	
Web Idle Time Out	<input type="text" value="5"/> (5 ~ 30 minutes)

In this page, you can change the password of the administrator and set the time of page timeout.

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.
Web Idle Time Out Settings	Set the time of page timeout. Its value range is 5 to 30 minutes. If you do not operate on a page for a period longer than the set time after login, the system switches to the login page when you try performing the next operation on a page.

Note:

For security measures, it is strongly recommended to change the default user name and 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 **admin** respectively.

6.10.5 Router Upgrade

Choose **System Tools > Router Upgrade** and the **Router Upgrade** page is displayed.

Router Upgrade

Locate and select the upgrade file from your hard disk:

<input type="text"/>	<input type="button" value="Browse..."/>	<input checked="" type="checkbox"/> Clear Config
<input type="button" value="Upload"/> <input type="button" value="Cancel"/>		

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. If you select **Clear Config**, the router restores to the default settings after upgrade. If you do not select it, the current settings remain.
- Step 3** Click **Upload** to start upgrading.

After the upgrade is complete, the router automatically reboots.

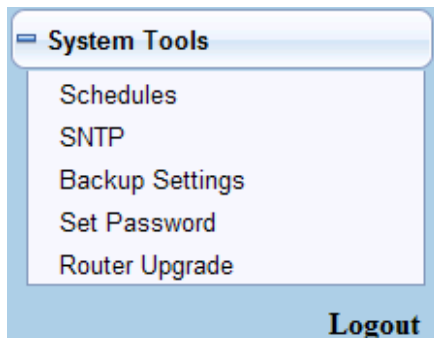
Caution:

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.

6.11 Logout

The Logout control is in the lower right of the navigation bar. 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".

To log out the router, do as follows:

- Step 1** Click **Logout** under the **System Tools** menu and the following dialog box appear:



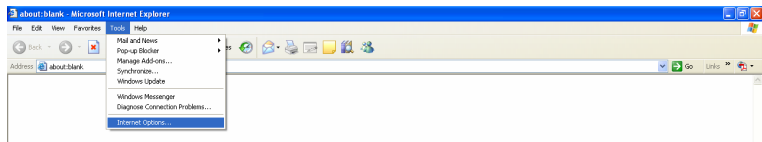
- Step 2** Click **OK** to log out. See the following figure. To return to the configuration page, click **Cancel**.

**Thank you for using the Router Configuration Utility.
Goodbye!**

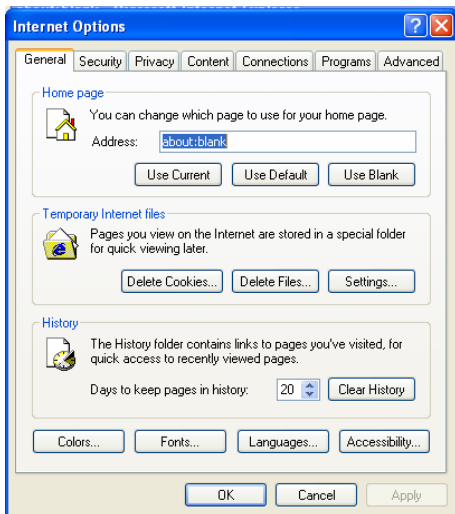
7 Troubleshooting

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:

