V1.0

Contents

1	Safety Precautions			3	
2	Overview			4	
	2.1	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	Hard	ware Installation	7	
		3.3.1	System Requirements	7	
		3.3.2	Before You Begin	7	
		3.3.3	Connecting the Device	7	
	3.4	Oper	ation Range	8	
	3.5	3.5 Roaming			
4	TCP/IP Settings and Wireless Connection Introduction			10	
	4.1	TCP/	TCP/IP Settings		
	4.2	Wirel	ess Connection Introduction	14	
5	Logg	jing In to	the Web Page		
6	Web Configuration			20	
	6.1	Setu	p Wizard	20	
	6.2	Runn	ning Status	24	
		6.2.1	Router Status	24	
		6.2.2	Clients List		
	6.3 Network Settings			29	
		6.3.1	LAN Interface Settings	29	
		6.3.2	WAN Interface Settings		
	6.4 Wireless Settings		ess 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		
		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	Acces	ss Control	61
	6.6.1	Block Sites	62
	6.6.2	Block Services	64
	6.6.3	QoS Setup	66
6.7	Dyna	mic DNS	73
6.8	Static	Routing	74
6.9	Secu	rity Options	76
	6.9.1	Remote Management	76
	6.9.2	WAN Setup	78
6.10	Syste	m Tools	80
	6.10.1	Schedules	80
	6.10.2	SNTP	82
	6.10.3	Backup Settings	83
	6.10.4	Set Password	84
	6.10.5	Router Upgrade	86
6.11	Logou	ut	87
Trout	Troubleshooting		

7

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	Describes the front and rear panels of the wireless router and the procedure for
Installation	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 300 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. Overburdened power outlets or damaged lines and plugs may cause electric shocks or fire accidents. Check the power cords regularly. If you find any power cord damage, replace the power cord at once.
- Leave proper space for heat dissipation to avoid damage caused by device overheating. Heat dissipation holes enable the device to work normally. Do not cover heat dissipation holes.
- Keep the device away from heat outlets or high temperature places. Prevent the device from direct sunlight.
- Keep the device in dry places. Do not spill any liquid on this device.
- Do not connect the 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 power or fire risks.
- Do not place the device on an unstable surface.

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, 500 mA) 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
	Use a fine needle to press Reset gently for 3 seconds and
Reset	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
WAN	network devices.
LAN1/LAN2/	RJ45 LAN interfaces, for connecting hubs, switches, or
LAN3/LAN4	computers in a LAN.
	This button is used for enabling the WPS PBC mode. When
WPS	WPS is enabled, press this button, and the AP starts to accept
	negotiation of the PBC mode.

▲ 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 sunlight. 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 is displayed.

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

🚣 Local Area Connection Properties 🛛 🔹 🔀
General Advanced
Connect using:
Broadcom 440x 10/100 Integrated Cc
This connection uses the following items:
Glient for Microsoft Networks Pile and Printer Sharing for Microsoft Networks QoS Packet Scheduler Timemet Protocol (TCP/IP)
Install
Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected ✓ Notify me when this connection has limited or no connectivity
OK Cancel

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.

	itomatically if your network supports to ask your network administrator for callu	
 Use the following IP address: 		
IP address:	192.168.1.123	
Sybnet mask:	255 . 255 . 255 . 0	
Default gateway:	192 . 168 . 1 . 1	
Obtain DNS server address au Oute the following DNS server a Preferred DNS server: <u>A</u> lternate DNS server:		

- 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:

Run	? 🛛
-	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	ping 192.168.1.1
	OK Cancel Browse

D 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.



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.

LAN or High-Speed	d Internet
Not conn	Network Connection 2 ected, Firewalled Connected, Firewalled
— (မုံ) HED HED	Disable Plerated AMD PCN
	View Available Wireless Networks
	Status
	Repair
	Bridge Connections
	Create Shortcut
	Delete
	Rename
	Properties

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 r9500. 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".

Wireless Basic Settings

Region Selection	
Region :	Europe 🗸
Wireless Network	
Enable SSID Broadcast	
Enable Wireless Isolation	
Name(SSID) :	Magic r9500
Mode :	Mixed 802.11b/g/n 💌
Channel:	Auto 🗸
Band Width :	40M 💌
Max Transmission Rate :	Auto 💙 Mbps
Security Options	
Security Options :	None
	Apply Cancel

A 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**.

	ADDON Extending flexibilities for people
UserName:	
Password:	
Login Reset	
	Magic r9500

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.



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.



Please wait a moment



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.

 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
Cli	ck Next and the following figure is displayed:
Dynamic IP Address	
Account Name (If Required)	
	Apply Cancel
En	ter the host name provided by the Internet service provider (ISP)
	the Account Name field. If the ISP does not provide it, you need t 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.
you believe you have received this message in error, please power cycle your modem (unplug the modem and plug it back in). Then close his 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	
IP Subnet Mask	
Gateway IP Address	
Domain Name Server (DNS) Address	
Primary DNS	
Secondary DNS	

Apply Cancel

The following table describes parameters in this page:

Field	Description			
IP Address	Enter the IP address of the WAN interface.			
ID Subnot Mook	Subnet mask of the WAN IP address. It is usually			
IP Subnet Mask 255.255.0.				
Gateway IP Address	Enter the IP address of the gateway if necessary.			
Drimon (DNC	Enter the IP address of the primary DNS server if			
Primary DNS	necessary.			
Constant DNC	If the ISP provides another DNS server, enter the IP			
Secondary DNS	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:

Se	tup	Wiz	ard	

	PPPoE	detected	
Successfully	detected the type	of Internet connection	you have.

Back	Next
------	------

Click Next and the following figure is displayed:

PPPoE	
Password Setting	
Login :	
Password :	
Service Name (If required) :	
Domain Name Server(DNS) Address	
 Get Automatically From ISP 	
O Use These DNS Servers	
Primary DNS :	
Secondary DNS :	

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.
Convice Name	Enter the service name provided by the ISP. If the ISP
Service Name	does not provide it, you need not enter any information.
	Select Use These DNS Servers and enter the IP
Domain Name Server	address information of the DNS server provided by the
(DNS) Address	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
Secondary DNS	address of that DNS server.

D 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:

Running Status	2
Router Status	
Clients List	

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.

_		
	1100	Info

System Info	
Hardware Version	V1.0
Firmware Version	V1.0
Product Name	Magic r9500
Time and Date	1971-01-01 09:06:10
Internet Port	
MAC Address	00:1E:E3:33:F9:C0
Internet Access Mode	Disconnected(DHCP)
IP address	0.0.00
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:E3:33:F9:BF
IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
Wireless Port	
Wireless Network Name (SSID)	Magic r9500
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

Poll Interval							
System Up Time 01:13:32							
WLAN	Auto	31155	354031	0	11580680	65449778	01:13:15
LAN 4	LinkDown	5495					00:00:00
LAN 3	LinkDown		5493 4028	0	4527049	441215	00:00:00
LAN 2	LinkDown	5402					00:00:00
LAN 1	100M/Full						01:13:22
WAN	LinkDown	0	0	0	0	0	00:00:00
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time

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	
Connect Disconnect		

Close Window

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	0.0.0.0	
DNS Server	0.0.0.0	
Lease Obtained	0Day,0Hour,0Minute	
Lease Expires	0Day,0Hour,0Minute	
	Release	
	Close Window	

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

Nired	Devices		
#	IP Address	MAC Address	Device Name
1	192.168.1.16	00:19:E0:23:C5:38	unknown
Wirele	ss Devices(Wireless intr	uders also show up here)	
#	IP Address	MAC Address	Device Name

This page displays the information of computers connected to the router, including the IP adress, 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	ection Both			
RIP Version E				
☑ Use Router as DHCP Server				
Starting IP Address		192 . 168 . 1 . 2		
Ending IP Address		192 . 168 . 1 . 254		
DHCP Lease Time(1 - 160 hours)		24		
Address Reservation				
# IP Address	Device Name	MAC Address		
	Add Edit Delete			
	Apply 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
	data sent by using RIP-2B or RIP-2M is in RIP-2 format.

Field	Description
	RIP-2B uses subnet broadcast and RIP-2M uses multicast.
Use Router as	If it is selected, the router serves as the DHCP server and
DHCP Server	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	After the DHCP lease time elapsed, the router automatically
(1 – 160 hours)	assigns new IP addresses for all connected computers.
Address	If an IP address is reserved for the network card of a PC in a
Reservation	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	Reserv	ation Table		
	#	IP Address	Device Name	MAC Address
0	1	192.168.1.16	unknown	00:19:E0:23:C5:38
IP Addre	SS	[
MAC Address		[
Device Name		[

Add Cancel Refresh

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.
Does your Internet Connection Requir	re A Login? 🔿 Yes 💿 No
Account Name (If Required)	Hostname
Internet IP Address	
Get Dynamically From ISP	
O Use Static IP Address	
IP Address	
IP Subnet Mask	
Gateway IP Address	
Domain Name Server (DNS) Address	1
Get Automatically From ISP	
O Use These DNS Servers	
Primary DNS	
Secondary DNS	
Router MAC Address	
Ose Default Address	
O Use Computer MAC Address	
O Use This MAC Address	00:1E:E3:33:F9:C0

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?	C Yes @ No
Account Name (If Required)	Hostname
Internet IP Address	
 Get Dynamically From ISP 	
C Use Static IP Address	
IP Address	
IP Subnet Mask	
Gateway IP Address	
Domain Name Server (DNS) Address	
Get Automatically From ISP	
C Use These DNS Servers	
Primary DNS	
Secondary DNS	
Router MAC Address	
Use Default Address	
C Use Computer MAC Address	
C Use This MAC Address	00:1E:E3:6A:31:F8
	Apply Cancel

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

Field	Description	
	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.

• 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?	C Yes @ No
Account Name (If Required)	Hostname
Internet IP Address	
C Get Dynamically From ISP	
CUse Static IP Address	
IP Address	
IP Subnet Mask	
Gateway IP Address	
Domain Name Server (DNS) Address	
Get Automatically From ISP	
Use These DNS Servers	
Primary DNS	
Secondary DNS	
Router MAC Address	
• Use Default Address	
C Use Computer MAC Address	
C Use This MAC Address	00:1E:E3:6A:31:F8

|--|

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 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 (DNS) Address	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.

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?	€Yes ∩No
Internet Service Provider	PPPoE -
Login	
Password	
Service Name (If Required)	
Connection Mode	Always On
Idle Timeout (In minutes)	5
Domain Name Server (DNS) Address	
C Get Automatically From ISP	
Use These DNS Servers	
Primary DNS	
Secondary DNS	
Router MAC Address	
Use Default Address	
C Use Computer MAC Address	
	00:1E:E3:6A:31:F8

Field	Description
Does your	
Internet	
Connection	Select Yes.
Require A	
Login?	
Internet	
Service	Select PPPoE.
Provider	
Login	Enter the user name for PPPoE dialup provided by the ISP.
Password	Enter the password for PPPoE dialup provided by the ISP.

Field	Description
Service Name	If several PPPoE servers are available, specify one in this field.
Connection Mode	 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

Field	Description
	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.

6.4 Wireless Settings

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

-	Wireless Settings	
	Wireless Basic Settings	
	Guest Network	
	WPS Setup	
	Wireless Advanced Settings	
	Wireless Repeating Function	

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	
Enable SSID Broadcast	
Enable Wireless Isolation	
Name(SSID) :	Magic r9500
Mode :	Mixed 802.11b/g/n 💌
Channel:	Auto 🗸
Band Width :	40M 🗸
Max Transmission Rate :	Auto 🛩 Mbps
Security Options	
Security Options :	None

Apply Cancel

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 finds 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.	
Mode	Select the appropriate wireless mode. The default is Mixed	

Field	Description		
	 802.11b/g/n. 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 802.11b/g: It is compatible with 802.11n and 802.11g. Mixed 802.11b/g/n: It is compatible with 802.11b, 202.11b, 202.11 		
Channel	802.11n, and 802.11g. 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.		
Band Width	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).		
Max Transmission Rate	Select one from the drop-down list that displays all rates that the system supports.		
Security Options	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.		

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	~

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

Security Options		
Security Options :	Wep	
Security Encryption(WEP)		
Authentication Type	Automatic 💌	
Encryption Strength	64 bits 💌	
Security Encryption(WEP) Key		
Key 1: 💿	1111111111	
Key 2: 🔘	222222222	
Кеу 3: 🔘	333333333	
Кеу 4: 🔘	444444444	

The following table describes parameters related to the WEP mode:

Field	Description
Authentication	You can select Automatic or Shared Keys. The default is
Туре	Automatic.
Encryption	Select the encryption strength of WEP. You can select 64
Strength	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
	hexadecimal digits. The key can be any combination of 0-9

Field	Description
	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 :	(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 :		(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+)	NPA2-PSK)	
PassPhrase :		(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.

D 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.

Network Pr	ofiles				
	Scheme	SSID	Security	Apply	SSID Broadcast
۲	1	SSID-002	None	NO	YES
0	2	SSID-003	None	NO	YES
0	3	SSID-004	None	NO	YES
0	4	SSID-005	None	NO	YES
Enable :	Guest Network SSID Broadcast Jest to access My Lo Wireless Isolation				
	ess Network Name(SSID):	SSID-002		
Security Op	tionsProfile 1		ll		
	tions		None		~

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
	If it is enabled, users connected to the network of this SSID can
Allow Guest to	access not only the Internet but also the LAN of the wireless
access My	router, like users connected to the network of the primary SSID.
Local Network	If this option is disabled, users connected to the network of this
	SSID cannot access the LAN of the wireless router.
	Enable or disable wireless isolation. If it is enabled, wireless
Enable Wireless	clients connected to the network of this SSID can access the
Isolation	Internet, but cannot communicate with other wireless clients or
	Ethernet clients.
Guest Wireless	Name of the guest network. The SSID can contain up to 32
Network Name	characters and can be any combination of letter, numerals, and
(SSID)	underlines. It is case-sensitive.
Security	Refer to descriptions and setting methods of Security Options
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



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

Next

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).	Start PBC
O 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[||||]

Cancel

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.



PIN mode

Add WPS Client

Select a setup method:	
O Push Button (recommended)	
IN (Personal Identification Number)	
If your Adapter supports WPS, please click on 'Generate a client Security Pin to input	Enter Client's PIN:
on the AP/Router/Gateway' and put the generated client PIN number here.	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[[]]]]]
Cancel
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.

OK

Wireless Advance	ed Setting		
Enable Wireles	s Router Radio		
Fragmentation Len	gth (256-2346)	2346	
CTS/RTS Threshold (1-2347) Preamble Mode Transmit Power Control		2346	
			100% 💌
		WPS Settings	
Router's PIN:	123456	70	
Enable WPS	Disable Router's PIN	🗹 Keep Existing Wireless Settings	
Wireless Card Ac	cess List		
Setup Acces	s List		

Field	Description
Enable Wireless	After it is selected, the WPS indicator on the rear panel of the
Router Radio	router blinks. The client can now connect to the router
	wirelessly.
Fragmentation	Set the threshold of fragmentation length. If the length of a
Length	packet is greater than the value, the packet is automatically
(256-2346)	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	Set the CTS/RTS threshold. If the length of a packet is greater
Threshold	than the value, the router sends an RTS frame to the destination
(1-2347)	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	Set the transmit power of the router. The default is 100% , which
Control	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	The PIN mode function in the WPS Setup page is available only
PIN	after this option is selected. If this option is not selected, the PIN
	mode option is greyed out.
Keep Existing	It determines whether WPS is configured on the router. If this
Wireless	option is not selected, newly added wireless clients changes the
Settings	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	You can set to allow only network cards of specific PCs to
Access List	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

Device Name	Mac Address
	Dalata
Add Edit	Delete

The following table describes parameters and buttons in this page:

Field	Description
Turn Access	Enable or disable wireless access control. If it is selected, you
Control On	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:

Available Wir	reless Cards		
	Device Name	Mac Address	
0	unknown	00:1D:0F:19:72:F0	
Wireless Card	dEntry(Max of terms:16)		
Device Name			
Mac Address			

Add	Cancel	Refresh
Add	Cancel	Refresh

The following table describes parameters in this page:

Field		Description
Available	Wireless	It displays all the available wireless network cards of
Cards		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 Nan	ne	Name of the device. You can customize one.
Mac Addres	SS	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

Disable Wireless Clients Asso	ociation
Wireless MAC of this router. 00:	1E:E3:AC:73:40
Wireless Repeater	
Repeater IP Address:	192 168 1
Basic Station MAC Address:	
O Wireless Basic Station	
Repeater MAC Address 1:	
Repeater MAC Address 2:	
Repeater MAC Address 3:	
Repeater MAC Address 4:	

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

Field	Description
	communicate with the central base station.
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 I	P Address			
192 . 16	8.1.Add			
Service L				
lax of rul	es: 32			
#	Server Name	Start Port	End Port	Server IP Address

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	Enter the IP address of the computer on which the service is to be
Address	provided.
Add	Click the button to add a service.
Service List	Display the information of configured services, including the
Service List	service name, start port, end port, and server IP address.
Edit Service	Click the button to edit a service entry in the Ports - Custom
Edit Service	Service page that is displayed.
Delete	
Service	Delete a service entry.

Field	Description
Add Custom Service	If the list does not contain your desired service, click the button to 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:		
Protocol :	ТСР	
Starting Port	(1~65535)	
Ending Port	(1~65535)	
Server IP Address		

Apply Cancel

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

ort Ti	riggering Timeout(i	in minutes) 20	(1-9999)	
Max of	rules: 32			
#	Server Name	Service Type	Required Inbound Connection	Service User
		Add Service	Edit Service Delete Service	

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	
Service User	Any 💌
Service Type	ТСР
Triggering Starting Port	(1~65535)
Triggering Ending Port	(1~65535)
Required Inbound Connecti	on
Connection Type	ТСР
Starting Port	(1~65535)
Ending Port	(1~65535)

Field	Description
Service Name	Enter the service name.
	You can select Any or Single address.
Service User	• 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.
Triccorion	The first port to which an application sends a connection request.
Triggering Storting Port	All relevant ports can be open only after connection is established
Starting Port	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

Advertiseme	nt Period(in minu	utes) 30			
Advertiseme	nt Time To Live(i	n hops) 4			
JPnP Portal	ole Table				
Active	Protocol	Int. Port	Ext. Port	IP Address	Description

Field Description

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

Note:

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

6.6 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	
ONever	
O Per Schedule	
Always	
Type Keyword or Domain Name Here.	
Add Keyword Block Sites Containing these Keyword	Is or Domain Names(Max of terms: 32) :
Delete Keyword Clear List	
Allow Trusted IP Address To Visit Bl	locked Sites
Trusted IP Address	
192 168 1	
	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	Select the mode of blocking. You can select Never, Per
Blocking	Schedule, or Always.

Field	Description
	Never: Website blocking is disabled.
	• Per Schedule: After you select it and set in System Tools >
	Schedules page, website blocking is enabled according to
	the settings in the Schedules page.
	Always: Website blocking is always enabled.
	Enter the keyword or domain name that you want to block.
Type Keyword	Domain name: For example, www.badstuff.com/xxx (bad stuff
or Domain	indicates improper information.
Name Here	Keyword: Enter certain words, for example, blasphemy or erotic
	readings, included in a link.
Add Keyword	Click the button to add the keyword or domain name you entered
	to the list under the button.
Block Sites	
containing	
these	The list displays the blocked entries. It can contain up to 32
Keywords or	entries.
Domain	
Names	
Delete	Select a keyword or domain name in the above list and click the
Keyword	button to delete it from the list.
Ole en List	Click the button and all keywords and domain names are deleted
Clear List	from the list.
Allow Trusted	
IP Address To	After it is selected, the specified computer has the full authority of
Visit Blocked	accessing the Internet.
Sites	
Trusted IP	Specify the IP address of a computer. You need to enter only a
Address	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.

Service Name	Port	IP

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

The following table describes parameters and buttons in this page:

Field	Description	
Services Blocking	 Select the mode of service blocking. You can select Never, Per Schedule, or Always. 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. 	
Block Service Rules Table	Always: Service blocking is always enabled. The table lists all services to be blocked. You can add, edit, or delete a capacity according to your capacity according to your capacity.	
Rules Table delete a service entry according to your requirement. Add Click the button to add a rule of service blocking in the B 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	

Field	Description	
	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	(1~65535)
Ending Port	(1~65535)
Service Type/User Defined	
Filter Service For:	
Only This IP Address:	192 . 168 . 1
O IP Address Range:	192 . 168 . 1 .
	to 192. 168. 1

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	

Field	Description	
	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 Defined	Enter the service name.	
Filter Service For	 It determines the computers to be blocked. 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.

2oS Setup
QoS Control
🗹 Enable WMM (Wi-Fi multi-media) Settings
Turn Internet Qos Access On
Turn Bandwidth Control On
Uplink bandwidth: maximum 100 Mbps 😒
QoS Priority Rule list
Setup QoS rule
Trust IP Control
Enable Trusted IP Address
Instant Instant <thinstant< th=""> <thinstant< th=""> <thi< td=""></thi<></thinstant<></thinstant<>

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	Enable or disable WMM. Wireless Multimedia (WMM) is a
(Wi-Fi	subset of the 802.11e standard. It supports setting priorities of
multi-media)	wireless traffics according to data types within a certain range.
Settings	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	Enable or disable QoS. After it is enabled, you can optimize the
Qos Access On	network access traffics according to the settings in the ${\bf QoS}$
	Priority Table page.
Turn Bandwidth	Set the maximum uplink bandwidth at the WAN port.
Control On	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.

Field	Description
Setup QoS rule	Click the button and the QoS Setup page is displayed
Enable Trusted	After it is enabled, you can reserve half egress bandwidth for a
IP Address	specified computer, to avoid impact to the computer because of
	Internet access behaviors by other users in the network.
Trusted IP	Specify the IP address of a computer. You need to enter only a
Address	numeral in the fourth field.

Click Setup QoS Rule and the QoS Setup page is displayed:

2	QoS Policy	Priority	Description
		Edit Delete	
		Add Priority Rule	

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.
	Click the button to set priority policy for an online game, an
Add Priority Rule	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		
Priority Category	Applications 🗸	
Applications	Add A New Application 💌	
Priority	High 💌	
Specified Port Range		
Connection Type	TCP/UDP 💌	
Starting Port	(1 - 65535)	

The following table describes parameters in this page:

Field	Description
QoS Policy For	Enter the name of the QoS policy.
Priority Category	Select Applications.
Applications	Select an application that you want to set. If your desired 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	
Priority Category	On-line Gaming 🗸
On-line Gaming	Add a new Game 💌
Priority	High 🔽
Specified Port Range	
Connection Type	TCP/UDP 💌
Starting Port	(1 - 65535)
Ending Port	(1 - 65535)

The following table describes parameters in this page:

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

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	Select the LAN port that you want to set. You can select 1, 2, 3	
Port	or 4 .	
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 Po	licy For				
Priority Category		MAC Address 👻			
MAC De	evice Example List				
	QoS Policy	Pi	riority	Device Name	MAC Address
0	Pri_MAC_23C	538 N	ormal	unknown	00:19:E0:23:C5:38
MAC De	evice Add List				
	QoS Policy	Priority		Device Name	MAC Address
MAC Ad	Idress				
Device	Name				
			High	~	

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.
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.

Field	Description
Priority	You can select Highest, High, Normal, or Low.
Add	Click the button to add a priority rule to the $\ensuremath{\textbf{MAC}}$ $\ensuremath{\textbf{Device}}$ $\ensuremath{\textbf{Add}}$
,	List.
Edit	Select a priority rule in the MAC Device Add List and click the
Lan	button to modify the priority rule.
Delete	Select a priority rule in the MAC Device Add List and click the
Delete	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 parameteres.

Dynamic DNS

Service Provider	DynDNS.org
Host Name	myhostname
User Name	User
Password	

Apply	Cancel
-------	--------

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

es: 32	
Active Name Destination Gat	teway

Click Add and the following figure is displayed:

Static Routes

Active	
Route Name	
Destination IP Address	
IP Subnet Mask	
Gateway IP Address	
Metric	

Apply Cancel

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	Indicate the destination address or network that you want to		
Address	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

Turn Remote Management On			
Remo	te Management Address :	http://0.0.0.8080	
Port N	umber :	8080	
Allow	Remote Access By :		
	Only This Computer :		
	IP Address Range :	From	
	in Address Hange .	То	
۲	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.

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. 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

Disable Port Scan and DC)S Protection
Respond to Ping on Intern	net Port
Disable IGMP Proxying	
Default DMZ Server	192 . 168 . 1 .
MTU Size(616~1500 bytes)	1500
NAT Filtering	
 Secured 	
O Open	
Disable SIP ALG	
Enable IPv6 Pass-Throug	h

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 communcation with a user or server on the WAN.

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	 Determines the mode of the router to handle the input traffics. 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:

-	System Tools		
	Schedules		
	SNTP		
	Backup Settings		
	Set Password		
	Router Upgrade		

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.

Days to Block:		
Every Day		
Sunday		
Monday		
🗹 Tuesday		
Wednesday		
I Thursday		
🗹 Friday		
🗹 Saturday		
Time of day to Block:(use	4-hour clock)	
All Day		
Start Blocking	00 Hour 00 Minute	
End Blocking	23 Hour 59 Minute	

If you already set content filtering in the **Block Sites** page or set sevice 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.
	If you want to fully restrict access every day, select All Day.
Time of Day to Block	If you want to restrict access in a specific time during certain days, select the days and enter the starting and ending time. Note that the system uses 24-hour clock.

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				
Automatically synchronize	with Inter	net time servers		
First NTP time server :	210.72.	145.44		
Second NTP time server :				
Time Configuration				
Current Router Time : 1	1971-01-01 09:43:17			
ourrent router rime.				
	GMT-00:0	0) Greenwich Mea	n Time: Dublin, Edin	burgh, Lisbon, London
	GMT-00:0	0) Greenwich Mea	n Time: Dublin, Edin	burgh, Lisbon, London
Time Zone :		0) Greenwich Mea	n Time: Dublin, Edin	burgh, Lisbon, London
Time Zone : Enable Daylight Saving Daylight Saving Offset :		-	n Time: Dublin, Edin Week	burgh, Lisbon, London Day
Time Zone :	0:00	✓		

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.

Field	Description		
Time Setting	 Automatically synchronize with Internet time servers: Enable or disable automatic synchronization with the network time server. 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.
	• Current Router Time: Display the current system time of
Time	the router.
Configuration	• Time Zone: Select the time zone that the router is in from
	the drop-down list.
	Enable or disable daylight saving time (DST), which is a
Enable Daylight	practice of temporarily advancing clocks during the
Saving	summertime so that afternoons have more daylight and
	mornings have less. It helps saving the lighting power.
Daylight Saving	Select a proper offset. If it is set to +1:00, 10:00 in the
Daylight Saving Offset	morning in standard time becomes 11:00 in the morning in
Oliset	DST.
Daylight Saving	Cat the starting time and anding time of DCT
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		
	Backup	
Restore Saved Setting from a File		
	Browse	
	Restore	
Revert to Factory Default Settings		
	Erase	
Reboot Device		
	Reboot	
	82	

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			
Old Password			
Set Password			
Repeat New Password			

Web Idle Time Out Settin	gs			
Web Idle Time Out	5	(5 ~ 30 minutes)		
		Apply Cancel		

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

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.

D 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

	Browse	Clear Confid
--	--------	--------------

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.



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:

-	System Tools
	Schedules
	SNTP
	Backup Settings
	Set Password
	Router Upgrade
	Logout

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

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

🗿 about:blank - Microsoft	Internet Explorer		
File Edit View Pavorites	Tools Help		
3 Back - 6 - 🖹	Pop-up Blocker	s 😧 🍰 🗟 🔜 🛄 🏭 🍇	
Address 🗃 about:blank	Manage Add-ons Synchronize Windows Update		💌 🔂 Go Unis 🎽 📆 -
	Windows Messenger Diagnose Connection Problems		
	Internet Options		

(2) Click Delete Cookies and Delete Files.

Internet	Options					? 🛛		
General	Security	Privacy	Content	Connections	Programs	Advanced		
Home	page							
	,	_		ge to use for yo	ur home pag	je.		
	J Addres	_	out:blank					
	Use Current Use Default Use Blank							
Temp	Temporary Internet files							
		you view k viewing		rnet are stored	in a special	folder		
	(Delete Co	okies	Delete Files	Settin	gs		
Histor	y							
				links to pages ; ewed pages.	you've visite	d, for		
	Days to	o keep pa	ges in histo	ну: 20 💲	Clear H	listory		
C	lors	For	its	Languages.	Acce	ssibility		
			ОК	Ca	ncel	Apply		

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:

