MC-WR11SE
BROADBAND
WIRELESS ROUTER

USER'S MANUAL

MODECOM

Contents:

About User Manual

This user manual describes how to install and configure the MC-WR11SE 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 : Configuring Your Computer and Wireless Connection	Describes how to set the TCP/IP for your computer and how to connect to MC-WR11SE 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 the Web pages and how to configure the parameters.

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 configuring static routing
- Support software 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 wireless repeater
- Support guest network
- Support restricting IP bandwidth
- Support filtering by MAC address and URL
- Support wireless security authentication
- Support 6 types of WAN connection modes, including DHCP, static IP, PPPoE, PPTP, L2TP, and Bridge
- Support remote access control
- Support firewall
- Support system status display
- Support backing up and restoring configuration files
- Support WMM

1. Safety Precautions

Before operating MC-WR11SE, 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.
- 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, high temperature places, and 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 this device on an unstable surface.

2. Overview

2.1 Product Introduction

MC-WR11SE is a high-performance network access device. It is fully compatible with IEEE802.11b, IEEE802.11g and IEEE802.11n standards. It can provide reliable and convenient access service for individual users and SOHO (Small Office, Home Office). It features Web-based GUI, allowing users to easily modify settings to connect the device to ISP (Internet Service Provider) and conveniently perform upgrade using the WEB page.

2.2 Packing list

Please check that your packing list includes the following items:
- 1 x MC-WR11SE
- 1 x Power adapter (12V DC, 500 mA)
- 1 x Ethernet cable
- 1 x Quick Installation Guide
- 1 x Warranty Card

3. Hardware Description and Hardware Installation

3.1 Front Panel and LED Status

There are 8 LED indicators on the front panel of MC-WR11SE. By observing their status, you can check whether the device runs normally.
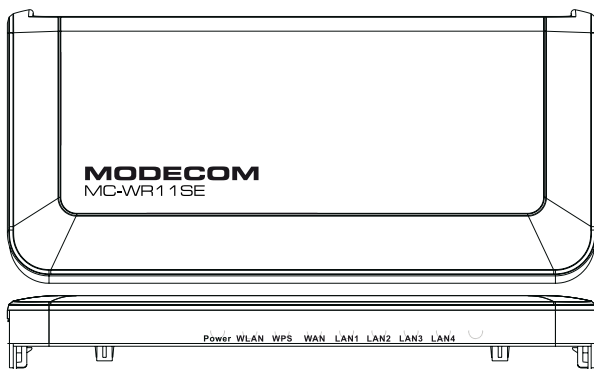
The following table describes the status of LED indicators on the front panel.

Indicator	Color	Status	Description
Power	Green	On	Power is on.
	N/A	Off	Power is off or the device is down.
WLAN	Green	On	The WLAN connection is in the communication state.
	Green	Blink	Data is being transmitted and received in the WLAN.
	N/A	Off	The WLAN connection is in the non-communication state.
WPS	Green	On	Connection succeeds under WPS (Wi-Fi Protected Setup).
	Green	Blink	Negotiation is in progress under WPS.
	N/A	Off	WPS is disabled.
WAN	Green	On	WAN connection succeeds.
	Green	Blink	Data is being transmitted.
	N/A	Off	No WAN connection.
LAN1/2/3/4	Green	On	LAN connection succeeds.
	Green	Blink	Data is being transmitted.
	N/A	Off	No LAN connection.

3.2 Rear Panel and Interface Description
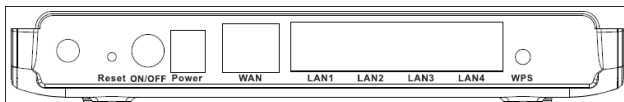
The following table describes interfaces and buttons on the rear panel.

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.
LAN1/2/3/4	RJ45 LAN interfaces, for connecting hub, switch, or computer in the 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 negotiation of PBC mode.

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.

3.3.1 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. Keep it away from direct sunlight. Avoid any metal in the device.
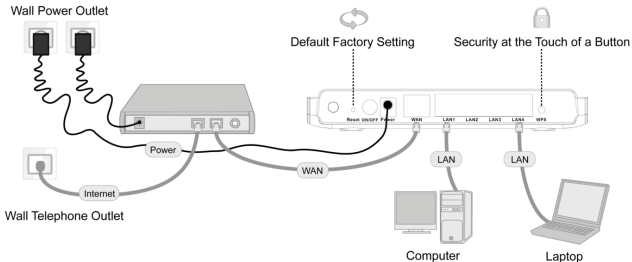- Place the device in the center of the area, and try to optimize the wireless coverage.

3.3.1 Connecting the Device

To connect the device, do as follows:

Step 1 Connect one end of the RJ45 cable to the LAN interface of MC-WR11SE.

Step 2 Connect the other end of the RJ45 cable to your PC.

Step 3 Connect the power adapter to the power socket of MC-WR11SE.


3.4 Operation Range

The operation range of the wireless router depends on the actual environment. The path and effect of signal transmission vary with 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.

4. Configuring Your Computer and Wireless Connection

4.1 Configuring Your Computer

The following takes Windows XP as an example. Do as follows to manually set the network adapter of your computer:
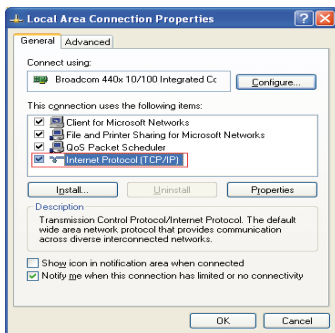
Step 4 Right-click the icon of My Network Places and choose Properties to display the Network Connections window.
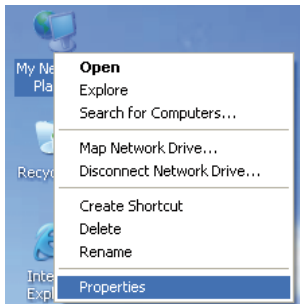

Step 5 Right-click the icon of a network interface card or wireless network adapter and choose Properties.

Step 6 Double-click Internet Protocol (TCP/IP).

Step 7 Set the IP address of your computer to 192.168.1.X (X is an integer in the range of 2 to 254), and the MAC address to 255.255.255.0. Set the gateway and the IP address of the DNS server. You can leave them blank if you do not know information about the gateway and DNS server. Click OK.

www.modecom.eu
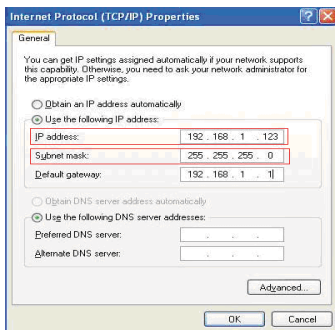
⚠ Note:

After you finish configuring the MC-WR11SE router, the domestic gateway can set the Internet protocol for the PC's network adapter. Set the IP address and DNS server to Obtain an IP address automatically.

4.2 Configuring Wireless Configuration

The following takes Windows XP as an example. Do as follows to connect the wireless network adapter of your PC to MC-WR11SE:

Click the [icon] icon displayed at the right bottom corner of the desktop (Note: Ensure that your PC is installed with a wireless network adapter).

Step 1 In the Wireless Network Connection page, double-click the desired wireless network.
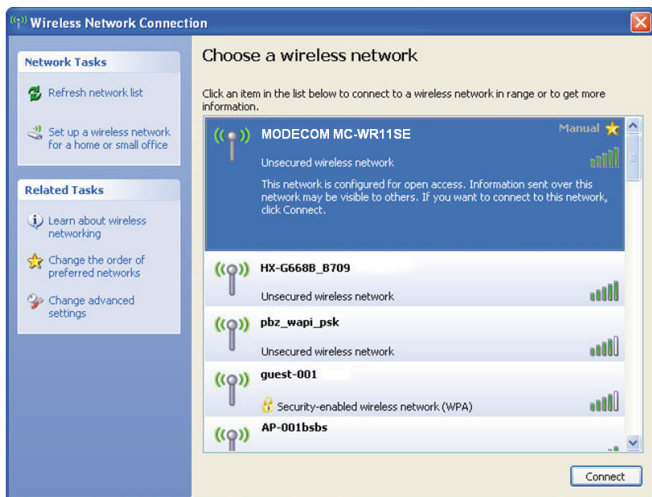
Step 2 Your computer successfully connects to the wireless net-work when Connected is displayed on the right upper corner.
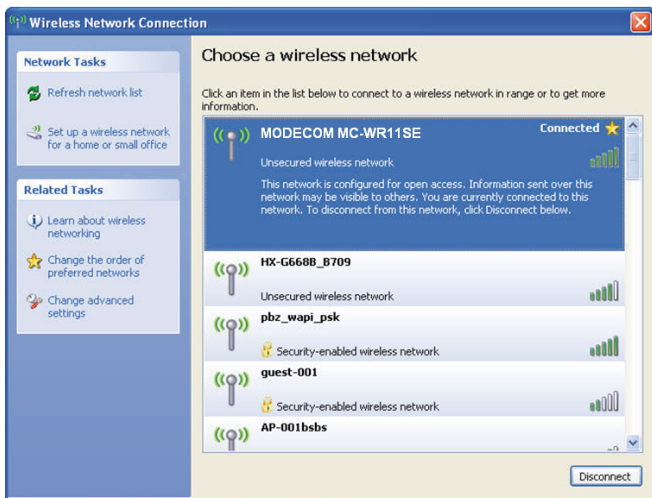
⚠ Note:

The default SSID of the MC-WR11SE router is MODECOM MC-WR11SE.

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 displayed window as shown in the following figure, enter the user name and password, and click Login. The default user name and password are both admin.
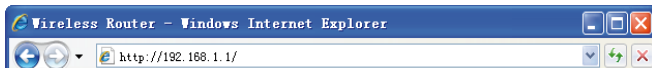

After logging in to the Web page, you can view, configure and modify the router settings. To make the settings and changes take effect, you need to reboot the wireless router sometimes.

⚠ 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 basic network parameters for accessing the Internet by following this wizard.

To configure the setup wizard, take the follow steps.

Step 3 After login, click Setup Wizard in the navigation bar on the left pane of the page. The Setup Wizard page appears.

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 4 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 appears.

Setup Wizard

Dynamic IP (DHCP) detected
Successfully detected the type of Internet connection you have.

[Back] [Next]

Click Next and the following figure appears.

Dynamic IP Address

Account Name (If Required)

[Finish] [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 from the connected DHCP server, including the IP address, subnet mask, gateway, and IP address of the DNS 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 appears.

Click Next and the following figure appears:

The following table describes parameters in this page:

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

After setting, click Apply and the settings take effect immediately. The setup wizard is now complete.

(3)   If the detected broadband type is PPPoE, the following figure appears.

Setup Wizard

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

Back Next

Click Next and the following figure appears:

PPPoE

Password Setting
Login :
Password :
Service Name (if required) :
Domain Name Server(DNS) Address
○ Get Automatically From ISP
● Use These DNS Servers
Primary DNS :
Secondary DNS :

Finish Cancel

The following table describes parameters in this page:

Field	Description
Login	Enter the user name provided by the ISP.
Password	Enter the password provided by the ISP.
Service Name (If required)	Enter the service name provided by the ISP. If the ISP does not provide it, you need not enter any information.
Domain Name Server (DNS) Address	Select **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.
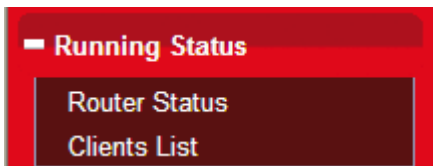
The submenu contains Router Status and Clients List.

6.2.1 Router Status

Choose Running Status > Router Status and the Router Status page appears.

Router Status

System Info	
Hardware Version	V1.0.0
Firmware Version	V1.0.0
Product Name	Wireless Router
Work Mode	Gateway Mode
Time and Date	2011-01-01 20:24:15
Internet Port	
MAC Address	00:1E:E3:72:FD:A6
Internet Access Mode	Disconnected(DHCP)
IP address	0.0.0.0
IP Subnet mask	0.0.0.0
Default Gateway	0.0.0.0
Domain Name Server	0.0.0.0,0.0.0.0
LAN Port	
MAC Address	00:1E:E3:72:FD:A5
IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
Wireless Port	
Wireless Network Name (SSID)	MODECOM MC-WR11SE
Region	Europe
Wireless Channel	2.437GHz- CH6
802.11 Mode	Mixed 802.11b/g/n
Wireless Radio	Enabled
Broadcast Name	ON
Wireless Isolation	OFF
Wi-Fi Protected Setup(WPS)	ON
Wireless Security Mode	None

Show Statistics   Connection Status

This page displays the information of the current running status of the device, including system information, connection status of the

Internet port, LAN port, and wireless port, and traffic statistics of each port.

Click Show Statistics and the Statistic Information page as shown in the following figure appears:

Statistic Information

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	100M/Full	11	9173	0	3733	1213535	00:14:07
LAN 1	100M/Full						00:14:01
LAN 2	LinkDown	4205	3341	0	3132980	483133	00:00:00
LAN 3	LinkDown						00:00:00
LAN 4	LinkDown						00:00:00
WLAN	Auto	4624484	29666576	0	0	254	03:28:24
System Up Time		00:25:39					
Poll Interval							

5 (1~86400 secs) [Set Interval] [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 appears. This page displays the information of current connection on the router.

If the WAN connection is set to PPPoE (Manually Connect), the Connection Status page is as shown in the following figure:

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

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 Connection Status page is as shown in the following figure:

Connection Status

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

Release   Renew

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 6.4.2 "WAN Interface Settings".

6.2.2   Clients List

Choose Running Status > Clients List and the Clients List page appears.

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 Mode Settings

Click Mode Settings and the Mode Settings page appears. In this page, you can choose router mode or WISP mode for the router.

Mode Settings

Please choose a mode as follows:

◉ Router Mode
The DHCP server is enabled by default in this mode. It is suggested that the computer's IP address and DNS address is set to obtain automatically.

◯ WISP Mode
The DHCP server is enabled by default in this mode. It is suggested that the computer's IP address and DNS address is set to obtain automatically.

[Apply] [Cancel]

In router mode, the device works as a router. WDS function is supplied to expand wireless network. If WDS function is enabled, the device could work as a "Wireless Repeater" and communicate with another "Base Station mode" wireless device to expand the "Base Station", or it could work as a "Wireless Base Station" and communicate with another "Repeater-mode" wireless device to expand the "Repeater".

In WISP mode, the WLAN Interface would serve as the WAN Interface. In the "Wireless Site Survey" page, you should scan wireless sites, select and associate the wireless modem which you want to connect, and then in the "WAN Interface Settings" page, configure the WAN Interface parameters. After that, you can surf the Internet. Other functions are the same as the corresponding functions in router mode, but it does not support WDS function.

6.4 Network Settings

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

■ Network Settings

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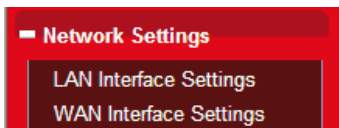
The submenu contains LAN Interface Settings and WAN Interface Settings.

6.4.1 LAN Interface Settings

Choose Network Settings > LAN Interface Settings and the LAN Interface Settings page appears.

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.

Field	Description
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. 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
⬤	1	192.168.1.21	unknown	00:22:B0:69:0D:64

IP Address	___ . ___ . ___ . ___
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.

6.4.2 WAN Interface Settings

Choose Network Settings > WAN Interface Settings and the WAN Interface Settings page appears.

The router supports 3 modes of WAN connection: Dynamic IP (DHCP), Static IP (Fixed) and PPPoE. In this page, you can select an 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:

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.**

Field	Description
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.

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.

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 **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 a**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?	● 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	
● Get Automatically From ISP	
● Use These DNS Servers	
Primary DNS	10 28 100 1
Secondary DNS	10 28 100 2
Router MAC Address	
● Use Default Address	
● Use Computer MAC Address	
● Use This MAC Address	00:1E:E3:72:FD:A6
	Apply 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	**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.

Field	Description
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.

6.5 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 Repeater.

6.5.1 Wireless Basic Settings

Choose Wireless Settings > Wireless Basic Settings and the Wireless Basic Settings page appears. 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) :	MODECOM MC-WR115E
Mode :	Mixed 802.11b/g/n
Channel:	6
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 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.

Field	Description
Mode	Select the appropriate wireless mode. The default is **Mixed 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 0" 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	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.

Field	Description
Security Options	Set the security encryption of the wireless network, to prevent unauthorized access and listening. You can select **None**, **Wep**, **WPA-PSK(TKIP)**, **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.

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

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 bit**s or **128 bits.**

Field	Description
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 and A-F.

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

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

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

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

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 :	WPA-PSK[TKIP]+WPA2-PSK[AES]
Security Options(WPA-PSK+WPA2-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.

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.

6.5.2 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 appears.

Guest Network

	Scheme	SSID	Security	Apply	SSID Broadcast
⊙	1	MODECOM MC-WR11SE-001	None	NO	YES
○	2	MODECOM MC-WR11SE-002	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):	MODECOM MC-WR11SE

Security Options--Profile 1

Security Options :	None

[Apply] [Cancel]

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.
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 6.5.1 "Wireless Basic Settings".

After setting, click Apply to save the settings.

6.5.3 WPS Setup

Choose Wireless Settings > WPS Setup and the WPS Setup page appears.
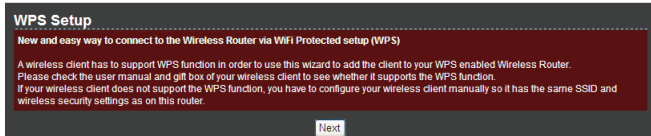
WPS refers to Wi-Fi Protected Setup. You can use the WPS setup function to add a wireless client to a network, without setting specific parameters, such as SSID, security mode, and password. To use this function, a wireless client must support WPS. If the wireless client does not support WPS, you must 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
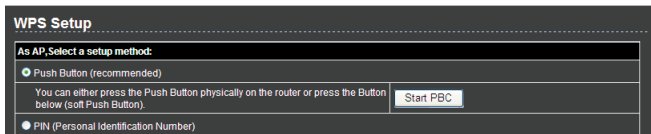
Select Push Button (recommended) and click Start PBC or press the WPS button on the router and the following page appears:
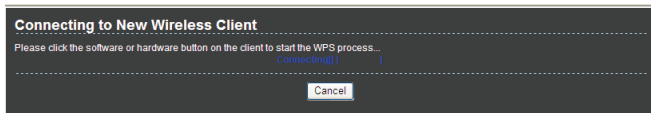
Press the button on the network card or click the button in the software page within two minutes to start WPS connection. After WPS connection is established, the following page appears. The client can now visit the LAN.

Success

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

OK

PIN mode

WPS Setup

As AP, Select a setup method:

● Push Button (recommended)

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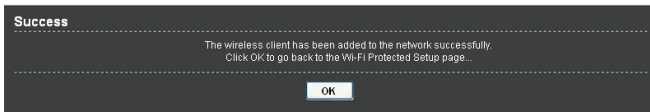
Select PIN (Personal Identification Number) and enter the PIN of the network (refer to the client of the network card), then click Start PIN to start WPS connection. The following page appears:

Connecting to New Wireless Client

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

Connecting!

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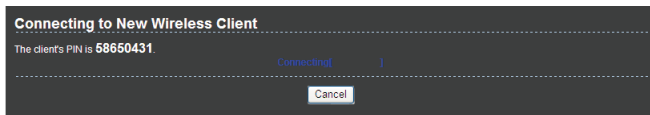
Click the PIN button on the client of the network card within two minutes to start WPS connection. After WPS connection is established, the following page appears. The client can now visit the LAN.

Success

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

OK
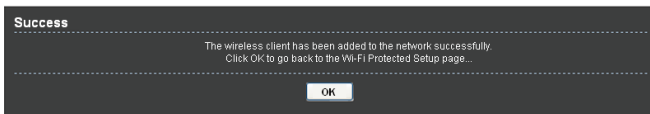
6.5.4   Wireless Advanced Settings

Choose Wireless Settings > Wireless Advanced Settings and the Wireless Advanced Settings page appears.

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.

Field	Description
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, 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.
Guard Interval	You may select short guard interval or long guard interval.
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.

Field	Description
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 appears:

Wireless Card Access List

☐ Turn Access Control On

Device Name	Mac Address

Add Edit Delete

Apply Cancel

WIRELESS ROUTER

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 appears:

Wireless Card Access Setup

Available Wireless Cards		
	Device Name	Mac Address
●	gj1301d	00:0C:43:26:60:40
Wireless Card Entry(Max of terms:16)		
Device Name		
Mac Address		

Add Cancel Refresh

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.

www.modecom.eu

Field	Description
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.

6.5.5   Wireless Repeater

The submenu Wireless Repeater is only available when the router is set to Router Mode. Refer to 6.3 Mode Settings.

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 Repeater and the Wireless Repeater page appears.

Wireless Repeater

- Enable Wireless Repeating Function
- Disable Wireless Clients Association
  - Wireless MAC of this router: 00:1E:E3:72:FD:A5
- Wireless Repeater

Repeater IP Address:	192 168 1
Basic Station MAC Address:	

- Wireless Basic Station

Repeater MAC Address 1:	
Repeater MAC Address 2:	
Repeater MAC Address 3:	
Repeater MAC Address 4:	

Apply   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.
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.

6.5.6 Wireless Site Survey

The submenu Wireless Site Survey is only available when the router is set to WISP Mode. Refer to 6.3 Mode Settings.

When WISP is enabled, the device can be connected with any wireless site. Click the "Site Survey" button, and the router will survey wireless sites.

Choose Wireless Settings > Wireless Site Survey and the Wireless Site Survey page appears.

Wireless Site Survey

This page help you to configure the wireless site survey.
Step1: Click "Site Survey" button to survey wireless sites when WISP mode is enabled. If any wireless site is found, the results will be displayed in the Site Survey List three seconds later, you could select anyone wireless modem to connect it manually. Then click "Next".

Site Survey

Number of Sites Scaned:14

Site Survey List

#	SSID	BSSID	Channel	Signal	Encrypt	Select
1	ChinaNet-yQVK	E0:1D:3B:2C:73:D4	6	50%	WPA-PSK(AES)WPA2-PSK(AES)	●
2	ChinaNet-9u9y	E0:1D:3B:2C:78:8C	4	39%	WPA-PSK(AES)WPA2-PSK(AES)	●
3	outformasia-datin	80:81:00:75:8B:48	5	29%	WPA-PSK(AES/TKIP)/WPA2-PSK(AES/TKIP)	●
4	Sagemcom F2744	00:15:58:CE:92:6B	1	20%	None	●
5	MobileWiFi-3391	0C:37:DC:EF:33:91	1	20%	WPA-PSK(AES)	●
6	ChinaNet-asia	00:27:19:FC:54:BE	2	0%	WEP	●
7	ÃÙÂê13¸ò1	02:E0:CB:07:91:2C	10	0%	WEP	●
8	TP-LINK_outform	14:E6:E4:2C:B9:28	6	0%	WPA-PSK(AES/TKIP)/WPA2-PSK(AES/TKIP)	●
9	TW-3A	00:1F:A4:91:2A:7E	11	0%	WPA2-PSK(AES)	●
10	TW_2A02	EC:6C:9F:07:7A:44	1	0%	WPA2-PSK(AES)	●
11	ÓÐ'ùÓÆ¶ˆ£ ÃÜª£° 12345£©	02:E0:2B:C2:86:53	10	0%	WEP	●
12	outformasia-office	1C:FA:68:C8:94:F4	6	0%	WPA-PSK(AES/TKIP)/WPA2-PSK(AES/TKIP)	●
13	ChinaNet-pSbA	A8:AD:3D:2F:F3:98	11	0%	WPA-PSK(AES)WPA2-PSK(AES)	●
14	JF-008	00:A1:B0:61:16:5F	8	0%	WPA-PSK(TKIP)WPA2-PSK(TKIP)	●

Next

Configure the device manually so it has the same wireless security settings as the wireless modem network which you selected, then device can communicate with the selected network.

Next you should configure the parameters of the WAN interface in "WAN Interfacd Settings" page. After that you can surf the Internet.

6.6 Forwarding Rule

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

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

6.6.1 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 appears.

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 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 appears:

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.

Field	Description
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.

6.6.2 Port Triggering

Certain applications, such as WAN network games, video confer-ences, 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 appears.

Port Triggering

☐ Enable Port Triggering				
Port Triggering Timeout(in minutes)	20	(1-9999)		
Max of rules: 32				
#	Server Name	Service Type	Required Inbound Connection	Service User

Add Service   Edit Service   Delete Service

Apply   Cancel

The following table describes parameters in this page:

Field	Description
Enable Port Triggering	Enable or disable port triggering.
Port Triggering Timeout (in minutes)	Enter a value not greater than 9999. The timeout value controls the inactive timer at the specified ingress port. Upon timeout of the inactive timer, the ingress port is disabled.

Field	Description
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 Service	Click the button to delete a selected rule.

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

The following table describes parameters in this page:

Field	Description
Service Name	Enter the service name.
Service User	You can select **Any** or **Single address.** **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.**

Field	Description
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.
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.

6.6.3 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 appears.

The following table describes parameters in this page:

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

Note:

Only applications that support UPnP can use the function.

The functionality of UPnP requires support by the application and operating systems such as Windows ME, Windows XP, and Windows Vista.

6.7 Access Control

Click Access Control and the extended navigation menu is shown as follows:
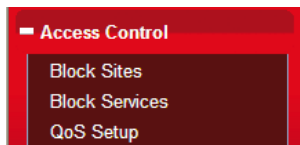
The submenu contains Block Sites, Bloack Services, and QoS Setup.

6.7.1 Block Sites

Choose Access Control > Block Sites and the Block Sites page appears.

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 appears, indicating that the firewall restricts access to the website.

The following table describes parameters and buttons in this page:

Field	Description
Keyword Block-ing	Select the mode of blocking. You can select **Never**, **Per Schedule**, or **Always.** **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.

Field	Description
Type Keyword or Domain Name Here	Enter the keyword or domain name that you want to block. Domain name: For example, *www.badstuff.com/xxx* (*bad stuff* indicates improper information. Keyword: Enter certain words, for example, blasphemy or erotic readings, included in a link.
Add Keyword	Click the button to add the keyword or domain name you entered to the list under the button.
Block Sites containing these Keywords or Domain Names	The list displays the blocked entries. It can contain up to 32 entries.
Delete Keyword	Select a keyword or domain name in the above list and click the button to delete it from the list.
Clear List	Click the button and all keywords and domain names are deleted from the list.
Allow Trusted IP Address To Visit Blocked Sites	After it is selected, the specified computer has the full authority 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.

6.7.2 Block Services

Choose Access Control > Block Services and the Block Services page appears.

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
S e r v i c e s 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. **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 appears:

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 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.

6.7.3   QoS Setup

Choose Access Control > QoS Setup and the QoS Setup page appears.

QoS 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

Trusted IP Address　　192 . 168 . 1 .

Apply　Cancel

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.**

Field	Description
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 appears:
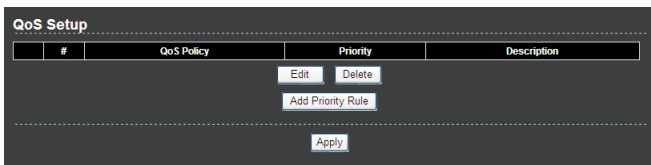
The following table describes buttons in this page:

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 appears:

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.**

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

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.**

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

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

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.**
Priority	You can select **Highest**, **High**, **Normal**, or **Low.**

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

The following table describes parameters in this page:

Field	Description
QoS Policy For	Enter the name of the QoS policy.
Priority Category	Select MAC Address.
MAC Device List	Display the existing priority rules of computers that have higher priorities according to MAC addresses. 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.
Priority	You can select **Highest**, **High**, **Normal**, or **Low.**
Add	Click the button to add a priority rule to the **MAC Device List.**
Edit	Select a priority rule in the **MAC Device List** and click the button to modify the priority rule.
Delete	Select a priority rule in the **MAC Device List** and click the button to delete the priority rule from the list.
Refresh	Click the button to update the priority rules in the **MAC Device List.**

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

6.8 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 in-

stalled 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 appears. In this page, you can configure the DDNS parameteres.

Dynamic DNS

☐ Use a Dynamic DNS Service	
Service Provider	DynDNS.org
Host Name	myhostname
User Name	User
Password	••••

Apply Cancel

The following table describes parameters in this page:

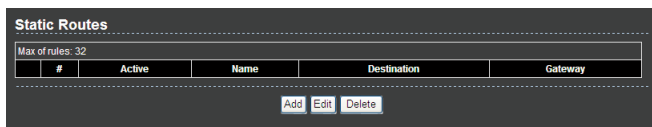| Field	Description
User a Dynamic DNS Service	Enable this function if you already register to the DDNS service provider.
Service Provider	Select a server from the drop-down list. You can select **Dyndns.org**, **3322.org**, **freedns.afraid.org**, **DtDNS.com**, or **www.oray.cn.**
Host Name	Enter the 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.

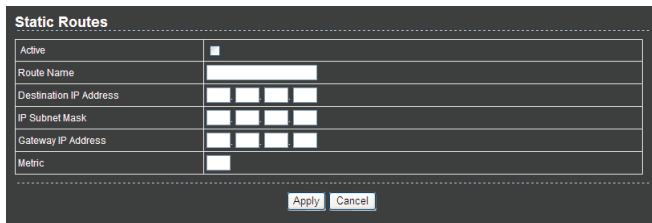After setting, click Apply to save the settings.

6.9 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 for-

warding 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 appears. 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

Add Edit Delete

Click Add and the following figure appears:

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 Address	Indicate the destination address or network that you want to access.
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.

Field	Description
Metric	Indicate the number of other routers in the user network. Its value range is 2 to 15. Usually, the value of 2 or 3 leads to the best performance. If the route is direction connection, set the **Metric** to **2.**

After setting, click Apply to save the settings.

6.10 Security Options

Click Security Options and the extended navigation menu is shown as follows:
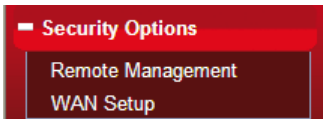
The submenu contains Remote Management and WAN Setup.

6.10.1 Remote Management

Choose Security Options > Remote Management and the Remote Management page appears.

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

The following table describes parameters in this page:

Field	Description
Turn Remote Management On	Enable or disable remote Web management.
Remote Management Address	IP address that is used to access the router from the Internet. The default is http://0.0.0.0:8080. When accessing the router, you need to enter the WAN IP address of the router, along with **:** and the port number in the address bar (of IE) or the location bar (of Netscape).
Port Number	Specify the port of Web management for accessing the broadband router.
Allow Remote Access By	Set the IP address of the computer on which remote Web management is carried out to access the router. **Only This Computer**: Only the specified IP address can access the router. You need to enter an IP address. **IP Address Range**: A number of IP addresses on the Internet can access the router. You need to enter the starting and ending IP addresses to specify the range. **Everyone**: Everyone on the Internet can access the router.

After setting, click Apply to save the settings.

6.10.2 WAN Setup

Choose Security Options > WAN Setup and the WAN Setup page appears.

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.

The following table describes parameters in this page:

Field	Description
Disable Port Scan and DOS Protection	This function protects your LAN against DoS attack. Do not disable this firewall function unless a special situation occurs.
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 (in bytes)	The maximum transmission unit. Normally, it is 1500 bytes for most Ethernet networks, 1492 bytes for PPPoE connection, and 1436 bytes for PPTP connection. Certain ISPs may require smaller MTU, but this is a rare case. Do not modify the value of MTU size unless it is necessary for your ISP connection.

Field	Description
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.
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.

6.11 System Tools

Click System Tools and the extended navigation menu is shown as follows:
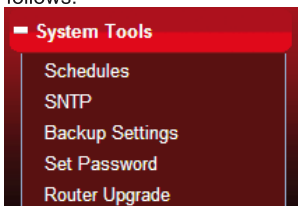
The submenu contains Schedules, SNTP, Backup Settings, Set Password and Router Upgrade.

6.11.1 Schedules

Choose System Tools > Schedules and the Schedule page appears.

Schedule

Days to Block:	
☑ Every Day	
☑ Sunday	
☑ Monday	
☑ Tuesday	
☑ Wednesday	
☑ Thursday	
☑ Friday	
☑ Saturday	
Time of day to Block:(use 24-hour clock)	
☑ All Day	
Start Blocking	00 Hour 00 Minute
End Blocking	23 Hour 59 Minute

Apply   Cancel

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

After setting, click Apply to save the settings.

6.11.2 SNTP

Choose System Tools > SNTP and the SNTP page appears.

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	**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 time server.
Time Configuration	**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.

Field	Description
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.

6.11.3 Backup Settings

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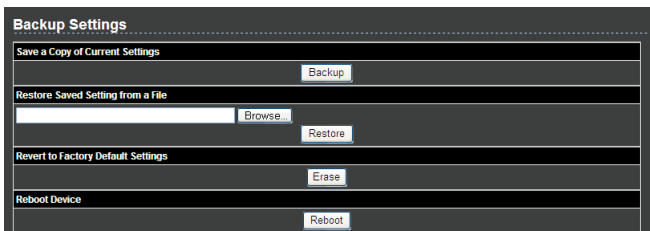
In this page, you can export the configuration information of the router in a file to the computer for later use, import a previously saved or a new configuration file, restore the factory default settings of the router, and reboot the router.

• 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 3-6 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.

6.11.4 Set Password

Choose System Tools > Set Password and the Set Password page appears.

Set Password	
Set Password	
Old Password	
Set Password	
Repeat New Password	
Apply Cancel	
Web Idle Time Out Settings	
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.

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.

6.11.5 Router Upgrade

Choose System Tools > Router Upgrade and the Router Upgrade page appears.

Router Upgrade

Locate and select the upgrade file from your hard disk:

[   ] Browse...   ☑ Clear Config

Upload   Cancel

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

Step 5 Click Browse… to navigate to the latest software.

Step 6 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 7 Click Upload to start upgrading.

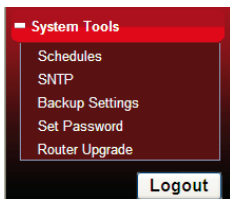After the upgrade is complete, the router automatically reboots.

⚠ 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.

6.12 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!

Environment protection:

This symbol on our product nameplates proves its compatibility with the EU Directive 2002/96 concerning proper disposal of waste electric and electronic equipment (WEEE). By using the appropriate disposal systems you prevent the potential negative consequences of wrong product take-back that can pose risks to the environment and human health. The symbol indicates that this product must not be disposed of with your other waste. You must hand it over to a designated collection point for the recycling of electrical and electronic equipment waste. The disposal of the product should obey all the specific Community waste management legislations. Contact your local city office, your waste disposal service or the place of purchase for more information on the collection. Weight of the device: 222 g

MODECOM