NSW-R2 Wireless Router

DISCLAIMER

- We spared no efforts to make sure that the information in this manual is correct and complete. However no liability is accepted for any errors or omissions. Gembird Electronics reserves the right to change the specifications of the hardware and software described in this manual without prior notice.
- No part of this manual may be reproduced, transmitted or translated in any language in any form, by any means, without the prior written permission of Gembird Electronics Ltd.
- Gembird Electronics makes no warranties for damages resulting from corrupted or lost data due to a mistaken operation or malfunction of the product, the software, personal computers or peripheral devices.

Gembird® is a registered trademark of GMB Tech (Holland) bv.
Other names or products not mentioned above may be registered trademarks or trademarks of their respective owners.

Table of Contents

CHAPTER 1 INTRODUCTION

Congratulations on your purchase of this outstanding Wireless Router. The Wireless Router integrates 4-port switch, firewall, NAT-router and Wireless AP. This product is specifically designed for Middling and Small Corporation needs. It will allow you to connect your network wirelessly better tan ever, sharing Internet Access, files and fun, easily and securely. it is easy to configure and operate for even non-technical users. Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read this manual carefully for full exploiting the functions of this product.

The Wireless Router complies with the IEEE802.11g/b standards so that the data transmission rate is up to 54Mbps.In the most attentive wireless security, The Wireless Router provides multiple protection measures. It can be set to turn off wireless network name (SSID) broadcast so that only stations that have the SSID can be connected. The router provides wireless LAN 64/128-bit WEP encryption security, and WPA/WPA2 authentication, as well as TKIP/AES encryption security.

1.1 Features

Designed for versatility and performance, the WR3104 router provides the following:

- Complies with IEEE802.11g, IEEE802.11b,IEEE802.3,IEEE802.3u standards
- All-in-one Internet-sharing Router, 4-port Switch, and Wireless-G (802.11g) Access Point
- Shares a single Internet connection and other resources with Ethernet wired and Wireless-G clients
- Support DHCP/Static IP/PPPoE Client
- Support PPPoE Auto-connect and Auto-disconnect
- Built-in DHCP server to automatically assign and manage LAN IP addresses
- Wireless data rates up to 54Mbps -- 5 times as fast as Wireless-B (802.11b), but also interoperable with Wireless-B devices (at 11Mbps)
- Support 64/128-bit WEP encryption security
- Support wireless LAN ACL (Access Control List) filtering
- Support WPA/WPA2 and WPA-PSK/WPA2-PSK authentication and TKIP/ AES encryption security.
- Operates in the 2.4GHz frequency range.
- Transmission Distance: indoor up to 120m, Outdoor up to 360m, it is li-mited in an environment.
- Built-in powerful firewall engine, Prevent hacker from attaching and controlling your computer
- Support IP Filter, URL Filter, Port Filter, and MAC Address Filter
- Support Time Schedule
- Support MAC Address and IP Address Binding
- Support MAC Address CLONE

- Support Static Route
- Support WDS
- Support Dynamic DNS

- Support UPnP
- Support Virtual Server
- Support Special Application
- Support DMZ host
- Support VPN Passthrough for IPSec, PPTP and L2TP Protocols
- Support TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP, ARP Protocols
- Support Web-based interface for Remote and Web Management
- Support firmware upgrade
- Support Security Logs

1.2 Environments

- Dimensions: 202 (L)X120 (W)X31 (H)mm
- Unit Weight: 324g
- Power Input: 5V DC, 2A
- Consumption: 13.5W(Max)
- Storage Temperature: -40ºC ~70ºC
- Operating Temperature : -10ºC ~50ºC
- Storage Humidity: 5% ~95% RH Non-condensing
- Operating Humidity: 10% ~90% RH Non-condensing

1.3 Package

- One Broadband Router
- One Power Adapter
- One Installation CD-ROM and Quick Installation Guide

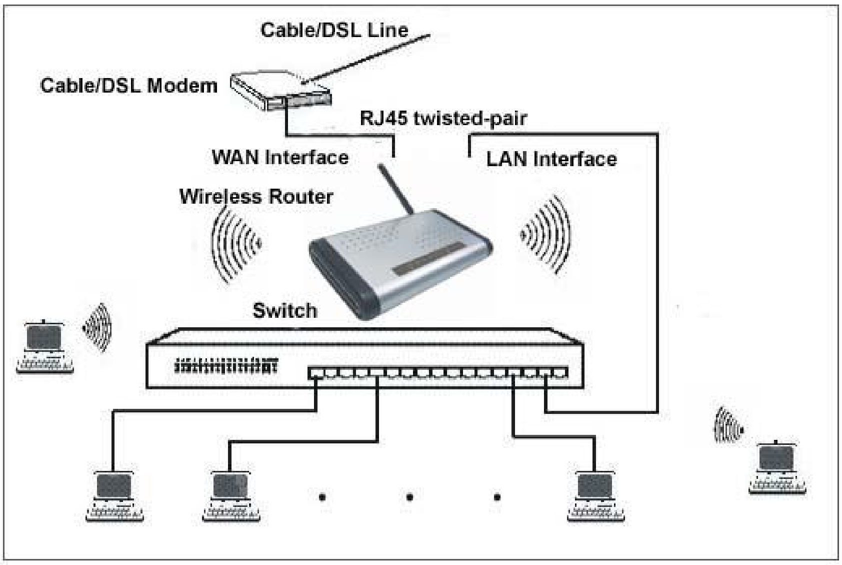
1.4 System Requirement

- One DSL/Cable Modem
- One 10M or 100M, 10/100M Ethernet Card on PC
- TCP/IP network protocol for each PC
- RJ45 Twisted-pair
- Microsoft IE4.0 (or Netscape Navigator 4.0) or later

CHAPTER 2 HARDWARE INSTALLATION

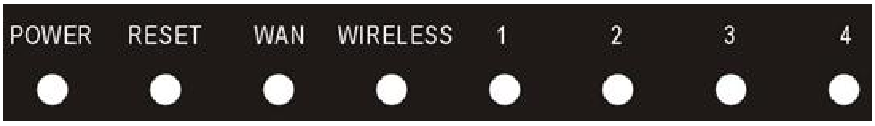
2.1 Typical Installation

Multifunction Broadband Router connection：



1. Make sure all devices, including your PCs, modem, and Router, are powered down.
2. Locate an optimum location for the router. The best place is usually near the center of the area in which your PC(s) will wirelessly connect.
3. Adjust the direction of the antenna.
4. Using an Ethernet network cable, connect the LAN or Ethernet network port of the cable or DSL modem to the Router's WAN port.
5. Connect the PC(s) and each Swtich/Hub on your LAN to the LAN ports on the router.
6. Power on the cable or DSL modem, and power on the PC you wish to use to configure the Router.
7. Connect the included power adapter to the Router. And connect the other end of the adapter to an electrical outlet.

2.2 LED indicators



- **POWER(green)**

The LED illuminates when the router is powered on.

- **RESET (green)**

The LED is continuously illuminated when the router is resetting.

- **WAN (green)**

The Link/Act LED serves two purposes. If the LED is continuously illuminated, the Router is successfully connected to a device through the corresponding port. If the LED is flickering, the Router is actively sending or receiving data over that port.

- **WIRELESS (green)**

The LED is flickering during wireless activity.

- **LAN 1,2,3,4(green)**

The Link/Act LED serves two purposes. If the LED is continuously illuminated, the Router is successfully connected to a device through the corresponding port. If the LED is flickering, the Router is actively sending or receiving data over that port.

2.3 Back Panel Features

- **LAN(1,2,3,4)**

10/100Mbps RJ45 Auto-sensing .
These four LAN ports are where you will connect networked devices, such as PCs, print servers, remote hard drives, and anything else you want to put on your network. if you connect this product with the Hub(or Switchboard) correctly, the Router's corresponding LED and the Hub's(or the Switchboard's) must be illuminates.

- **WAN**

10/100Mbps RJ45 port.
The WAN port is where you will connect Cable/DSL Modem or other LAN.

- **RESET**

The Reset Button for clear the Router's data and restore the factory default config.

- **5V DC, 2A**

Power inlet.

- **ANTENNA**

One wireless antenna.

CHAPTER 3 NETWORK SETTING AND SOFTWARE INSTALLATION

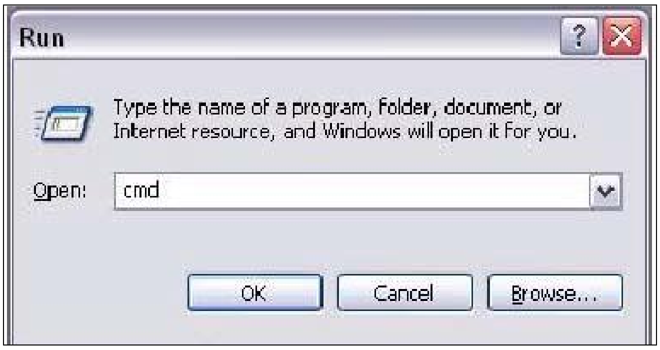
3.1 TCP/IP Configuration

1. Click ***Start*** button and choose ***Settings,*** then click ***Control Panel***.
2. Double click ***Network*** icon and select ***Configuration*** tab in the Network window.
3. Click ***Add*** button to add network component into your PC.
4. Double click ***Protocol*** to add TCP/IP protocol.
5. Select ***Microsoft*** item in the manufactures list. Add choose ***TCP/IP*** in the Network Protocols. Click ***OK*** button to return to Network window.
6. The ***TCP/IP*** protocol shall be listed in the Network window. Double click ***TCP/IP*** to set the TCP/IP protocol.
7. Select ***Obtain an IP address automatically*** in the ***IP Address*** tab.
8. Click ***OK*** to complete the install procedure and restart your PC to enable the TCP/IP protocol.

3.2 IP Setting

The following instruction set up the computer running windows 2000/ XP.

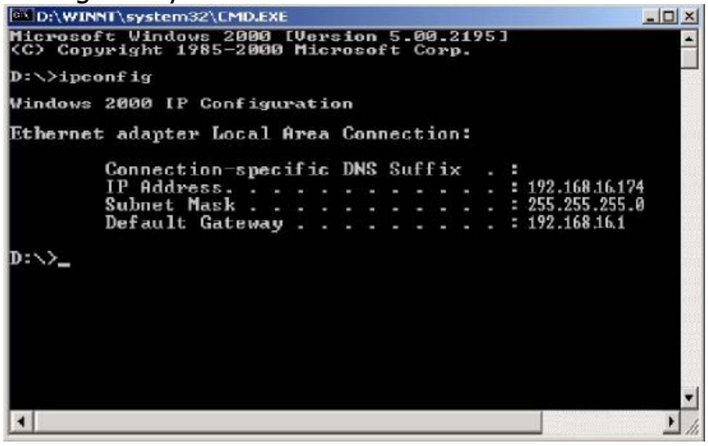
1. Click on ***Start*** and select ***Run***.
2. Type ***cmd*** then click ***OK*** button.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

3. From the Command Prompt, enter ***ipconfig***. It will return your IP Address, subnet mask, and default gateway.



D:\WINNT\system32\CMD.EXE

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

D:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.16.174
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.16.1

D:\>_
```

4. Type ***exit*** to close the command prompt.

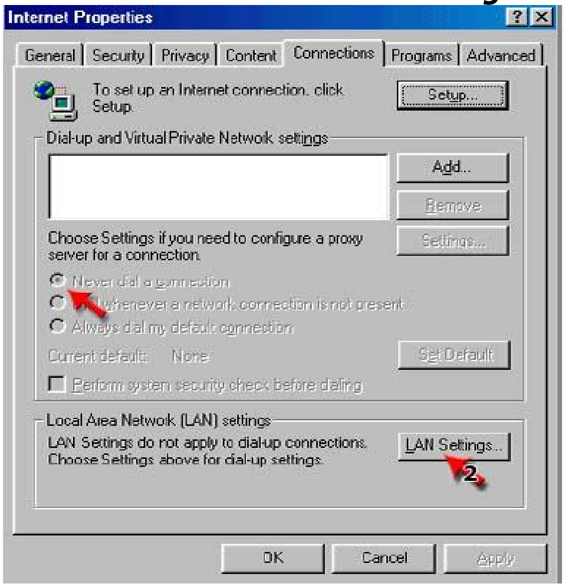
Make sure you take note of your computer's Default Gateway IP Address. The Default Gateway is the IP Address of the Router. By default, it should be 192.168.16.1

3.3 Wizard Setup

You may run Wizard Setup to quickly set up your router.

This product provides Web based configuration scheme, that is, configuring by Netscape Communicator or Internet Explorer. Take example for Microsoft Internet Explorer.

1. Activate your browser, select ***Tools*** , point to ***Internet option*** ,click ***connections*** tab, select ***never dial a connection***. Click ***LAN Settings*** button.



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection

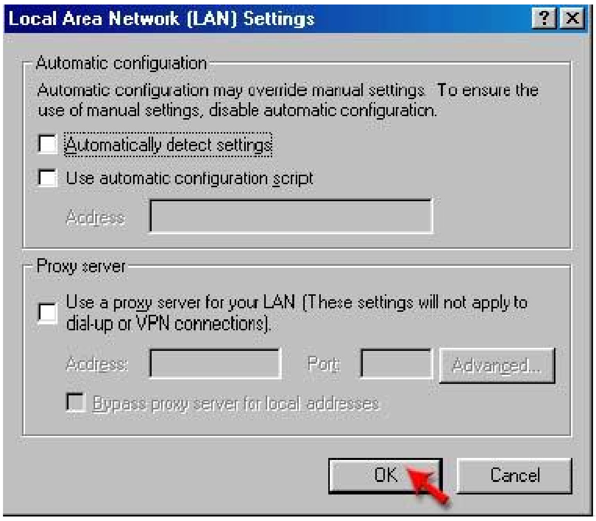
Current default: None

☐ Perform system security check before dialing

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

2. Nothing should be checked. Click ***OK*** button.



Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☐ Use automatic configuration script

Address

Proxy server

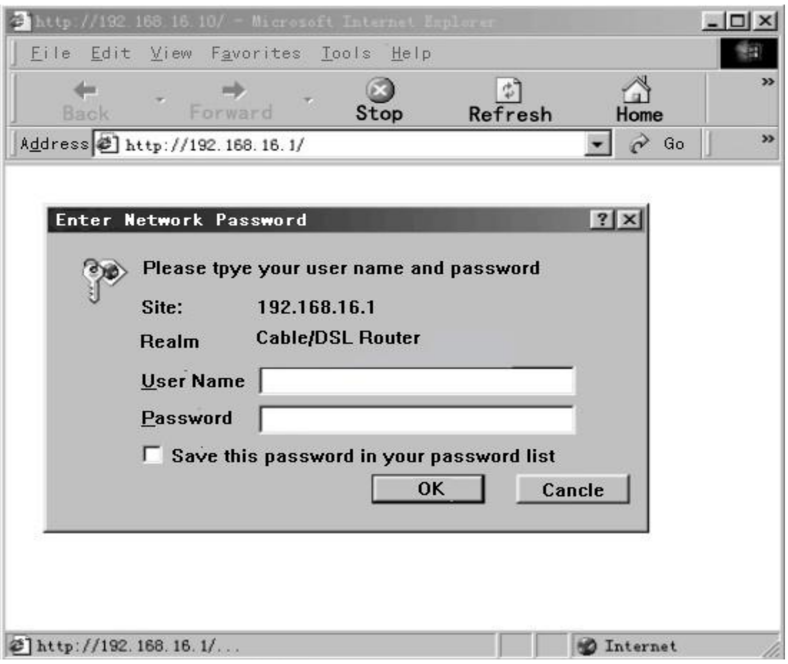
☐ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port:

☐ Bypass proxy server for local addresses

3. Click the ***OK*** button on the ***Connections*** tab, close the dialog box.

4. Type ***http://192.168.16.1*** in your web browser and press ***Enter***, Key in the user name and password (if you use it first, you can type the factory default setting .User name is ***admin*** and password is ***admin***), click on the ***OK*** button.


http://192.168.16.10/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Address http://192.168.16.1/
Go
http://192.168.16.1/...
Internet

Enter Network Password

Please tpye your user name and password

Site: 192.168.16.1

Realm Cable/DSL Router

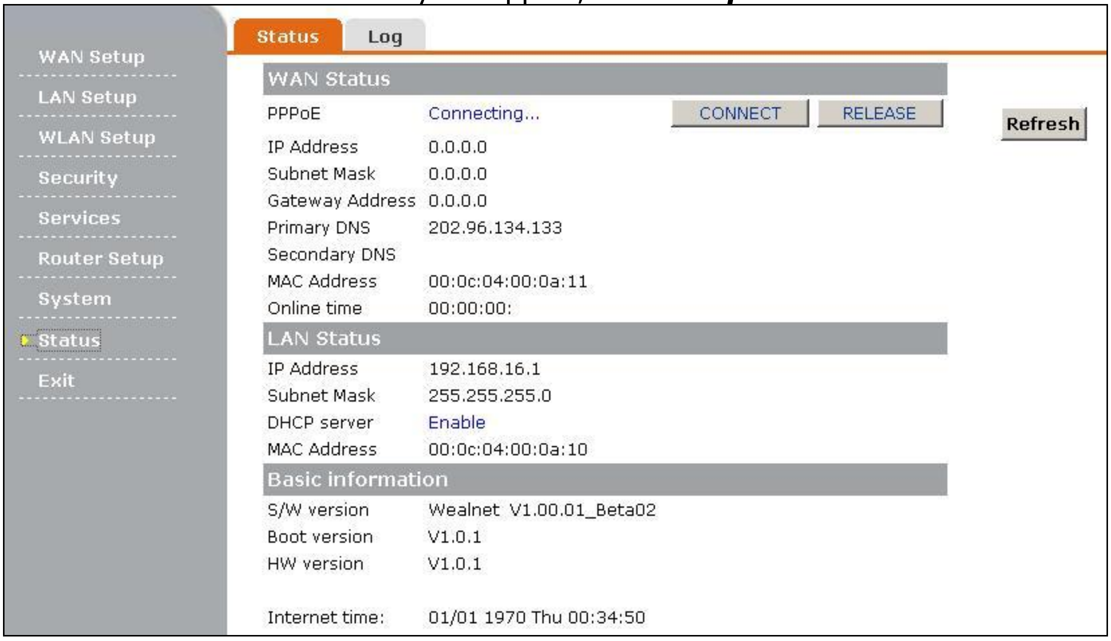
User Name

Password

□ Save this password in your password list

OK Cancle

5. The Router's Web-based Utility will appear, Click ***Setup***.



WAN Status

PPPoE	Connecting...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway Address	0.0.0.0
Primary DNS	202.96.134.133
Secondary DNS	
MAC Address	00:0c:04:00:0a:11
Online time	00:00:00:

LAN Status

IP Address	192.168.16.1
Subnet Mask	255.255.255.0
DHCP server	Enable
MAC Address	00:0c:04:00:0a:10

Basic information

S/W version	Wealnet V1.00.01_Beta02
Boot version	V1.0.1
HW version	V1.0.1
Internet time:	01/01 1970 Thu 00:34:50

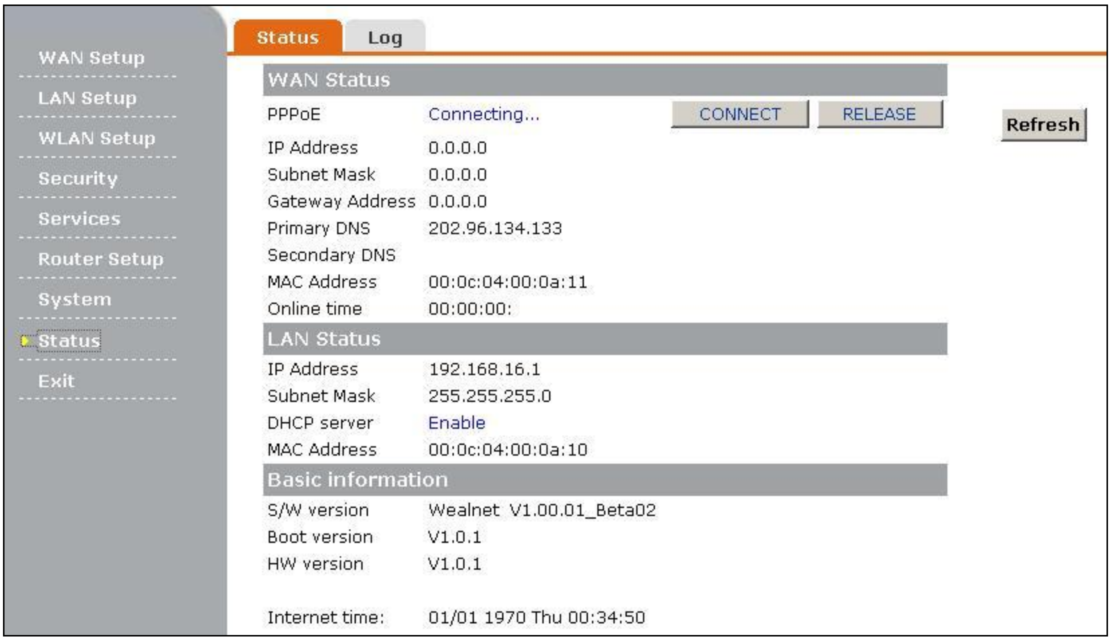
6. Click ***WAN Setup*** to setting the parameters (Please referent below **3.5**)

3.4 Status

This option provides the current status of the device.

3.4.1 Status

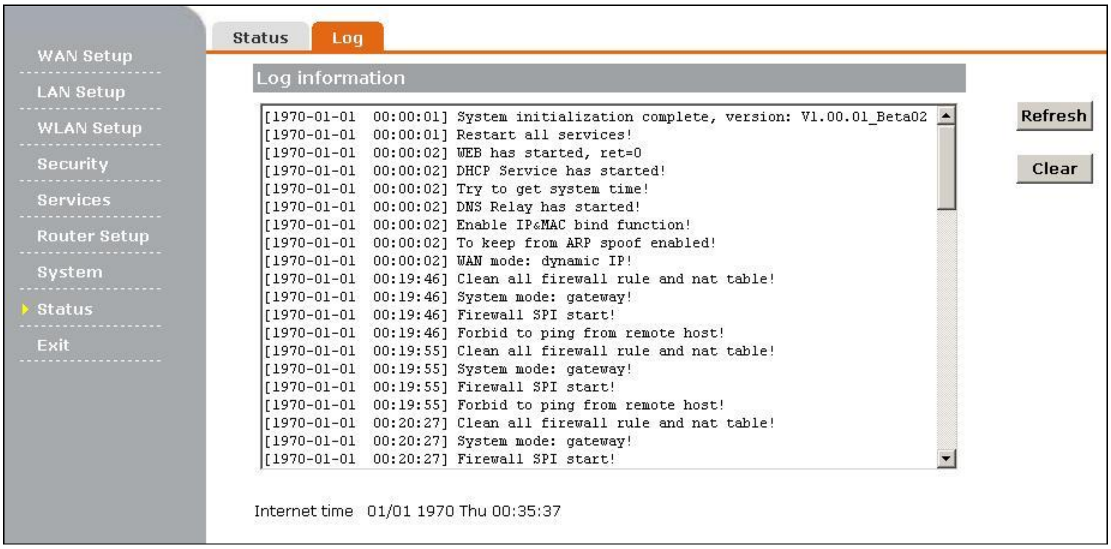
You can use the Status screen to see the connection status for the router's WAN/LAN interfaces, firmware version numbers.



WAN Status	
PPPoE	Connecting...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway Address	0.0.0.0
Primary DNS	202.96.134.133
Secondary DNS	
MAC Address	00:0c:04:00:0a:11
Online time	00:00:00:
LAN Status	
IP Address	192.168.16.1
Subnet Mask	255.255.255.0
DHCP server	Enable
MAC Address	00:0c:04:00:0a:10
Basic information	
S/W version	Wealnet V1.00.01_Beta02
Boot version	V1.0.1
HW version	V1.0.1
Internet time:	01/01 1970 Thu 00:34:50

3.4.2 System Log

System log displays any illegal attempts to access your network



Log information

```
[1970-01-01  00:00:01] System initialization complete, version: V1.00.01_Beta02
[1970-01-01  00:00:01] Restart all services!
[1970-01-01  00:00:02] WEB has started, ret=0
[1970-01-01  00:00:02] DHCP Service has started!
[1970-01-01  00:00:02] Try to get system time!
[1970-01-01  00:00:02] DNS Relay has started!
[1970-01-01  00:00:02] Enable IP&MAC bind function!
[1970-01-01  00:00:02] To keep from ARP spoof enabled!
[1970-01-01  00:00:02] WAN mode: dynamic IP!
[1970-01-01  00:19:46] Clean all firewall rule and nat table!
[1970-01-01  00:19:46] System mode: gateway!
[1970-01-01  00:19:46] Firewall SPI start!
[1970-01-01  00:19:46] Forbid to ping from remote host!
[1970-01-01  00:19:55] Clean all firewall rule and nat table!
[1970-01-01  00:19:55] System mode: gateway!
[1970-01-01  00:19:55] Firewall SPI start!
[1970-01-01  00:19:55] Forbid to ping from remote host!
[1970-01-01  00:20:27] Clean all firewall rule and nat table!
[1970-01-01  00:20:27] System mode: gateway!
[1970-01-01  00:20:27] Firewall SPI start!
```

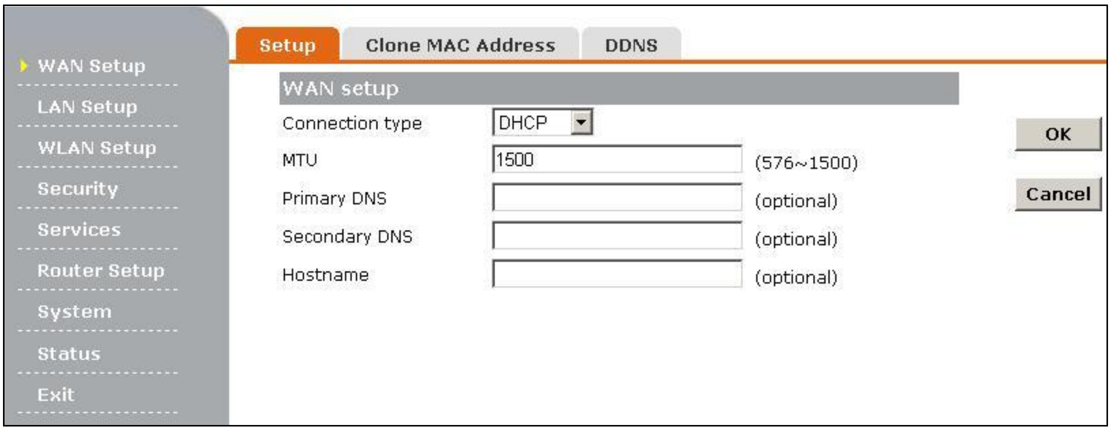
Internet time 01/01 1970 Thu 00:35:37

3.5 WAN Setup

The Router provides three connection Mode: Static IP Address, Dynamical IP address, and PPPoE. Specify the WAN connection Mode required by your Internet Service Provider, then click ***OK*** Button to provide detailed configuration parameters for the selected connection Mode. Proceed to the instructions for the connection type you are using.

3.5.1 Dynamic

Most Broadband ISPs assign their clients with a different IP address each time they log on. If this is the case with your ISPs, Select ***DHCP.***



WAN setup

Connection type	DHCP	
MTU	1500	(576~1500)
Primary DNS		(optional)
Secondary DNS		(optional)
Hostname		(optional)

MTU: Maximum Transmission Unit-you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU

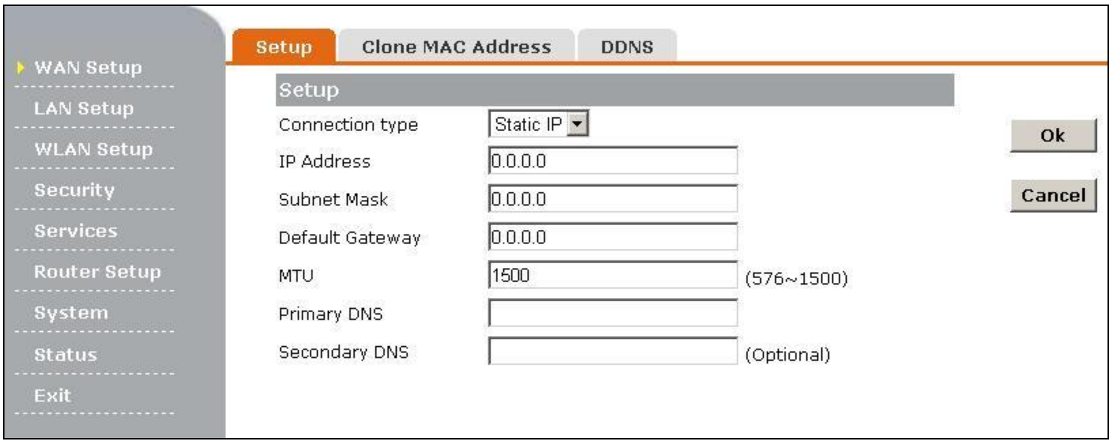
Primary DNS : Enter Primary DNS IP address assigned by your ISP, this is optional.

Secondary DNS: Enter the Secondary DNS IP address assigned by your ISP, this is optional.

HostName: The Host Name is optional but may be required by some ISPs.

3.5.2 Static

If your ISP assigns you a fixed IP address, select ***Static IP***.



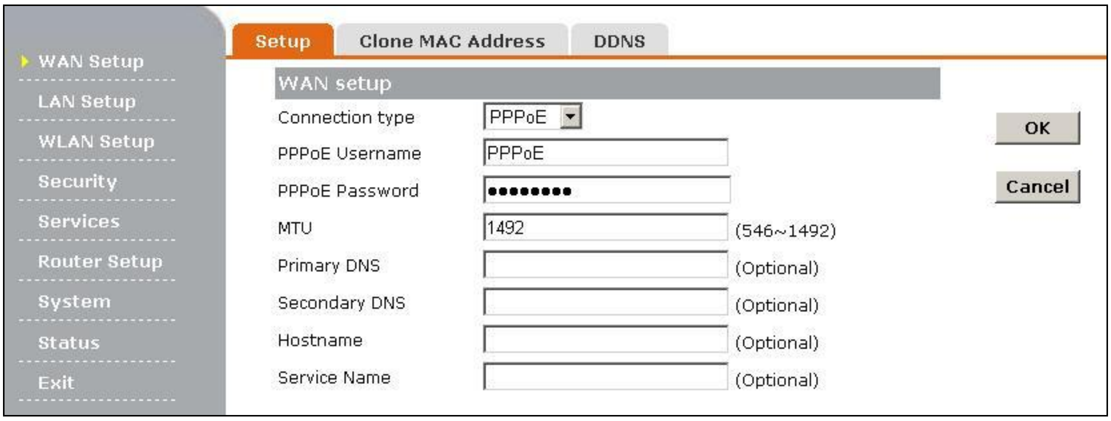
Setup

Connection type	Static IP	
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Default Gateway	0.0.0.0	
MTU	1500	(576~1500)
Primary DNS		
Secondary DNS		(Optional)

IP Address: Enter the IP address assigned by your ISP.
Subnet Mask: Enter the Subnet Mask assigned by your ISP.
Default Gateway: Enter the Gateway assigned by your ISP.
MTU: Maximum Transmission Unit-you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU
Primary DNS : Enter the Primary Server IP address assigned by your ISP.
Secondary DNS: Enter the Secondary DNS IP address assigned by your ISP, this is optional.

3.5.3 PPPoE

If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, select ***PPPoE***



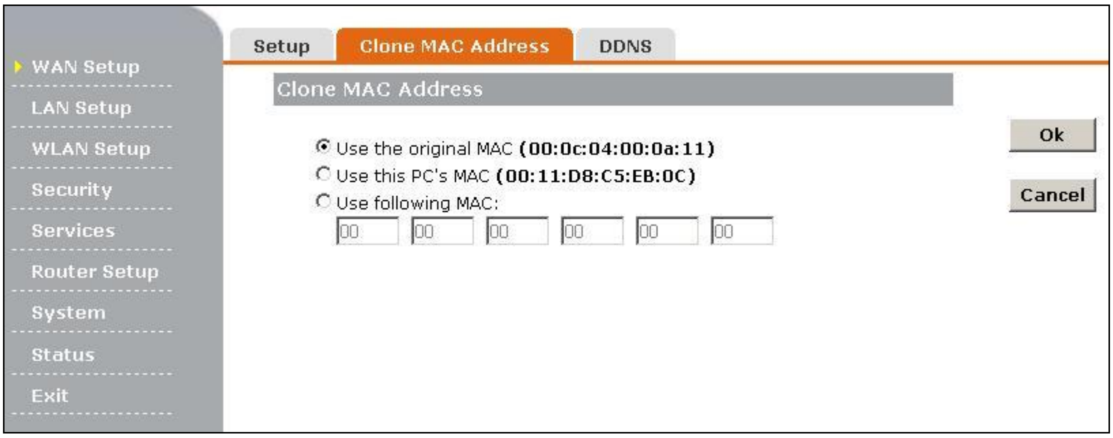
WAN setup

Connection type: PPPoE
PPPoE Username: PPPoE
PPPoE Password: •••••••••
MTU: 1492 (546~1492)
Primary DNS: (Optional)
Secondary DNS: (Optional)
Hostname: (Optional)
Service Name: (Optional)

PPPoE Username: Enter your PPPoE user name.
PPPoE Password: Enter your PPPoE password.
MTU: Maximum Transmission Unit-you may need to change the MTU for optimal performance with your specific ISP. 1492 is the default MTU
Primary DNS : Enter Primary DNS IP address assigned by your ISP, this is optional.
Secondary DNS: Enter the Secondary DNS IP address assigned by your ISP, this is optional.
HostName: The Host Name is optional but may be required by some ISPs. **Service Name:** The Service Name is optional but may be required by some ISPs.

3.5.6 Clone MAC Address

The default MAC address is set to the WAN’s physical interface MAC address on the Router. It is not recommended that you change the default MAC address unless required by your ISP.



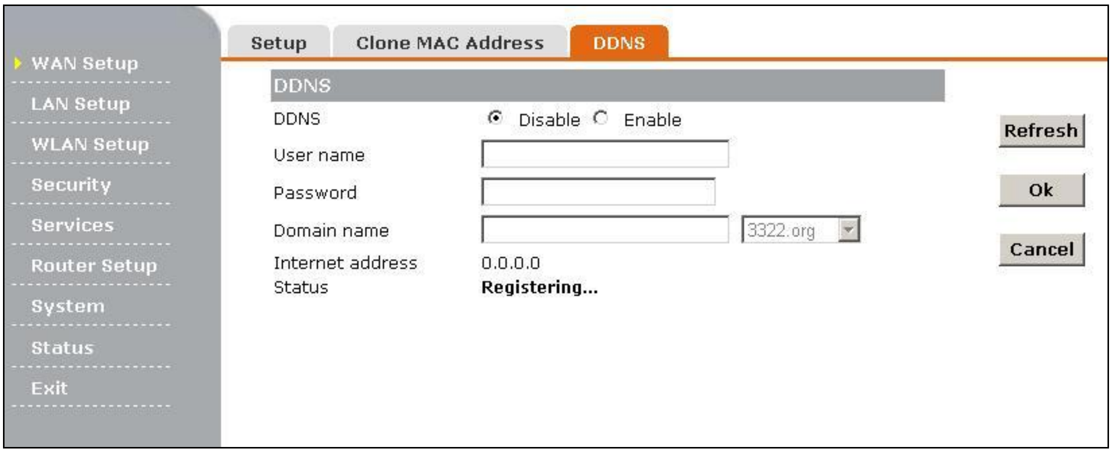
Clone MAC Address

● Use the original MAC **(00:0c:04:00:0a:11)**
○ Use this PC's MAC **(00:11:D8:C5:EB:0C)**
○ Use following MAC:
00 00 00 00 00 00

3.5.8 DDNS

The Router offers a DDNS feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router.

Before you can use this feature, you need to sign up for DDNS service at DDNS service provider,3322.org. IF you do not want to use this feature, keep the default setting, ***Disable***.



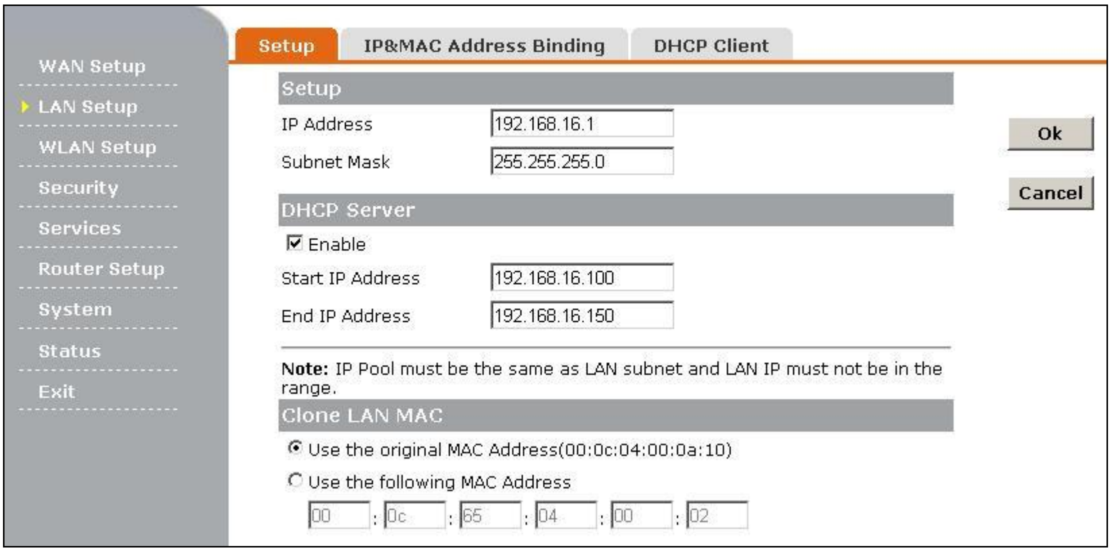
DDNS

DDNS	● Disable ○ Enable
User name	
Password	
Domain name	3322.org
Internet address	0.0.0.0
Status	**Registering...**

1. Click DDNS ***Enabled*** radio button.
2. Enter ***Name***, ***Password***, and ***Domain name***.
3. Click ***OK*** button to save it.

3.6 LAN Setup

3.6.1 LAN Setting



Setup

IP Address 192.168.16.1

Subnet Mask 255.255.255.0

DHCP Server

☑ Enable

Start IP Address 192.168.16.100

End IP Address 192.168.16.150

Note: IP Pool must be the same as LAN subnet and LAN IP must not be in the range.

Clone LAN MAC

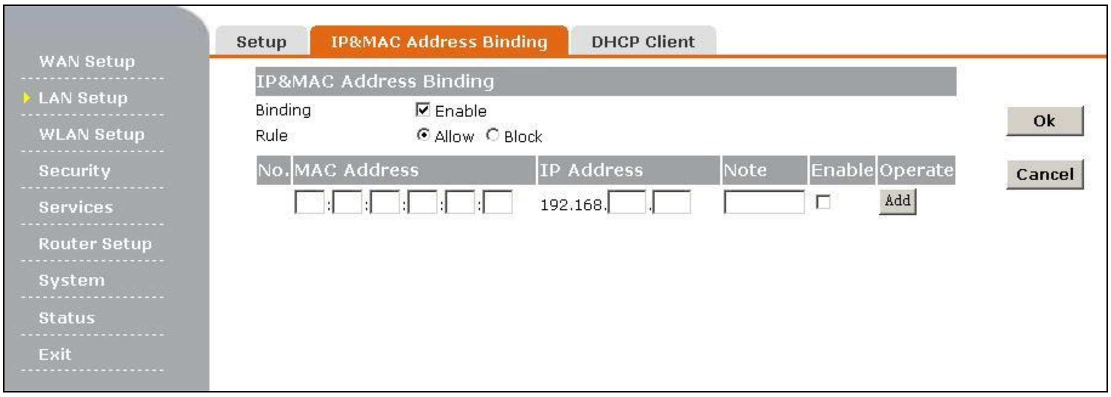
● Use the original MAC Address(00:0c:04:00:0a:10)

○ Use the following MAC Address

00 : 0c : 65 : 04 : 00 : 02

IP Address and Subnet Mask: The value refer to your internal network settings. Unless you have specific internal needs, these should be no reason to change the value.
DHCP Server: The settings of TCP/IP environment include Host IP, Subnet Mask, Gateway, and DNS configurations. It is not a simple task to correctly configure all the computers in your LAN environment. Fortunately, DHCP provides a rather simple approach to handle all these settings. This product supports the function of DHCP server. If you enable this product's DHCP server and configure you computers as ***automatic IP allocation*** mode, when your computer is powered on, it will automatically load the proper TCP/IP settings from this product.
Starting IP Address: Enter a value for the DHCP server to start with when issuing IP addresses. This value must be 192.168.16.2 or greater, because the default IP address for the Router is 192.168.16.1.
End IP Address: Enter a value for the DHCP server to end with when issuing IP addresses. This value must be greater the IP pool Starting Address.
Clone LAN MAC: The default MAC address is set to the LAN's physical interface MAC address on the Router. If you need to change the LAN's MAC address, you can use this option.

The Router provides IP&MAC Address Binding. The computer that has the same MAC in the list will obtain a specific IP address.



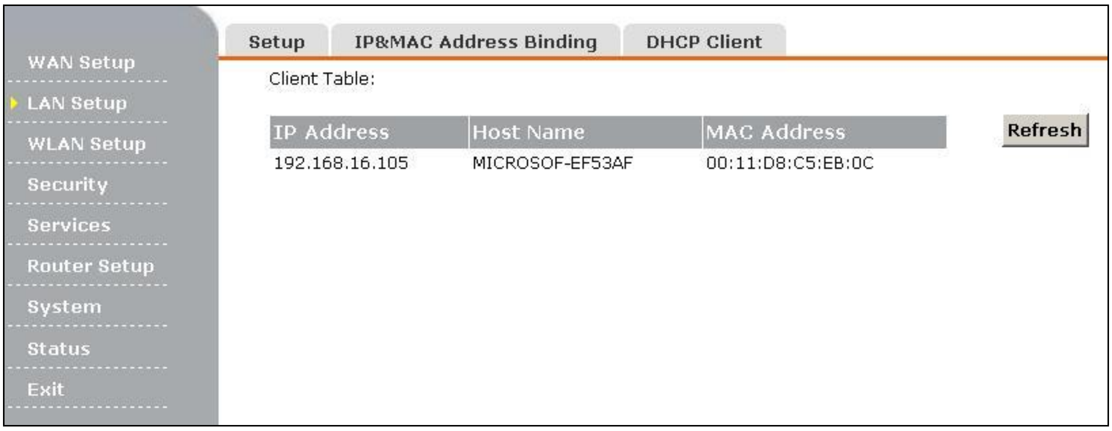
IP&MAC Address Binding

Binding ☑ Enable

Rule ● Allow ○ Block

No.	MAC Address	IP Address	Note	Enable	Operate
	: : : : :	192.168. .		□	Add

The Table lists the information about the hosts which have obtain an IP address from this route’s DHCP server.



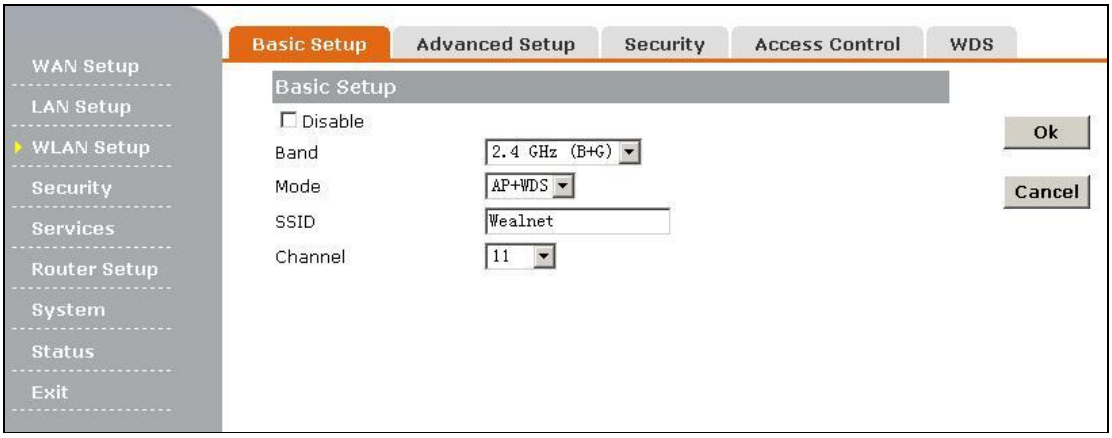
Client Table:

IP Address	Host Name	MAC Address
192.168.16.105	MICROSOF-EF53AF	00:11:D8:C5:EB:0C

3.7 WLAN Setup

Wireless Access Point builds a wireless LAN and can let all PCs equipped with IEEE802.11g and 802.11b wireless network adaptor connect to your Intranet.

The basic settings for the wireless network are set on this page. You can set parameters that are used for the wireless stations to connect to this router.



Basic Setup

□ Disable

Band 2.4 GHz (B+G)

Mode AP+WDS

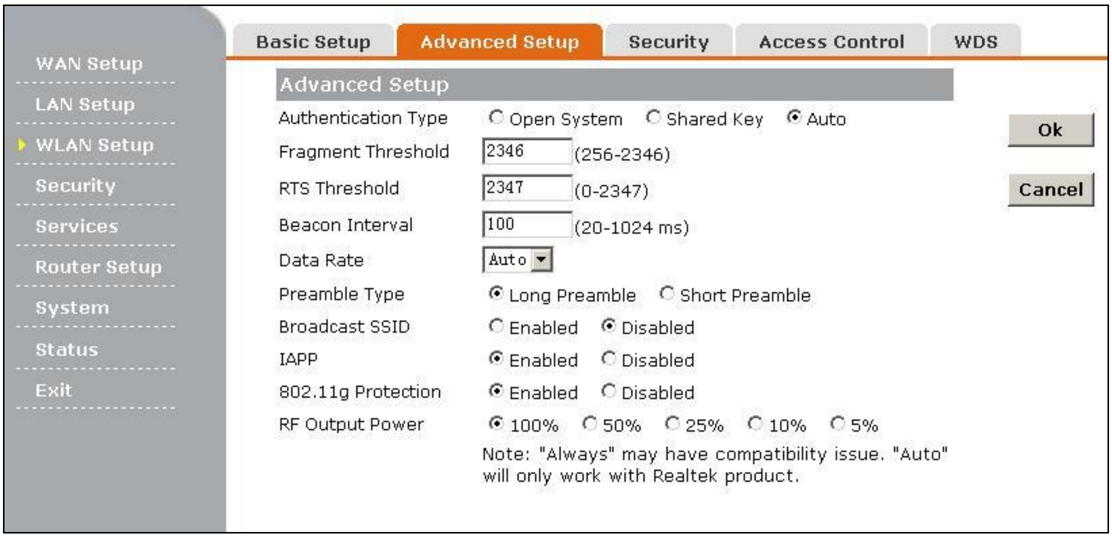
SSID Wealnet

Channel 11

Band: The options are 2.4GHz(B+G), 2.4GHz(B), and 2.4GHz(G). Select the desired wireless Band.
2.4 GHz(B+G)- Both 802.11g and 802.11b wireless stations can connect to the router.
2.4 GHz(B)- Only 802.11b wireless stations can connect to the router.
2.4 GHz(G)- Only 802.11g wireless stations can connect to the router.

Mode: The options are AP, WDS, and AP+WDS, Select the desired wireless Mode.
SSID: An SSID is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must employ the same SSID in order to communicate with each other. SSIDs are case sensitive text strings. The SSID is a sequence of alphanumeric characters (letters or numbers). SSIDs have a maximum length of 32 characters. The default SSID is **wealnet**, but it is recommended strongly that you change your network name (SSID) to a different value.
Channel: This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. All devices in the same wireless LAN should use the same channel.

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.



Advanced Setup

Authentication Type ○ Open System ○ Shared Key ● Auto

Fragment Threshold 2346 (256-2346)

RTS Threshold 2347 (0-2347)

Beacon Interval 100 (20-1024 ms)

Data Rate Auto

Preamble Type ● Long Preamble ○ Short Preamble

Broadcast SSID ○ Enabled ● Disabled

IAPP ● Enabled ○ Disabled

802.11g Protection ● Enabled ○ Disabled

RF Output Power ● 100% ○ 50% ○ 25% ○ 10% ○ 5%

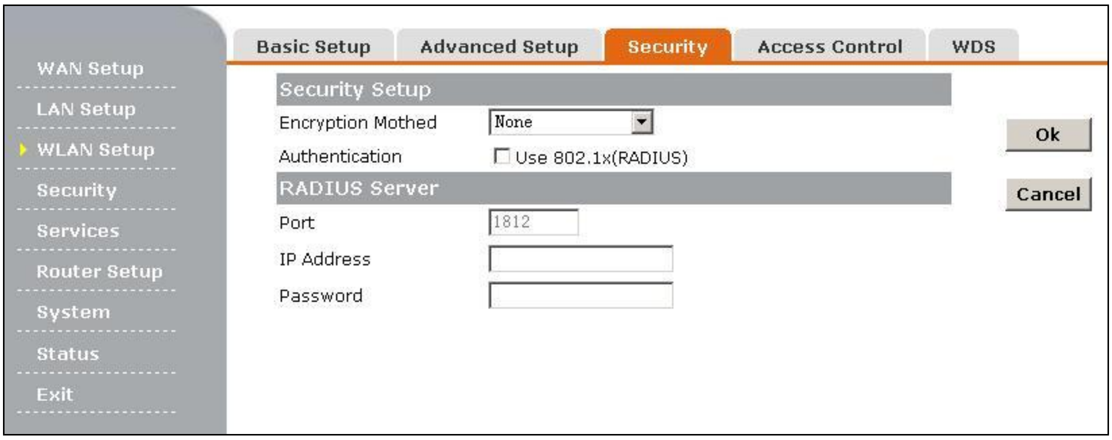
Note: "Always" may have compatibility issue. "Auto" will only work with Realtek product.

Authentication Type: You can select one of the following authentication types:
Open Sytem: Select 802.11 Open System authentication
Shared Key: Select 802.11 Shared Key authentication
Auto: Select Shared key or Open System authentication type automatically based on the wireless station request.

Fragment Threshold: The fragmentation threshold is a way of limiting the size of packets (frames) transmitted over the network. If a packet exceeds the fragmentation threshold set here, the fragmentation function will be activated and the packet will be sent as multiple 802.11 frames. The default is 2346.
RTS Threshold: The RTS threshold specifies the packet size of a request to send (RTS) transmission. This helps control traffic flow through the access point, especially one with a lot of clients. The default is 2347.
Beacon Interval: Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second).
Date Rate: indicate rates that the access point will advertise to the network for the purposes of setting up communication with other APs and client stations on the network. It is generally more efficient to have an AP broadcast a subset of its supported rate sets.
Preamble Type: It defines the length of CRC block in the frames during the wireless Communication. "Short Preamble" is suitable for heavy traffic wireless network. "Long Preamble" provides much communication reliability.
SSID Broadcast: The router automatically transmit their network name (SSID) into open air at regular intervals (every few seconds). This feature of the Routernet is intended to allow clients to dynamically discover and roam between WLANs. However, this feature also makes it easier for hackers to break into your home network. Because SSIDs are not encrypted or otherwise scrambled, it becomes easy to grab one by snooping the WLAN looking for SSID broadcast messages coming from the router or AP. Knowing your SSID brings hackers one step closer to a successful intrusion. So you should disable this feature to improve the security of your WLAN. Once your wireless clients are manually configured with the right SSID, they no longer require these broadcast messages.

IAPP: Inter-Access Point Protocol (IAPP) is being standardized by IEEE 802.11F as well as the IETF SEAMOBY WG. IAPP enables seamless, authenticated fast handoff between 802.11 Access Points.
RF Output Power: There are five options: 100%,50%,25%,10%,5%

The wireless station will be able to connect the router without encryption. It is recommended strongly that you choose this optional to encrypt your wireless network. The Security Mode are None, Wep, and WPA/WPA2/Mixed. You have to setup the same security parameters both on your router and wireless client devices.



Security Setup

Encryption Mothed: None

Authentication: ☐ Use 802.1x(RADIUS)

RADIUS Server

Port: 1812

IP Address:

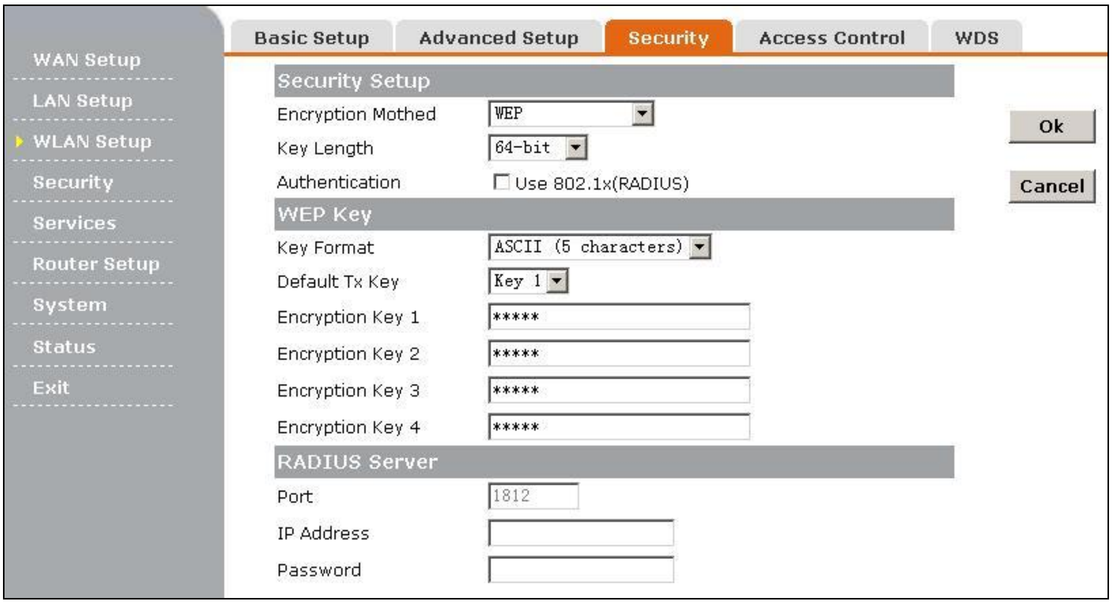
Password:

Encryption Method: you can select **None,WEP, WPA/WPA2/Mixed**.
Authentication: Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. Click the checkbox to Use 802.1x.

Port: Enter the port that Radius Server used, the default value is 1812 .
IP Address: Enter the IP Address of Radius Server.
Password: Set encryption keys. Commonly used in Wi-Fi Protected Access and WEP.

3.7.3.1 WEP

WEP is a protocol that adds security to wireless local area networks (WLANs) based on the 802.11b standard. WEP was designed to give wireless networks the equivalent level of privacy protection as a comparable wired network.



Security Setup

Encryption Mothed: WEP

Key Length: 64-bit

Authentication: □ Use 802.1x(RADIUS)

WEP Key

Key Format: ASCII (5 characters)

Default Tx Key: Key 1

Encryption Key 1: *****

Encryption Key 2: *****

Encryption Key 3: *****

Encryption Key 4: *****

RADIUS Server

Port: 1812

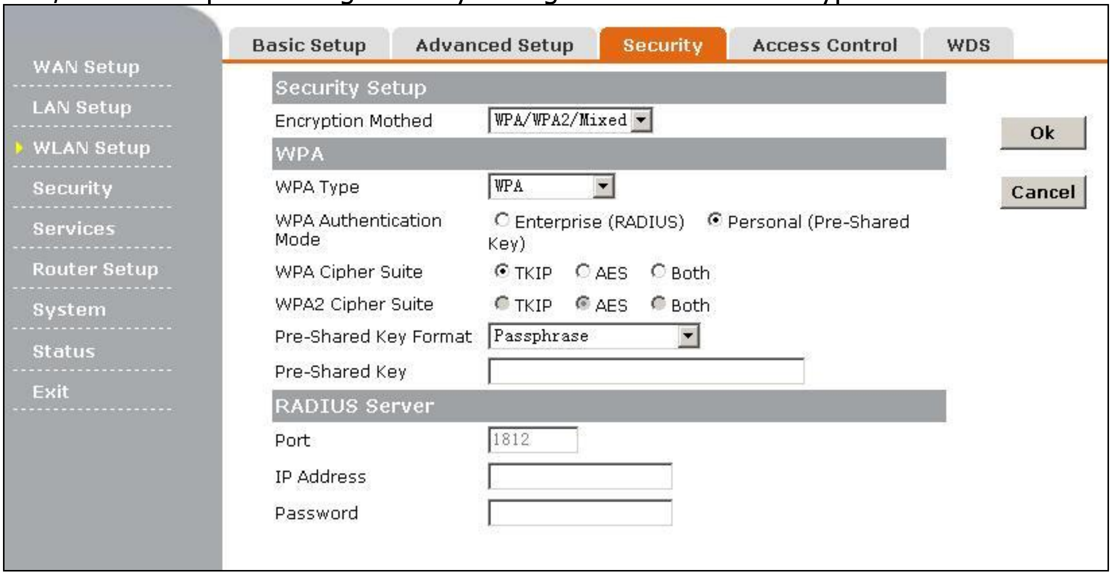
IP Address:

Password:

Key Length: Select ***64 bits 10 hex digits*** or ***128 bits 26 hex digits*** to encrypt data.
Key Format: You may select to select ASCII Characters or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key.
Default Tx Key: Select one of the four keys to encrypt your data. Only the key you select it in the ***Default Tx Key*** will take effect.
KEY1~KEY4: The WEP keys are used to encrypt data transmitted in the wireless network. For 64 bits 10 hex digits, you can enter 10 hexadecimal digits(any combination of 0-9, a-f, A-F). For 128 bits 26 hex digits, you can enter 26 hexadecimal digits(any combination of 0-9, a-f, A-F).

3.7.3.2 WPA/WPA2/Mixed

WPA/WPA2-PSK provides significantly stronger wireless data encryption than WEP.



Security Setup

Encryption Mothed: WPA/WPA2/Mixed

WPA

WPA Type: WPA

WPA Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

WPA Cipher Suite: ● TKIP ○ AES ○ Both

WPA2 Cipher Suite: ○ TKIP ● AES ○ Both

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

RADIUS Server

Port: 1812

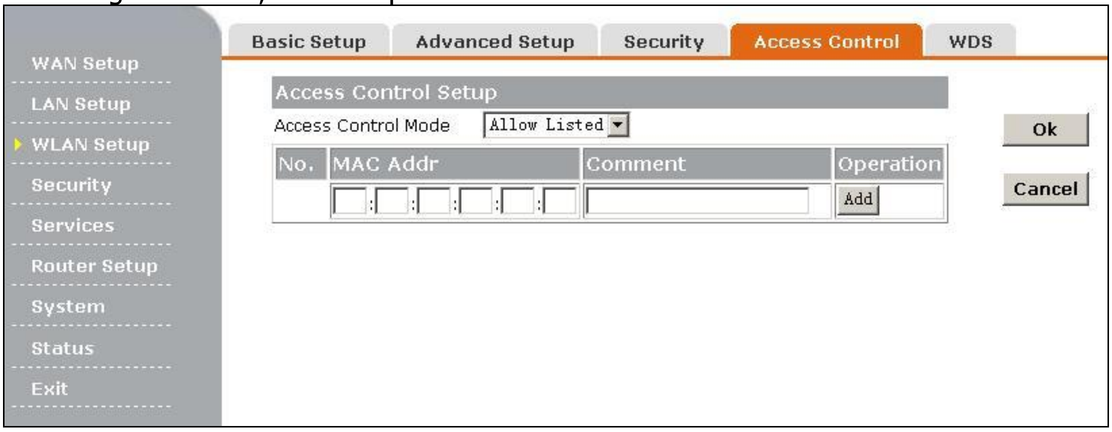
IP Address:

Password:

WPA Type: Enter the P Address of Radius Server.

WPA Authentication Mode: Keys can be managed using two different mechanisms. WPA can either use an external authentication server (e.g., RADIUS) and EAP just like IEEE 802.1X is using or pre-shared keys without need for additional servers. Wi-Fi calls these "WPA-Enterprise" and "WPA-Personal", respectively. Both mechanisms will generate a master session key for the Authenticator (AP) and Supplicant (client station).
WPA Cipher Suite: You can select either TKIP, AES or Both as Encryption.
WPA2 Cipher Suite: You can select either TKIP, AES or Both as Encryption.
Pre-Shared Key Format: You can select PASSPHRASE or HEX(64 CHARACTERS).
Pre-Shared Key: Pre-shared key(PSK) is a method to set encryption keys. Commonly used in Wi-Fi Protected Access and WEP.

The Wireless MAC Address Filtering feature allows you to control wireless stations accessing the router, which depend on the station's MAC addresses.



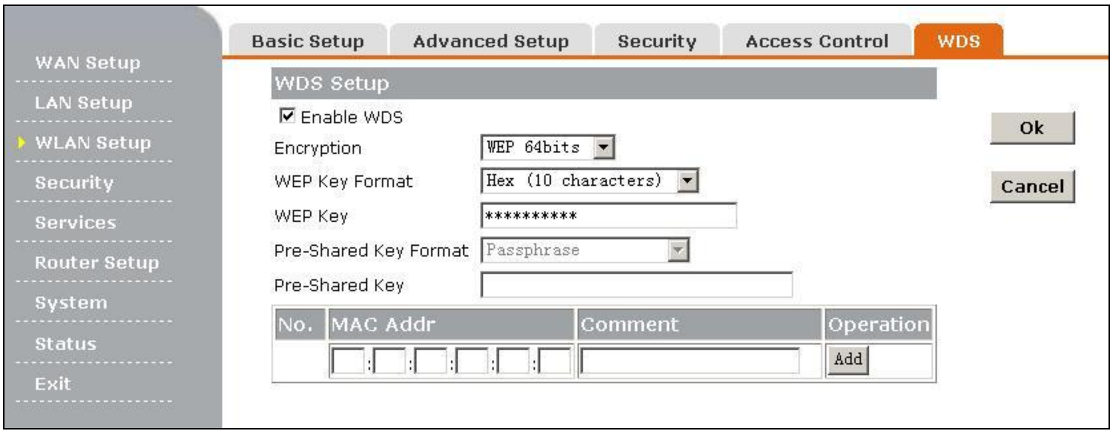
Access Control Setup

Access Control Mode: Allow Listed

No.	MAC Addr	Comment	Operation
	: : : : :		Add

Access Control Mode: If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS



WDS Setup

☑ Enable WDS

Encryption: WEP 64bits

WEP Key Format: Hex (10 characters)

WEP Key: **********

Pre-Shared Key Format: Passphrase

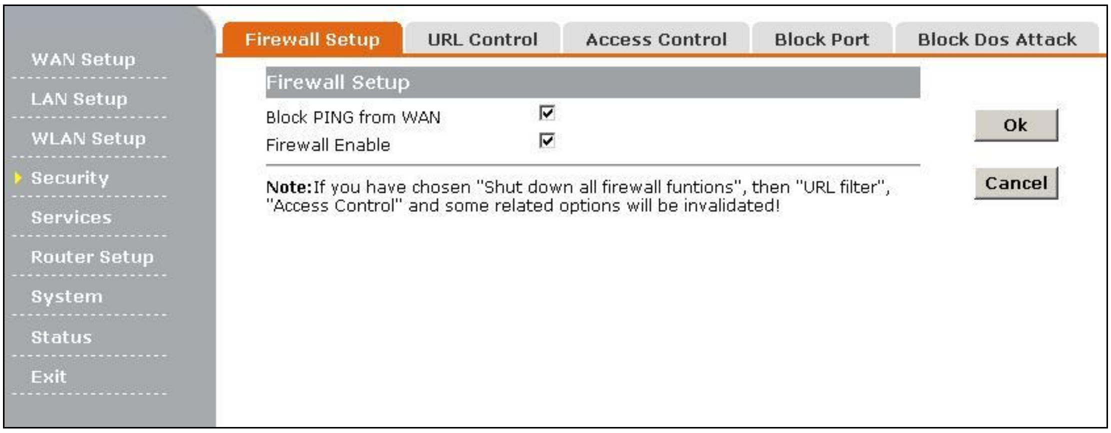
Pre-Shared Key:

No.	MAC Addr	Comment	Operation
	: : : : :		Add

Encryption: You may select WEP 64bits, WEP 128bits, WPA (TKIP), WPA (AES).
WEP Key Format: You may select to select ASCII Characters or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key.
WEP Key: Set key to encrypt your data
Pre-Shared Key Format: You can select PASSPHRASE or HEX(64 CHARACTERS).
Pre-Shared Key: Pre-shared key(PSK) is a method to set encryption keys. Commonly used in Wi-Fi Protected Access and WEP.

3.8 Security

The router provides extensive firewall protection by restricting connection parameters to limit the risk of intrusion and defending against a wide array of common hacker attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a demilitarized zone (DMZ).



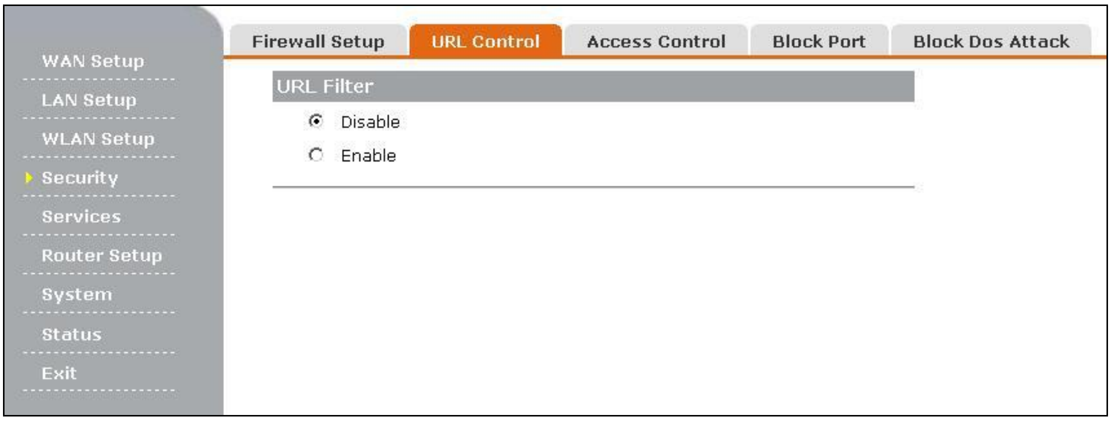
Firewall Setup

Block PING from WAN ☑

Firewall Enable ☑

Note: If you have chosen "Shut down all firewall funtions", then "URL filter", "Access Control" and some related options will be invalidated!

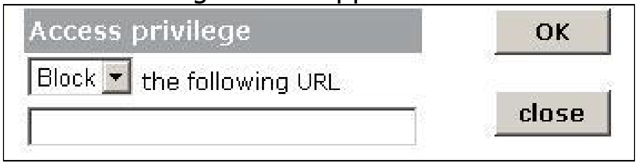
To configure the URL Filtering feature, use the table as flow to specify the web sites (www.somesite.com) or web URLs containing the keyword you want to filter on your network.



URL Filter

● Disable
○ Enable

1. Click ***Enable*** button. The dialog box will appear as follow.

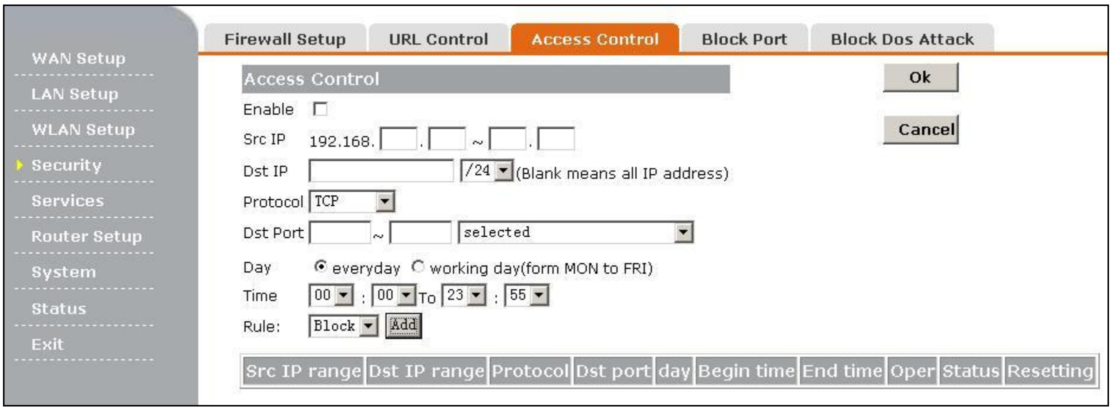


Access privilege

Block ▾ the following URL

2. Select ***Block*** or ***Allow*** the URL.
3. Type the Web sites.
4. Click ***OK*** button. The text to be blocked will appear in the URL Filter Table.

You can filter Internet access for local clients based on IP addresses, application types, (i.e., HTTP port), and time of day.



Access Control

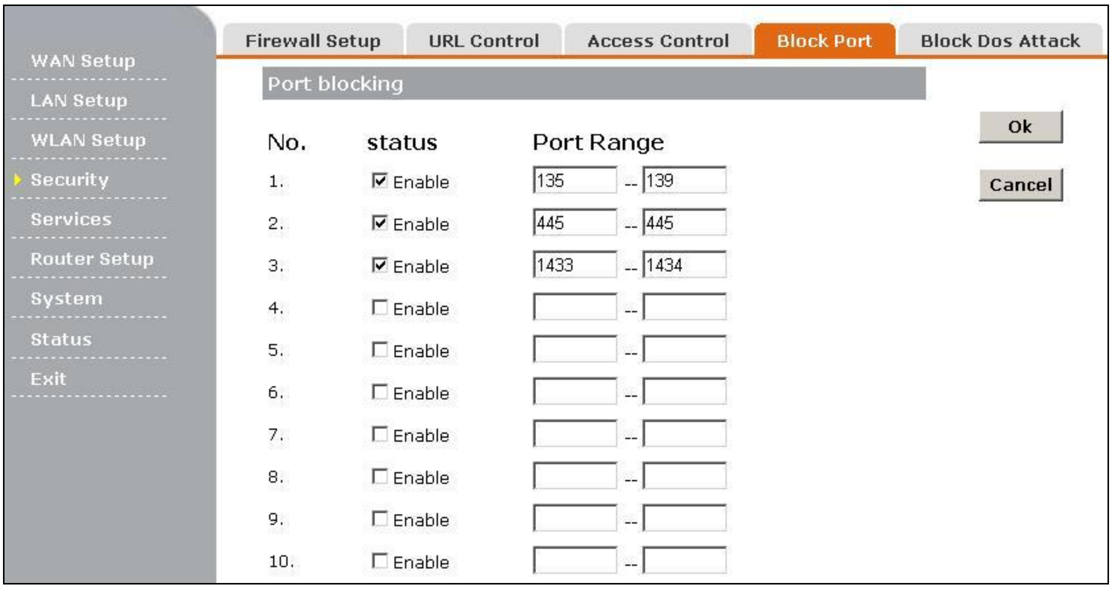
Enable □
Src IP 192.168. [ ] . [ ] ~ [ ] . [ ]
Dst IP [ ] /24 ▾ (Blank means all IP address)
Protocol TCP ▾
Dst Port [ ] ~ [ ] selected ▾
Day ● everyday ○ working day(form MON to FRI)
Time 00 ▾ : 00 ▾ To 23 ▾ : 55 ▾
Rule: Block ▾

Src IP range	Dst IP range	Protocol	Dst port	day	Begin time	End time	Oper	Status	Resetting

Enble: If this function is enabled, only the list will be allowed or blocked access to the Internet.
Src IP: The IP address of the LAN computer that will be control to the Internet.
Dst IP: The IP address of the Internet that will be control.
Protocol: Select the protocol type , TCP or UDP
Dst Port: The single prot or port range that will be control to the Internet.
Rule: There are two option, Block and Allow option. If you select Block, the Router will block the list to access the Internet. If you select Allow, the Router will Allow the list to access the Internet.

Click Add button to add the list to the table.
When finished making your change on this tab, click the ***Ok*** button to save this changes, or click the ***Cancel*** button to undo your changes.

This page is used to filter or block ports form Internet access by Port Range

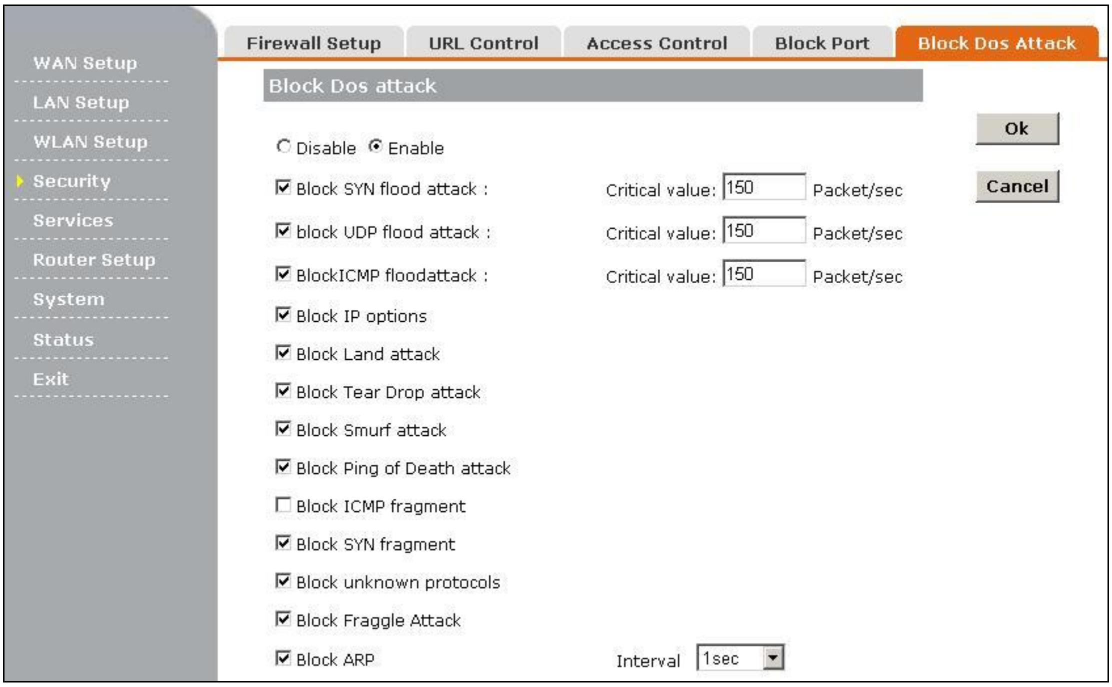


Port blocking

No.	status	Port Range
1.	☑ Enable	135 -- 139
2.	☑ Enable	445 -- 445
3.	☑ Enable	1433 -- 1434
4.	☐ Enable	--
5.	☐ Enable	--
6.	☐ Enable	--
7.	☐ Enable	--
8.	☐ Enable	--
9.	☐ Enable	--
10.	☐ Enable	--

1. Enter the port numbers you want to filter in the Port Range fields.
2. Click ***Enable*** checkbox for each filter you want the Gateway to use.
3. When finished making your change on this tab, click the ***Ok*** button to save this changes, or click the ***Cancel*** button to undo your changes.

This page used to Block Dos attack.



Block Dos attack

○ Disable ● Enable

☑ Block SYN flood attack : Critical value: 150 Packet/sec

☑ block UDP flood attack : Critical value: 150 Packet/sec

☑ BlockICMP floodattack : Critical value: 150 Packet/sec

☑ Block IP options

☑ Block Land attack

☑ Block Tear Drop attack

☑ Block Smurf attack

☑ Block Ping of Death attack

□ Block ICMP fragment

☑ Block SYN fragment

☑ Block unknown protocols

☑ Block Fraggle Attack

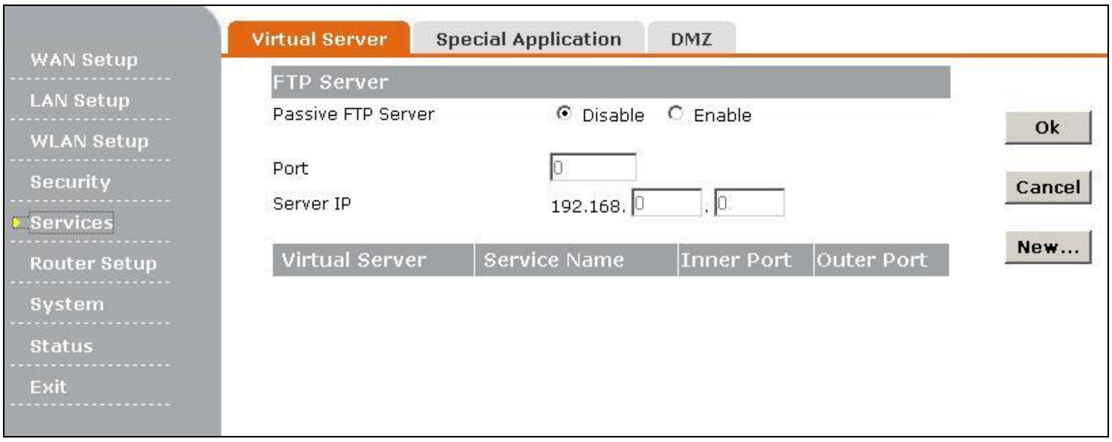
☑ Block ARP Interval 1sec

1. Click each Block attack checkbox for each filter you want the Gateway to use.
2. Select ***Enable*** button to Block Dos Attack.
3. When finished making your change on this tab, click the ***Ok*** button to save this changes, or click the ***Cancel*** button to undo your changes.

3.9 Services

If you configure the router as Virtual Server, remote users accessing services such as Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP address. In other words, depending on the requested service (TCP/UDP port number), the router redirects the external service request to the appropriate server.

Before using Virtual Server, you should add a static IP address to the designated PC. The following will allow you to open a single port or a range of ports.



FTP Server

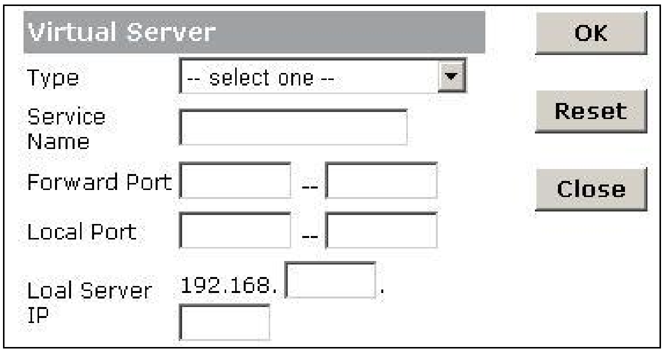
Passive FTP Server ● Disable ○ Enable

Port 0

Server IP 192.168. 0 . 0

Virtual Server	Service Name	Inner Port	Outer Port

1. Click ***New*** button. The Virtual Server dialog box will appear as follow.



Virtual Server

Type -- select one --

Service Name

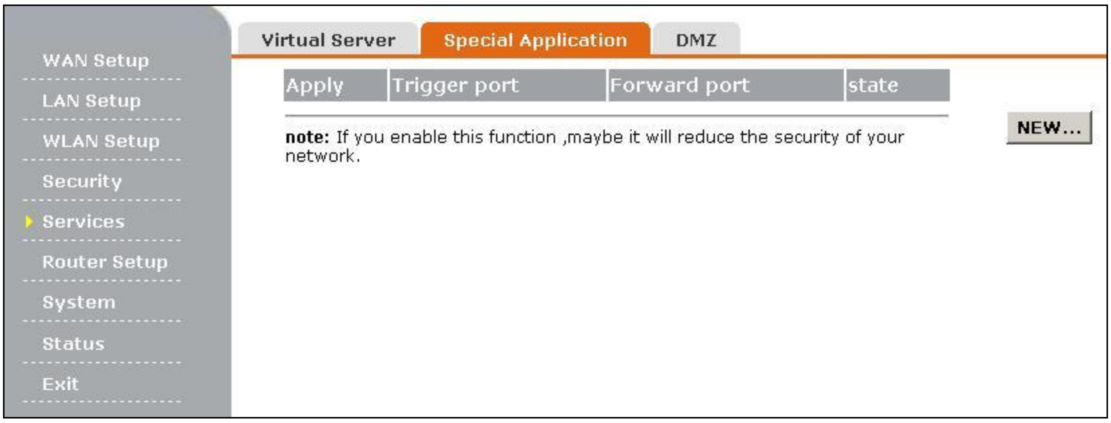
Forward Port --

Local Port --

Loal Server IP 192.168. .

2. Enter the Service Name, Forward Port, Local Port, and Local Server IP Address.
3. Click ***OK*** button to add the setting in the list and close the dialog box.

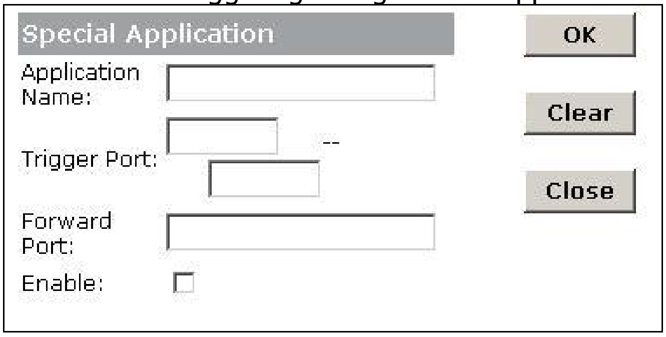
Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the ***Trigger Port*** field, then enter the ***Forward ports*** associated with the trigger port to open them for inbound traffic.



Apply	Trigger port	Forward port	state

note: If you enable this function ,maybe it will reduce the security of your network.

1. Click ***New*** button. The Port Triggering dialog box will appear as follow.



Special Application

Application Name:

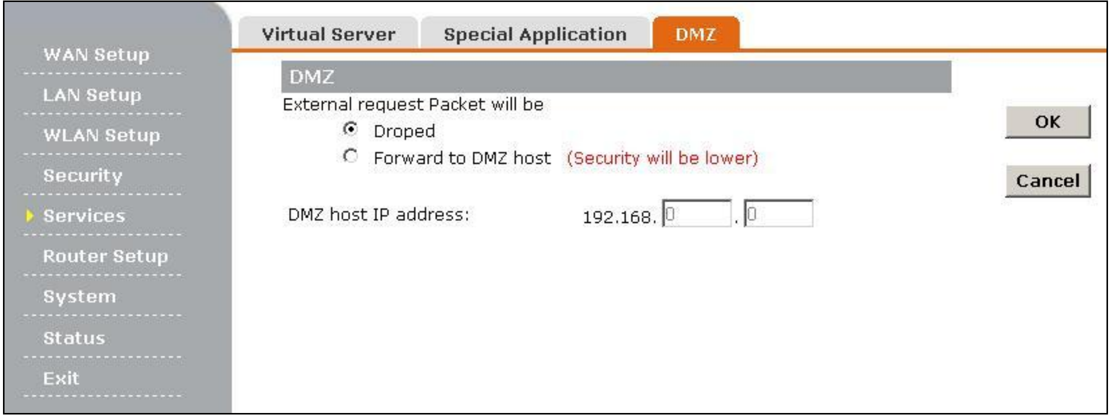
Trigger Port: --

Forward Port:

Enable: ☐

2. Enter the Application Name, Trigger Port, Forward Port.
3. Click ***Enable*** frame button.
4. Click ***OK*** button to add the setting in the list and close the dialog box.

If you have a client PC that cannot run Internet application properly from behind the NAT firewall or after configuring the Virtual Server, then you can open the client up to unrestricted two-way Internet access.



DMZ

External request Packet will be

● Droped

○ Forward to DMZ host (Security will be lower)

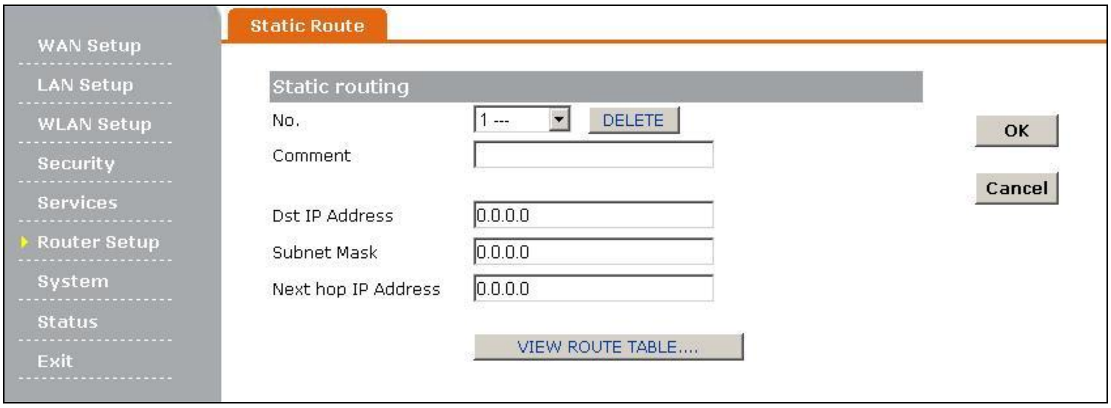
DMZ host IP address: 192.168. 0 . 0

Set ***Forward to DMZ host***, Enter the IP address of a DMZ host to ***DMZ Host IP Address***. Adding a client to the DMZ (Demilitarized Zone) may expose your local network to a variety of security risks, so only use this option as a last resort.

3.10 Route Setup

Static Route

A static route is a pre-determined pathway that network information must travel to reach a specific host or network.



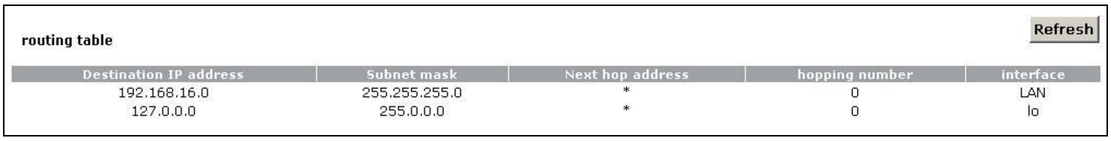
Static routing

No.	1 ---
Comment	
Dst IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Next hop IP Address	0.0.0.0

1. Select a number form drop-down menu.
2. Enter Destination IP address, Subnet Mask, and Next hop IP Address.
3. Click OK button to save the setting.

View Route Table

The routing table displays the current routing information in system.

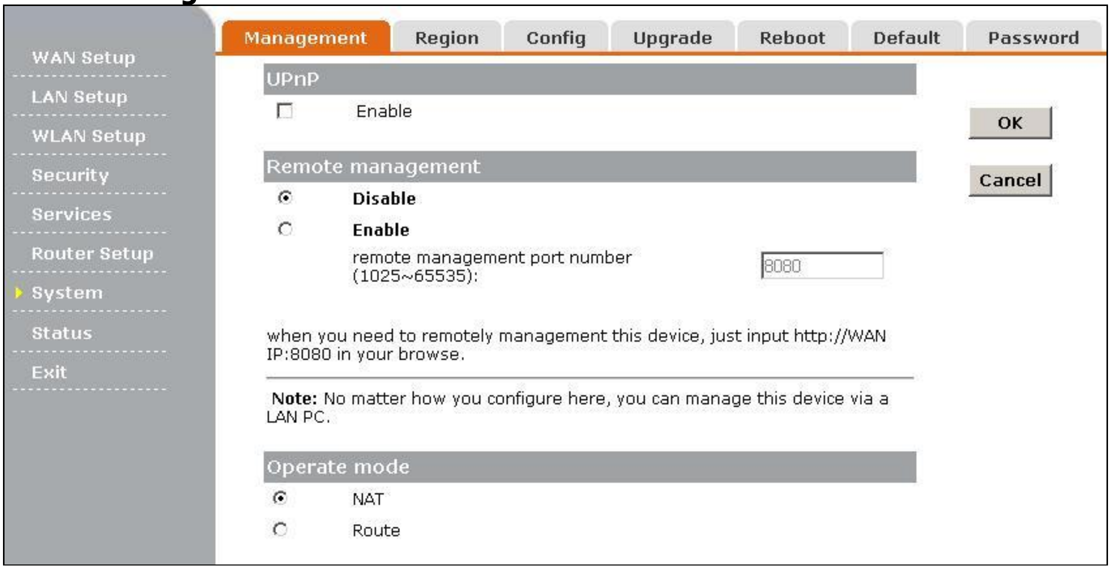


routing table

Destination IP address	Subnet mask	Next hop address	hopping number	interface
192.168.16.0	255.255.255.0	*	0	LAN
127.0.0.0	255.0.0.0	*	0	lo

3.11 System

3.11.1 Management



UPnP

□ Enable

Remote management

● Disable

○ Enable

remote management port number (1025~65535): 8080

when you need to remotely management this device, just input http://WAN IP:8080 in your browse.

Note: No matter how you configure here, you can manage this device via a LAN PC.

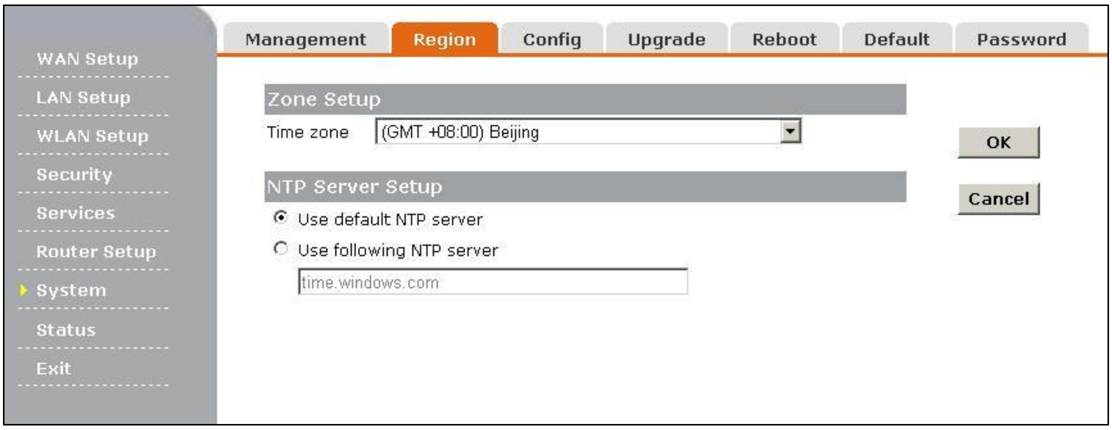
Operate mode

● NAT

○ Route

UPnP: UPnP (Universal Plug and Play) allows automatic discovery and configuration of equipment attached to your LAN. UPnP is by supported by Windows ME, XP, or later.
Remote mamagement: This feature allows you to manage the router from a remote location, via the Internet. To Enable Remote Management, Click the ***Enable*** radio button, then enter the port number you will use to remotely access the Router. The default port is 8080. Finally click ***OK*** button to save it.
Operate mode: Select the Router's operate mode, NAT or Route.

3.11.2 Region



Zone Setup

Time zone (GMT +08:00) Beijing

NTP Server Setup

● Use default NTP server

○ Use following NTP server

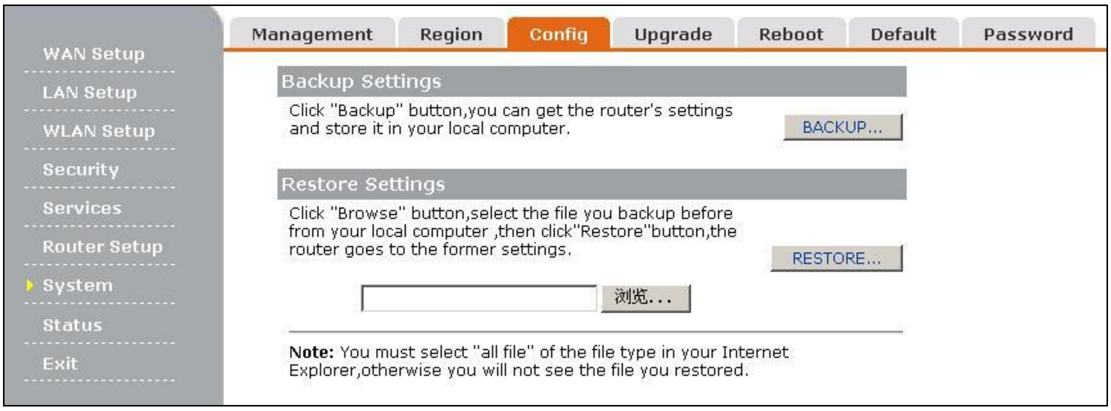
time.windows.com

Backup Settings

Click ***Backup*** button, you can get the router's settings and store it in your local computer.

Restore Settings

Click ***Browse*** button, select the file you backup before from your local computer, then click ***Restore*** button, the router goes to the former settings.



Backup Settings

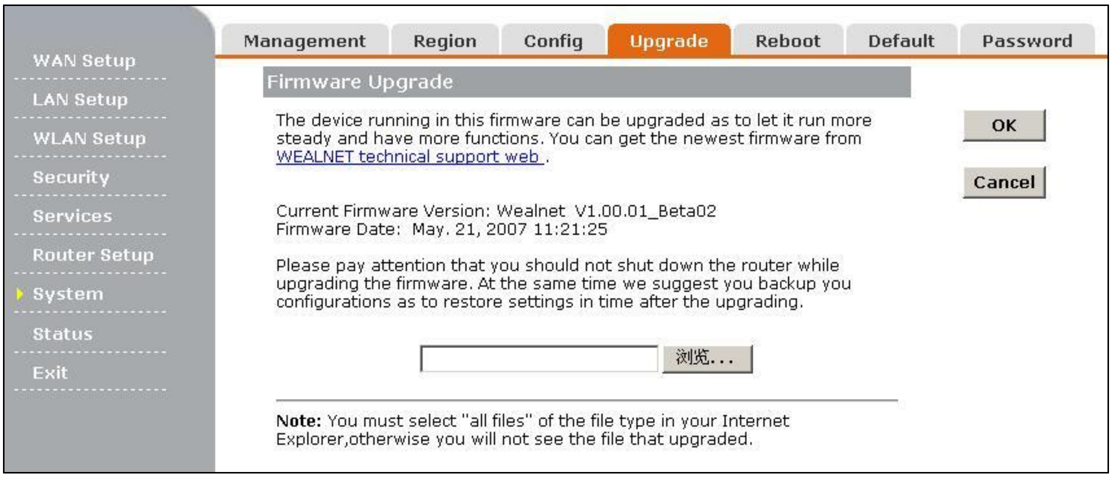
Click "Backup" button,you can get the router's settings and store it in your local computer.

Restore Settings

Click "Browse" button,select the file you backup before from your local computer ,then click"Restore"button,the router goes to the former settings.

Note: You must select "all file" of the file type in your Internet Explorer,otherwise you will not see the file you restored.

You can upgrade the firmware of the Router here.



Firmware Upgrade

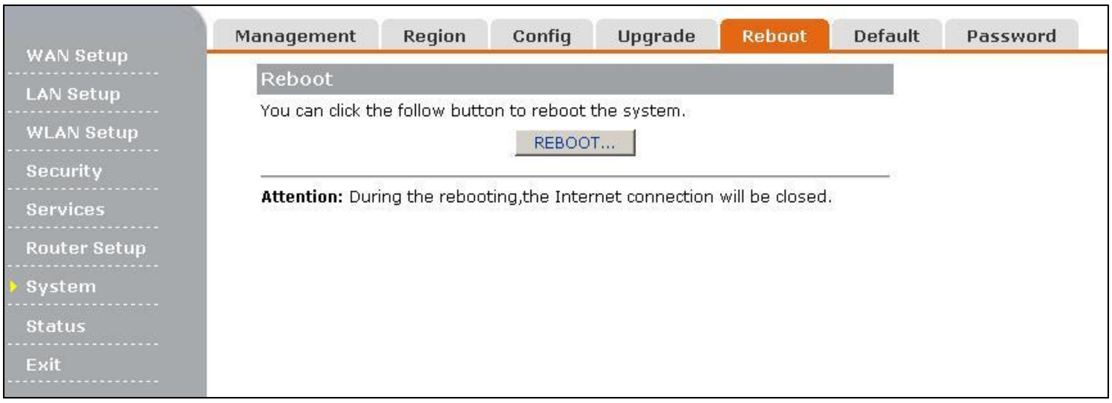
The device running in this firmware can be upgraded as to let it run more steady and have more functions. You can get the newest firmware from WEALNET technical support web .

Current Firmware Version: Wealnet V1.00.01_Beta02
Firmware Date: May. 21, 2007 11:21:25

Please pay attention that you should not shut down the router while upgrading the firmware. At the same time we suggest you backup you configurations as to restore settings in time after the upgrading.

Note: You must select "all files" of the file type in your Internet Explorer,otherwise you will not see the file that upgraded.

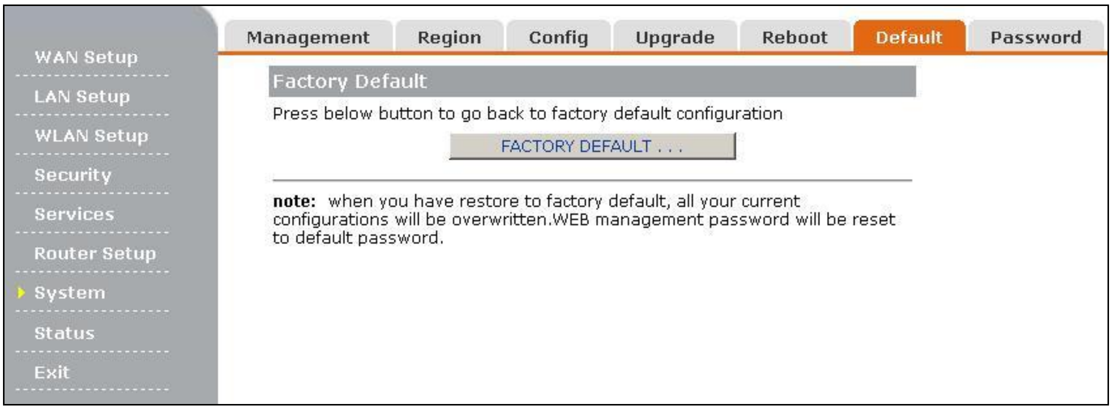
You can click the ***Reboot*** button to restart the Router.



Reboot

You can click the follow button to reboot the system.

Attention: During the rebooting,the Internet connection will be closed.



Factory Default

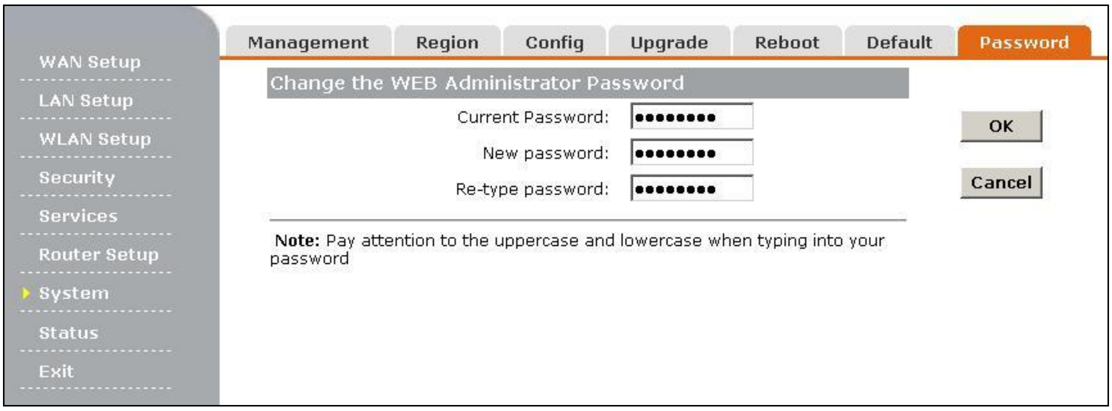
Press below button to go back to factory default configuration

note: when you have restore to factory default, all your current configurations will be overwritten.WEB management password will be reset to default password.

Click **Factory Default** button, the router’s settings will be restored factory default config, at the same time and the administrator web password will restore to the default password.

To ensure the Router’s security, you will be asked for your password when you access the Router’s Web-based Utility. The default user name is **admin** and password is **admin**.

This page will allow you to change the User name and User passwords.



Change the WEB Administrator Password

Current Password: ●●●●●●●●●

New password: ●●●●●●●●●

Re-type password: ●●●●●●●●●

Note: Pay attention to the uppercase and lowercase when typing into your password

3.12 Resetting the router

The router has a ***reset*** button at the rear panel of the device. For some circumstances you might need to reset the router. Please follow these steps:

1. Leave the device powered on, do not disconnect the power
2. Press the reset button and hold
3. Keep the button pressed about 5 seconds
4. Release the button.

The Router will then automatically reboot itself.

If the Router locks up, simply power it down for 3 to 5 seconds by removing the power cable from the Router’s Power Port.