MONOPRICE®

User Guide

MW368R

www.monoprice.com

Wireless 802.11N Router

with Internal Antenna and WPS Function -2T2R MIMO

Copyright Statement

MONOPRICE® is the registered trademark of Monoprice, Inc. All the products and product names mentioned herein are the trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Monoprice, Inc. Without the permission of Monoprice, Inc., any individual or party is not allowed to copy, plagiarize, reproduce or translate it into other languages.

All the photos and product specifications mentioned in this manual are for references only. Upgrades of software and hardware may occur, and if there are changes, Monoprice is not responsible for notifying in advance. If you would like to know more about our products, please visit our website at www.monoprice.com

Contents

Chapter 1 Product Introduction

Thank you for purchasing the Monoprice Wireless N Broadband Router!

This easy-to-use router provides a simple configuration interface, which allows you to configure it with ease. It is based on the latest IEEE802.11n standard and is backwards compatible with devices using the IEEE802.11b/g standards.

The Monoprice wireless router provides router, wireless AP, four-port switch, and firewall functions in one package. It provides a powerful online monitor function and supports URL and MAC filtering. With the WDS function, it can repeat and amplify wireless signals to expand wireless network coverage area. It fully supports UPnP and WMM for better video streaming and VOIP quality. With the QoS function it can efficiently manage bandwidth availability for connected clients. Wireless ISP functionality allows this router to wirelessly connect to an Access Point and provide wired access to client computers.

1.1 Package Contents

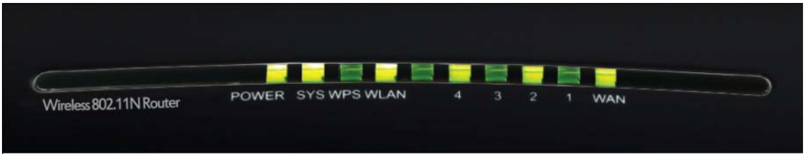
Please verify the following items are in the package:

- One Wireless N Broadband Router
- One Quick Installation Guide
- One Power Adapter
- One Software CD

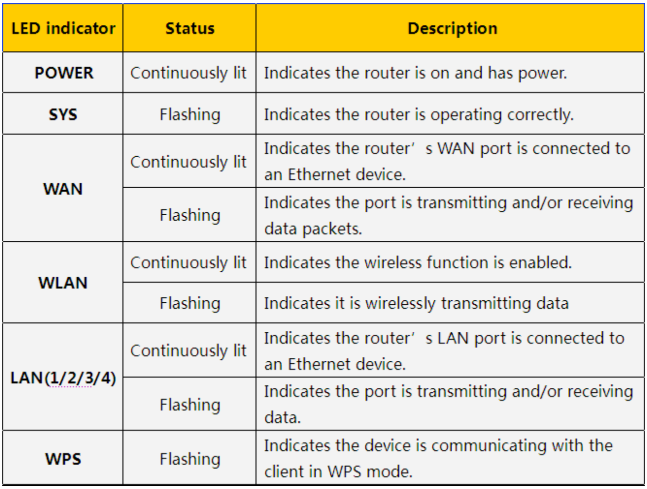
If any of the listed items are missing or damaged, please contact Monoprice for immediate replacement.

1.2 LED Indicators and Port Description

Panel and LED indicators show:

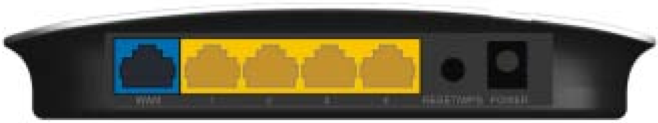


LED indicator description on the front panel

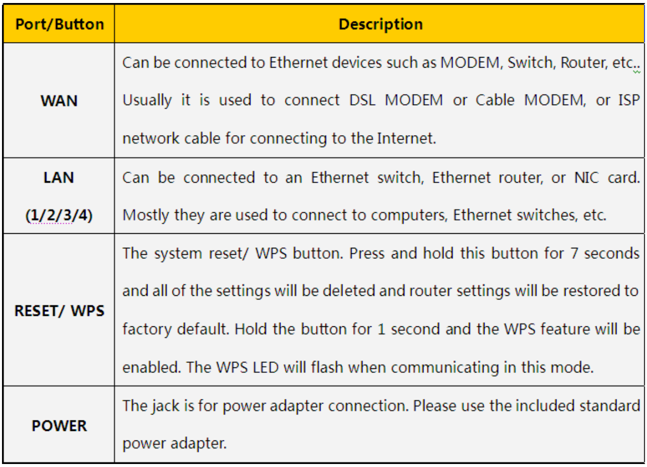


LED indicator	Status	Description
POWER	Continuously lit	Indicates the router is on and has power.
SYS	Flashing	Indicates the router is operating correctly.
WAN	Continuously lit	Indicates the router' s WAN port is connected to an Ethernet device.
	Flashing	Indicates the port is transmitting and/or receiving data packets.
WLAN	Continuously lit	Indicates the wireless function is enabled.
	Flashing	Indicates it is wirelessly transmitting data
LAN(1/2/3/4)	Continuously lit	Indicates the router' s LAN port is connected to an Ethernet device.
	Flashing	Indicates the port is transmitting and/or receiving data.
WPS	Flashing	Indicates the device is communicating with the client in WPS mode.

Back panel ports



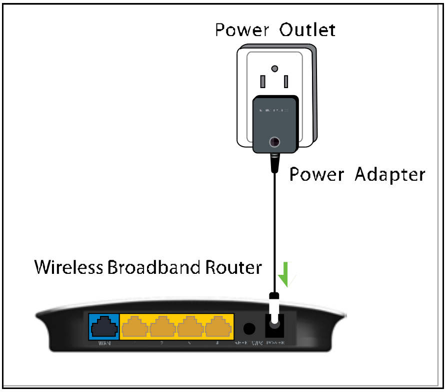
Back panel port description



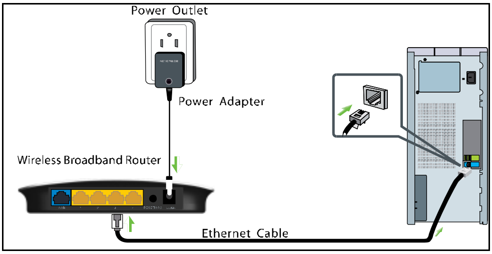
Port/Button	Description
WAN	Can be connected to Ethernet devices such as MODEM, Switch, Router, etc.. Usually it is used to connect DSL MODEM or Cable MODEM, or ISP network cable for connecting to the Internet.
LAN (1/2/3/4)	Can be connected to an Ethernet switch, Ethernet router, or NIC card. Mostly they are used to connect to computers, Ethernet switches, etc.
RESET/ WPS	The system reset/ WPS button. Press and hold this button for 7 seconds and all of the settings will be deleted and router settings will be restored to factory default. Hold the button for 1 second and the WPS feature will be enabled. The WPS LED will flash when communicating in this mode.
POWER	The jack is for power adapter connection. Please use the included standard power adapter.

Chapter 2 Product Installation

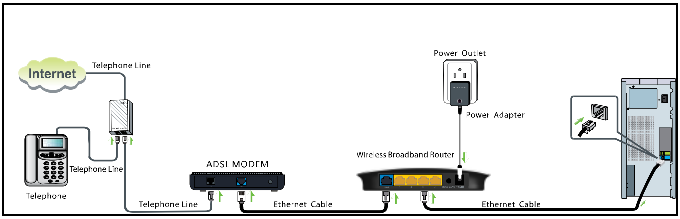
1. Warning! Use only the included power adapter to power your router. **NOTE**: Use of an unmatched power adapter could cause damage to this product.



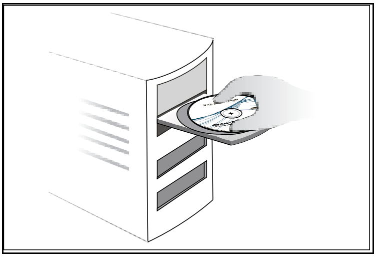
2. Connect the router's LAN port to your computer with an Ethernet cable as shown below.



3. Connect your broadband line provided by your ISP to the router's WAN port.



4. Insert the included software CD into the CD drive of your computer. After the disc has loaded double click the **Setup** icon and follow the instructions to complete the installation. You can also use the router's Web-based Utility to complete the configuration.

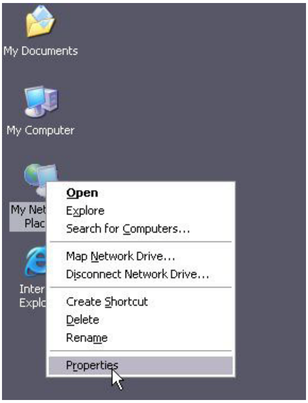


Chapter 3 Preparing to Access the Internet

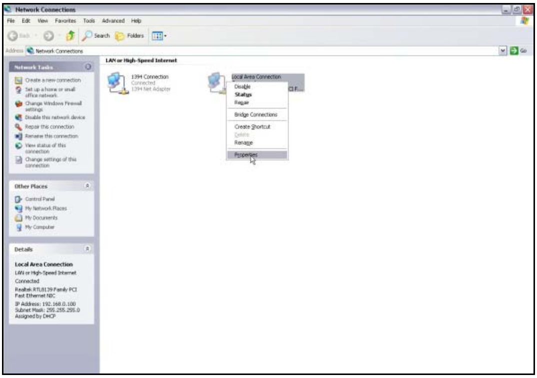
3.1 Setup the Network Configuration on Your PC

Network Configuration under windows XP

1. Right click **My Network Places** on your computer desktop and select **Properties**.

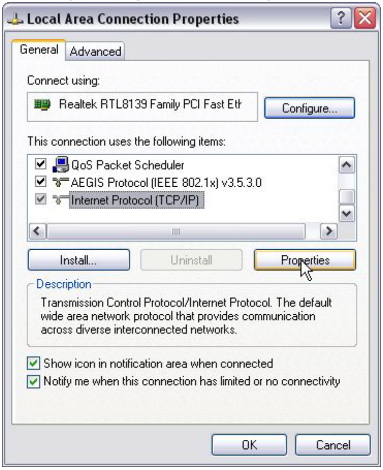


2. Right click **Local Area Connection** and select **Properties**.



Local Area Connection
LAN or High-Speed Internet
Connected
Realtek RTL8139 Family PCI Fast Ethernet NIC
IP Address: 192.168.0.100
Subnet Mask: 255.255.255.0
Assigned by DHCP

3. Select **Internet Protocol (TCP/IP)** and click **Properties**.



Local Area Connection Properties

Connect using:

Realtek RTL8139 Family PCI Fast Eth

This connection uses the following items:

☑ QoS Packet Scheduler
☑ AEGIS Protocol (IEEE 802.1x) v3.5.3.0
☑ Internet Protocol (TCP/IP)

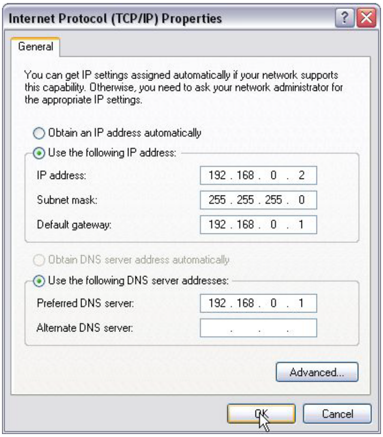
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

4. Select **Use the following IP address** and enter the IP address, Subnet mask, Default gateway as follows:

- **IP Address:** 192.168.0.XXX: (XXX is a number from 2~254)
- **Subnet Mask:** 255.255.255.0
- **Gateway:** 192.168.0.1
- **DNS server:** You should input the DNS server address provided by your ISP. Otherwise, you can enter 192.168.0.1. Click **OK** to save the configurations.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

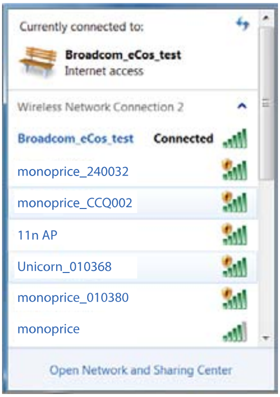
IP address: 192 . 168 . 0 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 1
Alternate DNS server: . . .

Network Configuration under windows 7

1. Click the network icon on the lower right corner of your computer desktop, and then click **Open Network and Sharing Center**.



Currently connected to:

Broadcom_eCos_test
Internet access

Wireless Network Connection 2

Broadcom_eCos_test **Connected**

monoprice_240032

monoprice_CCQ002

11n AP

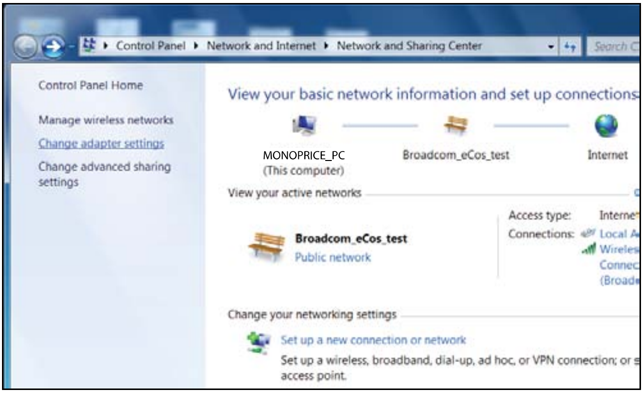
Unicorn_010368

monoprice_010380

monoprice

Open Network and Sharing Center

2. Click **Change adapter settings** on the left side of the window.



Control Panel ▸ Network and Internet ▸ Network and Sharing Center

Search C

Control Panel Home

Manage wireless networks

Change adapter settings

Change advanced sharing settings

View your basic network information and set up connections

MONOPRICE_PC
(This computer)

Broadcom_eCos_test

Internet

View your active networks

Broadcom_eCos_test
Public network

Access type: Interne

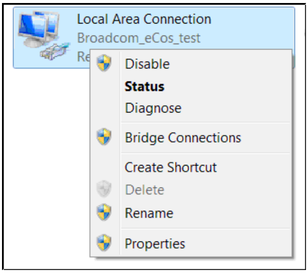
Connections: Local A
Wireles
Connec
(Broad

Change your networking settings

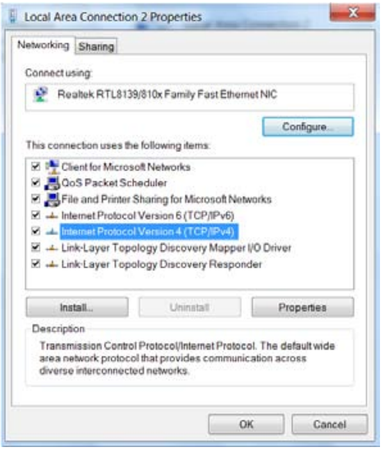
Set up a new connection or network

Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or s access point.

3. Right click **Local Area Connection** and select **Properties**.



4. Double click **Internet Protocol Version 4 (TCP/IPv4)**.



Connect using:

Realtek RTL8139/810x Family Fast Ethernet NIC

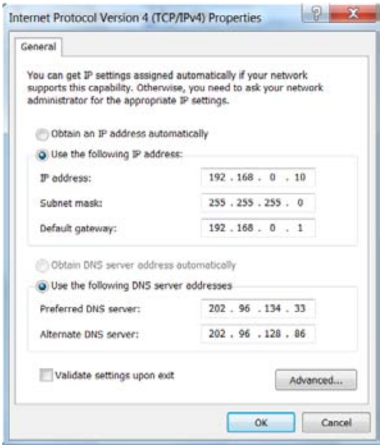
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

5. Select **Use the following IP address** and enter the IP address, Subnet mask, Default gateway as follows:



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses

Preferred DNS server: 202 . 96 . 134 . 33

Alternate DNS server: 202 . 96 . 128 . 86

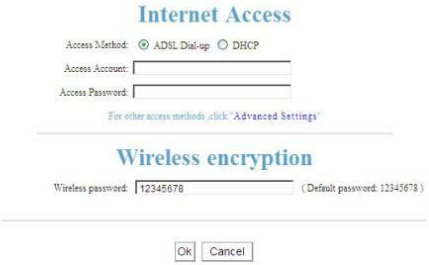
□ Validate settings upon exit

- **IP Address:** 192.168.0.XXX: (XXX is a number from 2~254)
- **Subnet Mask:** 255.255.255.0
- **Gateway:** 192.168.0.1
- **DNS server:** You should input the DNS server address provided by your ISP. Otherwise, you can enter 192.168.0.1. Click **OK** to save the configurations.

3.2 Log in to the Router

To access the Router's Web-based Utility, launch a web browser such as Internet Explorer or Firefox and enter http://192.168.0.1. Press **Enter**.

http://192.168.0.1/



Internet Access

Access Method: ● ADSL Dial-up ○ DHCP

Access Account:

Access Password:

For other access methods ,click "Advanced Settings"

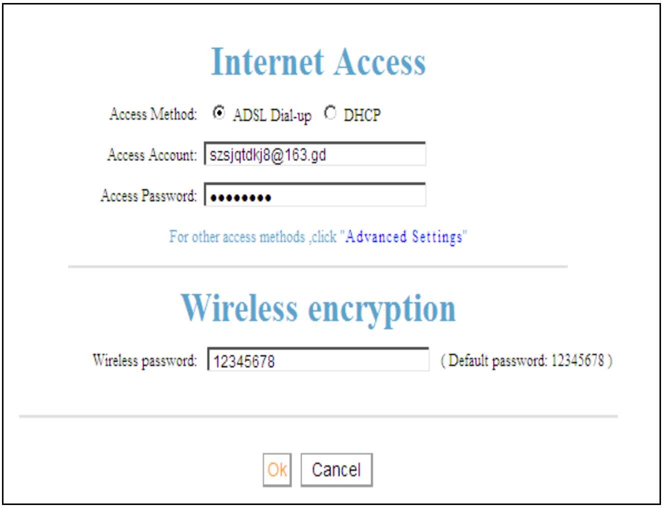
Wireless encryption

Wireless password: 12345678 （Default password: 12345678）

3.3 Fast Internet Access

Two kinds of fast access methods are provided on the router's web-based utility: ADSL Dial-up and DHCP.

If you select ADSL Dial-up, you need to enter the access account name and access password for your ADSL account (provided by your ISP), as well as the wireless password (default is **12345678**), then click **Ok** to complete the settings.



Internet Access

Access Method: ● ADSL Dial-up ○ DHCP

Access Account: szsjqtdkj8@163.gd

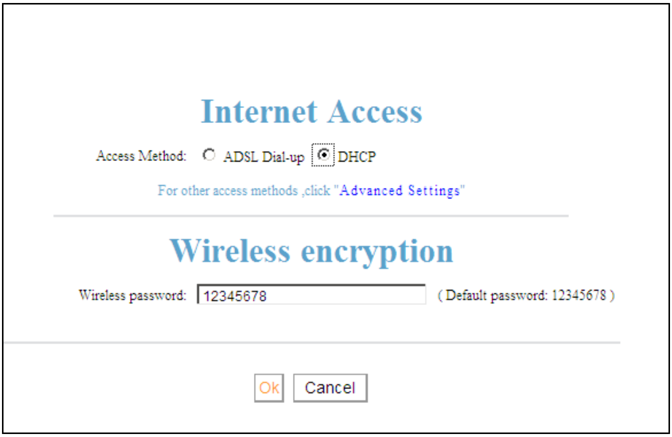
Access Password: ••••••••

For other access methods ,click "Advanced Settings"

Wireless encryption

Wireless password: 12345678 (Default password: 12345678)

If you select DHCP, you only need to enter the wireless password (default is **12345678**) and click **Ok** to complete the settings.



Internet Access

Access Method: ○ ADSL Dial-up ● DHCP

For other access methods ,click "Advanced Settings"

Wireless encryption

Wireless password: 12345678 (Default password: 12345678)

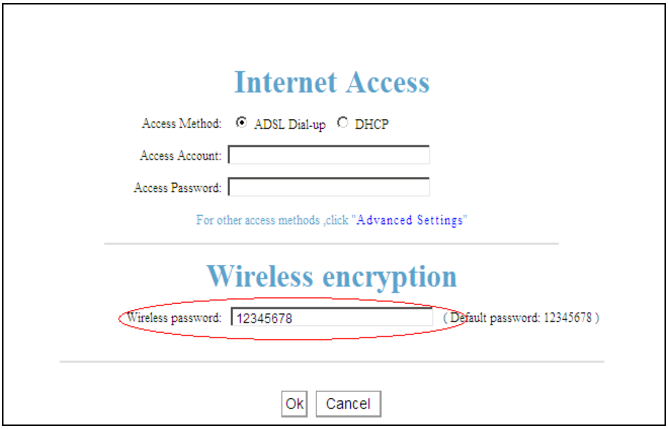
The default access method is ADSL Dial-up and the access account and access password are the same as the ADSL Dial-up account and password, which you can obtain from your broadband ISP. For other access methods, please refer to WAN settings in chapter 4.The wireless password can only consist of 8 characters, the default is **12345678**, and you can modify it when necessary.

3.4 Fast Encryption

The router provides two encryption setting screens, one is simple and easy, the other is advanced. For instructions on using the advanced setting, please refer to chapter 5.2.

Simple and easy setup:

Log on to the router's web-based utility and choose the encryption method for the router. The default method uses the WPA-PSK mode and AES algorithm. The default password is **12345678**, as shown below.



Internet Access

Access Method: ● ADSL Dial-up ○ DHCP

Access Account:

Access Password:

For other access methods ,click "Advanced Settings"

Wireless encryption

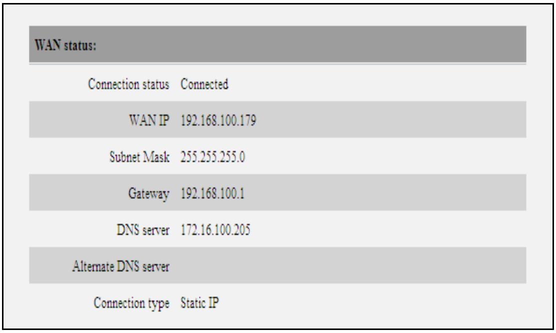
Wireless password: 12345678 (Default password: 12345678)

⚠**NOTE: The wireless password can only be 8 characters in length and the default is 12345678. You can modify it when necessary.**

Chapter 4 Advanced Settings

4.1 System Status

Click **Advanced Settings > System Status** to view the router's WAN port and system status.



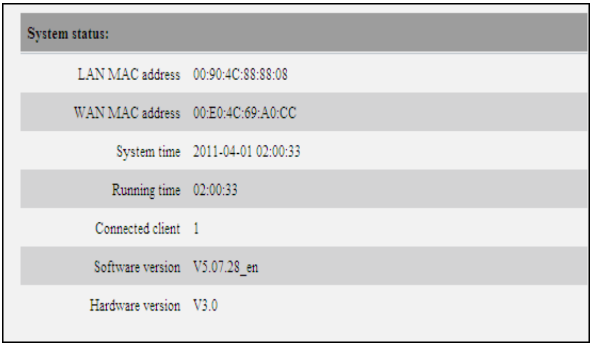
WAN status:	
Connection status	Connected
WAN IP	192.168.100.179
Subnet Mask	255.255.255.0
Gateway	192.168.100.1
DNS server	172.16.100.205
Alternate DNS server	
Connection type	Static IP

- **Connection status:** Displays the router's WAN connection status.

  Disconnected: Indicates the router's WAN port hasn't been connected with a network cable.

  Connecting: Indicates the router's WAN port is obtaining an IP address.

  Connected: Indicates the Router is properly connected to the ISP.
- **WAN IP:** IP address obtained from ISP.
- **Subnet mask:** Obtained from ISP.
- **Gateway:** Obtained from ISP.
- **DNS server:** Obtained from ISP.
- **Alternate DNS server:** Obtained from ISP.
- **Connection type:** Displays your current access method.



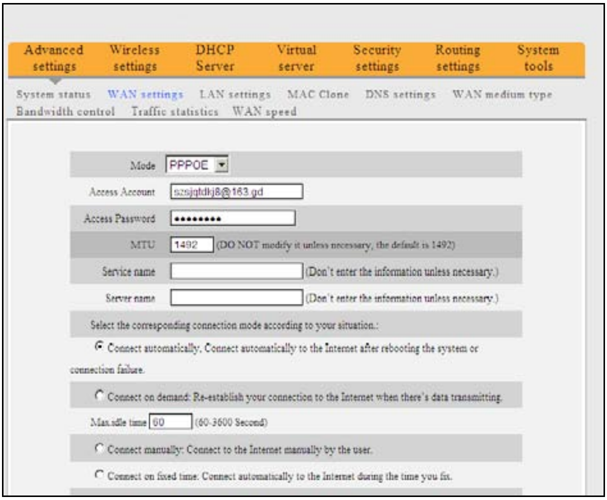
System status:	
LAN MAC address	00:90:4C:88:88:08
WAN MAC address	00:E0:4C:69:A0:CC
System time	2011-04-01 02:00:33
Running time	02:00:33
Connected client	1
Software version	V5.07.28_en
Hardware version	V3.0

- **LAN MAC address**：Displays the Router's LAN MAC address.
- **WAN MAC address**：Displays the Router's WAN MAC Address.
- **System time**：Displays the system's updated time
- **Connected client**：Displays the number of the connected computers (normally displays the number of clients whose IP addresses are obtained via DHCP server).
- **Software version**：Displays the Router's software version.
- **Hardware versio**n：Displays the Router's hardware version.

4.2 WAN Settings

Click **Advanced Settings > WAN settings** to configure the router's WAN settings.

Virtual Dial-up (PPPoE)



Mode PPPOE

Access Account szsjqtdkj8@163.gd

Access Password ●●●●●●●●●

MTU 1492 (DO NOT modify it unless necessary, the default is 1492)

Service name (Don't enter the information unless necessary.)

Server name (Don't enter the information unless necessary.)

Select the corresponding connection mode according to your situation.:

● Connect automatically, Connect automatically to the Internet after rebooting the system or connection failure.

○ Connect on demand: Re-establish your connection to the Internet when there's data transmitting.

Max idle time 60 (60-3600 Second)

○ Connect manually: Connect to the Internet manually by the user.

○ Connect on fixed time: Connect automatically to the Internet during the time you fix.

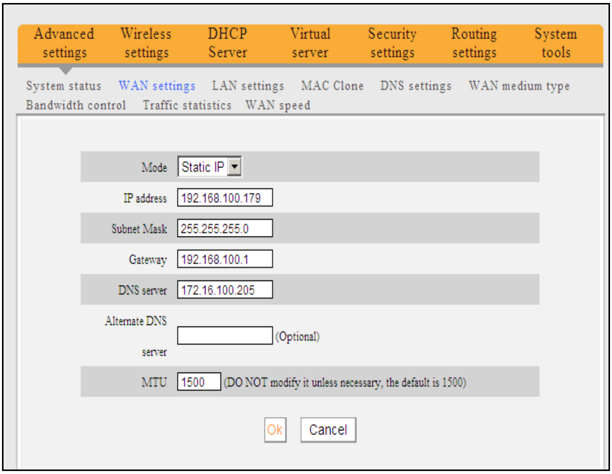
- **Mode:** Shows your current connection mode.
- **Access Account:** Enter the account provided by your ISP.
- **Access Password:** Enter the password provided by your ISP.
- **MTU:** Maximum Transmission Unit. This is the size of the largest data packet that can be sent over the network. The default value is 1492. Do NOT modify it unless necessary. If a specific website or web application software cannot open or be enabled, you can try to change the MTU value to 1450, 1400, etc.
- **Service Name:** The connection name for the current PPPOE. Enter it if required, otherwise leave it blank.
- **AC Name:** The service name. Enter it if required, otherwise leave it blank.
- **Connect Automatically:** Connects automatically to the Internet after rebooting the system or after a connection failure.
- **Connect on Demand:** Connects to the internet whenever internet activity is detected (e.g., checking email). After a set period of time, the connection will be terminated (Max Idle Time). A setting of zero means you will be connected to the Internet at all times. Otherwise, enter the number of minutes of inactivity before you are disconnected from the internet.
- **Connect Manually:** Users connect to the internet manually.
- **Connect on Fixed Time:** Connects to the internet automatically at the time specified.

⚠**NOTE:**

The "Connect on Fixed Time" setting goes into effect only when you have set the current time in "Time settings" from the "System tools" menu.

Static IP

If your ISP provides you with a static IP, please choose static IP. You will need to enter the IP address, subnet mask, gateway, DNS server, and alternate DNS server provided by your ISP or network administrator.

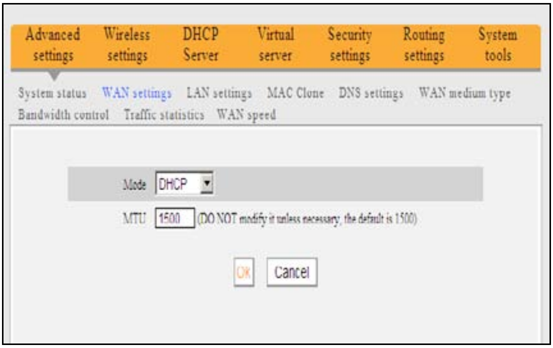


Mode	Static IP
IP address	192.168.100.179
Subnet Mask	255.255.255.0
Gateway	192.168.100.1
DNS server	172.16.100.205
Alternate DNS server	(Optional)
MTU	1500 (DO NOT modify it unless necessary, the default is 1500)

- **Mode:** Shows your current connection mode.
- **IP address:** Enter the WAN IP address provided by your ISP. If you are unsure of what it is, please contact your local ISP for assistance.
- **Subnet mask:** Enter the WAN Subnet Mask provided by your ISP. Generally it is 255.255.255.0.
- **Gateway:** Enter the Gateway provided by your ISP. If you unsure of what it is, please contact your local ISP for assistance.
- **DNS server:** Enter the necessary DNS server provided by your ISP.
- **Alternate DNS server:** Enter the secondary DNS address if your ISP provides one (this is optional).

Dynamic IP (Via DHCP)

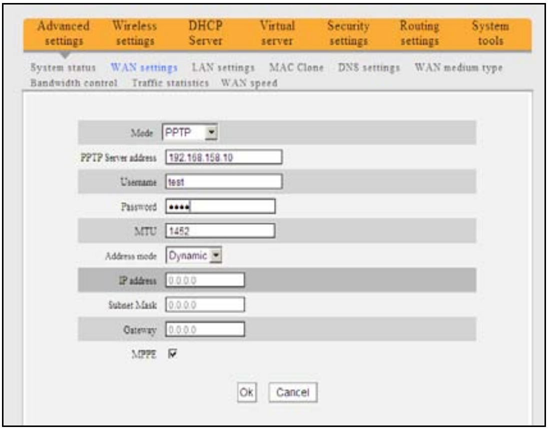
If your connection mode is Dynamic IP, it means every time you access the Internet, you will get a different IP. You don't need to enter any parameters in this mode, just click **Ok** to finish the settings.



Mode DHCP

MTU 1500 (DO NOT modify it unless necessary, the default is 1500)

PPTP



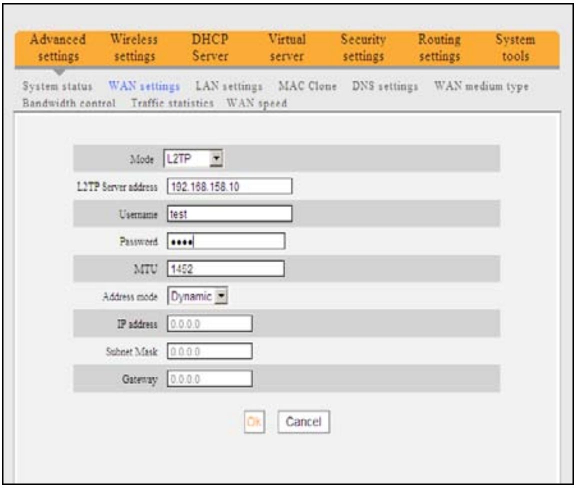
Mode	PPTP
PPTP Server address	192.168.158.10
Username	test
Password	••••
MTU	1452
Address mode	Dynamic
IP address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
MPPE	☑

- **Mode:** Shows your current connection mode.
- **PPTP server address:** The IP address or domain name of the destination server, used to specify the destination address, which is needed for a PPTP connection.
- **Username/Password:** Used to log in to the PPTP server.
- **Address mode:** Sets the router's IP address mode. You can select either **Dynamic** or **Static**. If your ISP doesn't provide a fixed IP address, please select **Dynamic**.
- **IP address:** Enter the IP address provided by your ISP. If you are unsure of what this should be, contact your local ISP for assistance.
- **Subnet mask:** Enter the subnet mask provided by your ISP, usually it is 255.255.255.0
- **Gateway:** Enter the gateway provided by your ISP. If you are unsure of what this

should be, contact your local ISP for assistance.

All the above values are provided by your ISP.

L2TP



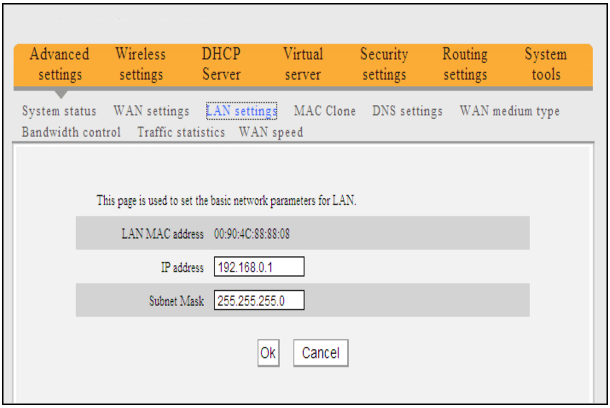
Mode	L2TP
L2TP Server address	192.168.158.10
Username	test
Password	••••
MTU	1452
Address mode	Dynamic
IP address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0

- **Mode:** Shows your current connection mode.
- **L2TP server address:** The IP address or domain name of the destination server, used to specify the destination address, which is needed for a L2TP connection.
- **Username/Password:** Used to log in to the L2TP server.
- **Address mode:** Set the router's IP address mode, you can select either **Dynamic** or **Static**. If your ISP doesn't provide a fixed IP address, please select **Dynamic**.
- **IP address:** Enter the IP address provided by your ISP. If you are unsure of what this should be, contact your local ISP for assistance.
- **Subnet mask:** Enter the subnet mask provided by your ISP, usually it is 255.255.255.0
- **Gateway:** Enter the gateway provided by your ISP. If you are unsure of what this should be, contact your local ISP for assistance.

All the above values are provided by your ISP.

4.3 LAN Settings

Click **Advanced settings > LAN settings** to configure the router's IP address and Subnet Mask.



This page is used to set the basic network parameters for LAN.

LAN MAC address 00:90:4C:88:88:08

IP address 192.168.0.1

Subnet Mask 255.255.255.0

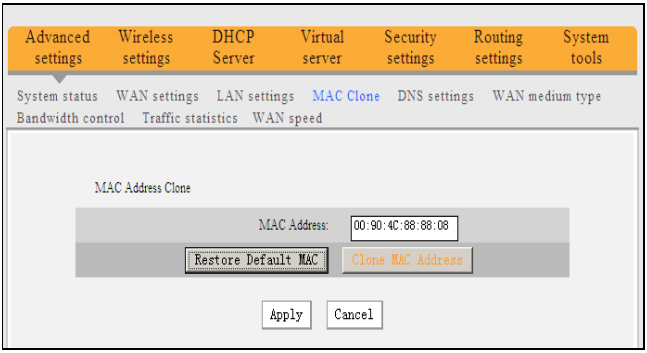
- **LAN MAC address:** The router's LAN MAC address, which cannot be changed.
- **IP address:** The router's LAN IP address (not your PC's IP address).The default value is 192.168.0.1. You can change it when necessary.
- **Subnet Mask:** The router's LAN Subnet Mask. The default value is 255.255.255.0

⚠**NOTE:**

Once you modify the IP address, you need to remember it for next time you log in to the web-based utility.

4.4 MAC Clone

Click **Advanced settings > MAC Clone** to view the following screen. This screen allows you to configure the router's WAN MAC address.



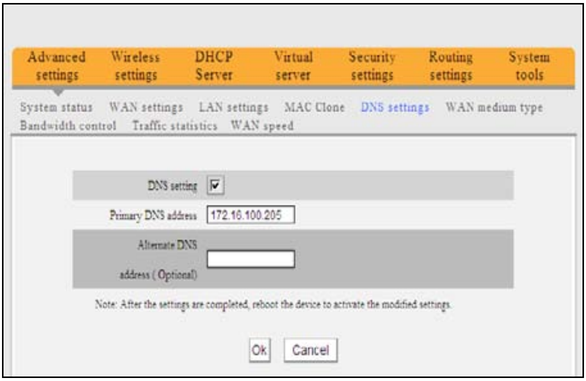
MAC Address Clone

MAC Address: 00:90:4C:88:88:08

- **MAC Address:** Set the router's WAN MAC address.
- **Clone MAC Address:** Clicking this button changes the router's WAN MAC address from the default to the MAC address of the PC you are currently using. Don't use this button unless your PC's MAC address is the one bound by your ISP.
- **Restore Default MAC:** Restores the router's WAN MAC to default settings.

4.5 DNS Settings

Click **Advanced settings > DNS settings** to view the following screen. DNS stands for Domain Name System (or Service).



DNS setting ☑

Primary DNS address 172.16.100.205

Alternate DNS address (Optional)

Note: After the settings are completed, reboot the device to activate the modified settings.

- **DNS setting:** Select to enable the DNS server.

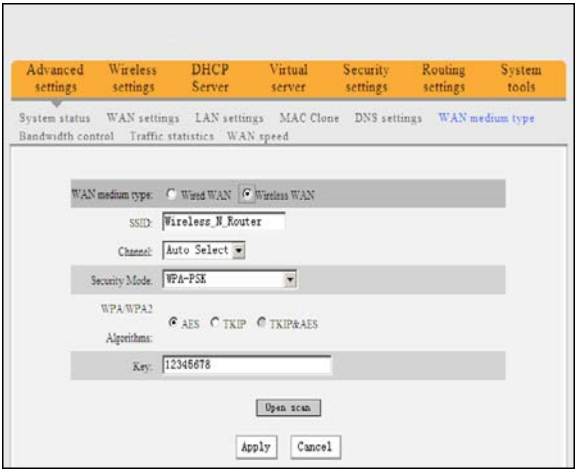
- **Primary DNS address:** Enter the necessary DNS address provided by your ISP.
- **Alternate DNS address:** Enter the secondary DNS address if your ISP provides one (this is optional).

⚠**NOTE:**

After the settings are completed, reboot the router to activate the modified settings.

4.6 WAN Medium Type

Click **Advanced settings > WAN medium type** to configure the type of WAN the router will utilize (wired or wireless).



WAN medium type: ○ Wired WAN ● Wireless WAN

SSID: Wireless_N_Router

Channel: Auto Select

Security Mode: WPA-PSK

WPA/WPA2 Algorithms: ● AES ○ TKIP ○ TKIP&AES

Key: 12345678

- **Wired WAN:** In this mode, the cable is directly connected to the WAN port. Wired WAN is the default mode.
- **Wireless WAN:** Enable this mode if your ISP provides you a wireless connection

service or you want to use the router to expand your wireless signal coverage.

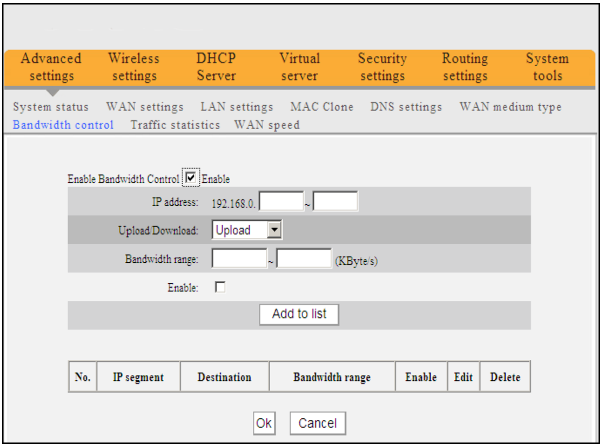
- **SSID:** SSID (Service Set Identifier) is the identity of the wireless device. You can only access the ISP's network by entering the correct SSID of the ISP's wireless device. You can click the **Open scan** button to let the router automatically search for any available SSIDs. The SSID can also be the SSID of the primary wireless device when using the router as a wireless bridge.
- **MAC:** To connect to the ISP's wireless device you need to know the device's MAC address. You can click the **Open scan** button to let the router automatically search for an available MAC address or the primary wireless device's MAC address.
- **Channel:** The wireless device's communication channel. You must select the same channel as the ISP's wireless device to enable communications. It can also be scanned by clicking the **Open scan** button.
- **Security mode**: When the ISP wireless device is secured, the access device should set the same security mode, encryption mode, and key as the ISP's wireless device.

Example:

If your ISP's wireless device's SSID is **Wireless** then just enter **Wireless** into the SSID field, plus the wireless MAC address and channel into the corresponding fields of the above picture. If the ISP device is secured, set your router's encryption type to the same as used by the ISP's device. Alternatively, you can click the **Open scan** button to let the router automatically fill in the SSID, Channel, and wireless MAC. After saving these values, go to the WAN Setting screen to select the corresponding WAN connection type to complete the configuration.

4.7 Bandwidth Control

Bandwidth control is used to limit the communication traffic of LAN computers when accessing the Internet. It can simultaneously control the traffic for a maximum of 254 PCs. Additionally, IP address range configuration is also supported.



Enable Bandwidth Control ☑ Enable

IP address:	192.168.0. ___ ~ ___
Upload/Download:	Upload
Bandwidth range:	___ ~ ___ (KByte/s)
Enable:	□

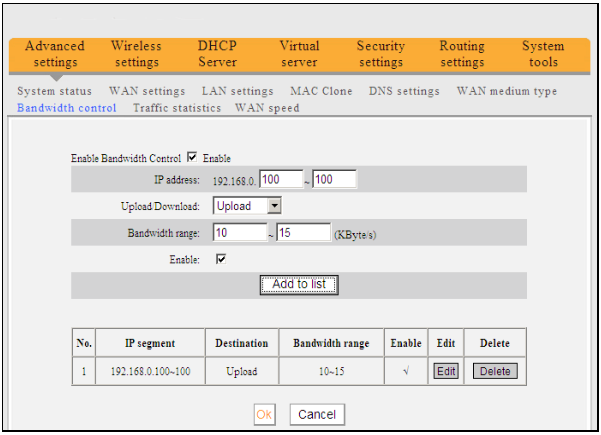
No.	IP segment	Destination	Bandwidth range	Enable	Edit	Delete

- **Enable Bandwidth Control:** Enable or disable the internal IP bandwidth control. The default is disabled.
- **IP Address:** The IP address range of the connected client computers whose traffic you want to control. It can be a single IP address or IP address range.
- **Upload/Download:** Specifies the direction in which traffic is to be controlled for the selected IP addresses, either uploading or downloading.
- **Bandwidth Range:** Specifies the minimum and maximum bandwidth (in KBytes/sec) to allow for use by client computers within the specified IP range. The specified bandwidth cannot exceed the WAN port bandwidth limitation range.
- **Enable:** Enables the rule that is currently being edited. Otherwise, the rule will not go into effect.
- **Add to list:** After you edit the rule, click the **Add to list** button to add the current rule to the rule list. You can have multiple rules that operate simultaneously.

Let's take 2Mbps bandwidth as an example. Theoretically, the fastest downloading rate for 2Mbps bandwidth is 2Mbps / 8 = 256KByte/s, and the fastest uploading speed is 512kbps / 8 = 64KByte/s.

Example 1

If you want to set the maximum download rate of the computer at the IP address 192.168.0.100 to 80-90KByte/s, with a corresponding upload rate of 10-15KByte/s, first add an upload rule as follows:



Enable Bandwidth Control ☑ Enable

IP address: 192.168.0. 100 ~ 100

Upload/Download: Upload

Bandwidth range: 10 ~ 15 (KByte/s)

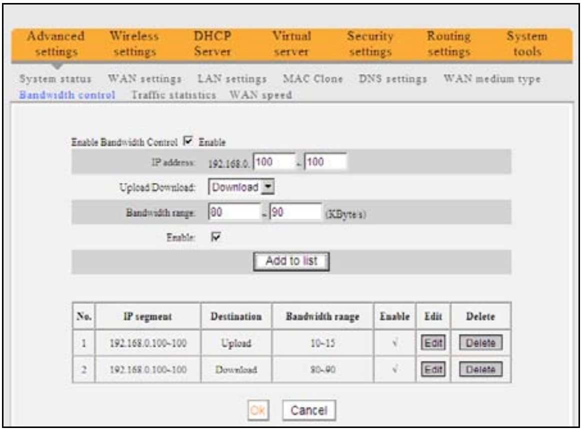
Enable: ☑

No.	IP segment	Destination	Bandwidth range	Enable	Edit	Delete
1	192.168.0.100~100	Upload	10~15	√	Edit	Delete

1. Enter **100** - **100** in the IP address field
2. Select **Upload** in the Upload/Download field.
3. Enter **10** - **15** in the Bandwidth range field
4. Click the box next to the Enable field so that it has a check mark in it.
5. Click the **Add to list** button.
6. Click **Ok** to finish setting the upload rule settings.

Next add a download rule as shown in the following image using the following steps, as illustrated in the next image:

1. Enter **100** - **100** in the IP address field
2. Select **Download** in the Upload/Download field.
3. Enter **80** - **90** in the Bandwidth range field.
4. Click the box next to the Enable field so that it has a check mark in it.
5. Click the **Add to list** button.
6. Click **Ok** to finish setting the upload rule settings.



Enable Bandwidth Control ☑ Enable

IP address: 192.168.0. 100 - 100

Upload Download: Download

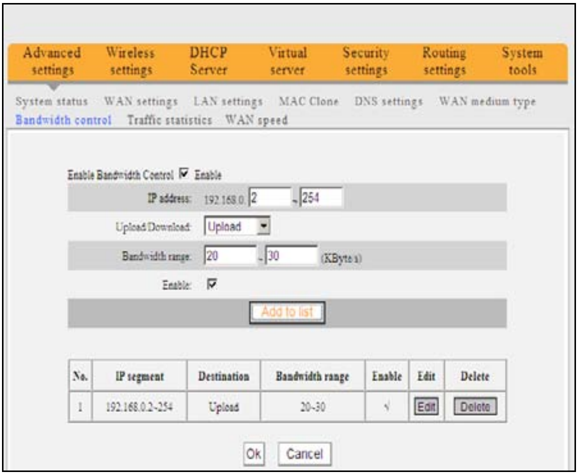
Bandwidth range: 80 - 90 (KByte/s)

Enable: ☑

No.	IP segment	Destination	Bandwidth range	Enable	Edit	Delete
1	192.168.0.100-100	Upload	10-15	√	Edit	Delete
2	192.168.0.100-100	Download	80-90	√	Edit	Delete

Example 2

The following two screen shots depict how to set an upload rate limit of 20-30 KBytes/s and a download rate limit of 100-120 KBytes/s for computers within the IP address range 192.168.0.2 to 192.168.0.254.



Enable Bandwidth Control ☑ Enable

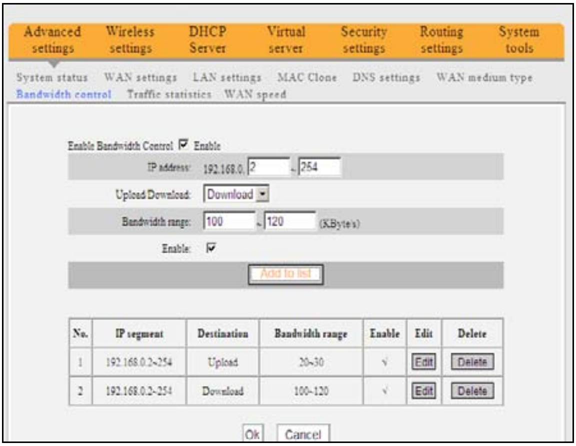
IP address: 192.168.0. 2 - 254

Upload Download: Upload

Bandwidth range: 20 - 30 (KByte/s)

Enable: ☑

No.	IP segment	Destination	Bandwidth range	Enable	Edit	Delete
1	192.168.0.2-254	Upload	20-30	√	Edit	Delete



Enable Bandwidth Control ☑ Enable

IP address: 192.168.0. 2 ~ 254

Upload/Download: Download

Bandwidth range: 100 ~ 120 (KByte/s)

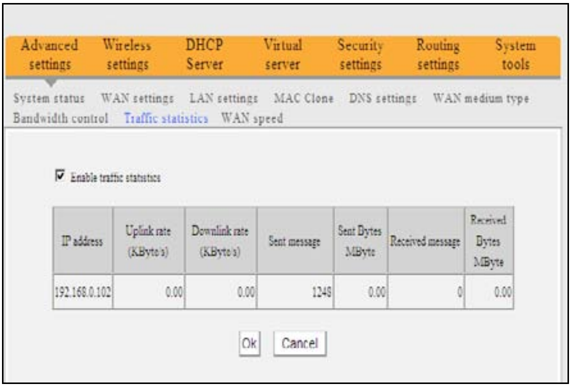
Enable: ☑

No.	IP segment	Destination	Bandwidth range	Enable	Edit	Delete
1	192.168.0.2~254	Upload	20~30	√	Edit	Delete
2	192.168.0.2~254	Download	100~120	√	Edit	Delete

These values are set using the same method as in **Example 1.**

4.8 Traffic Statistics

The Traffic Statistics screen is used to display the bandwidth used by each connected PC.



☑ Enable traffic statistics

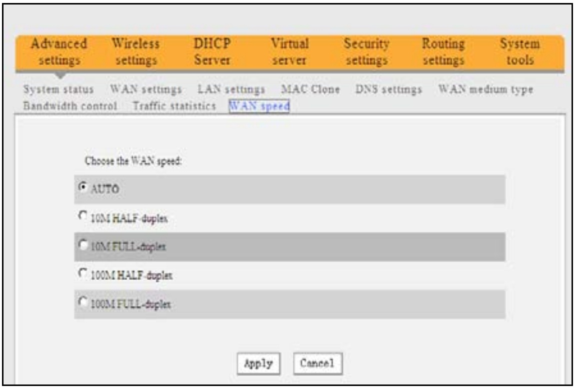
IP address	Uplink rate (KByte/s)	Downlink rate (KByte/s)	Sent message	Sent Bytes MByte	Received message	Received Bytes MByte
192.168.0.102	0.00	0.00	1248	0.00	0	0.00

Enable Traffic statistics: Check this box to allow the router to calculate the traffic used by each computer connected to the LAN. Usually it is best to leave this disabled to improve the router's data packet processing ability, and the default is disabled. Although each computer's traffic is constantly monitored when this function is enabled, the webpage will refresh automatically every five minutes.

- **IP address:** the IP address of the computer whose traffic is being calculated.
- **Uplink rate:** the data sending speed per second in KBytes/s.
- **Downlink rate:** the data receiving speed per second in Kbytes/s.
- **Sent message:** the number of data packets sent out through the router.
- **Sent Bytes:** the total volume of data that is sent out through the router.
- **Received message:** the number of data packets received through the router.
- **Received Bytes:** the total volume of data received through the router.

4.9 WAN Speed

This section allows you to configure the WAN speed. It is recommended that the default settings are retained.



Choose the WAN speed:

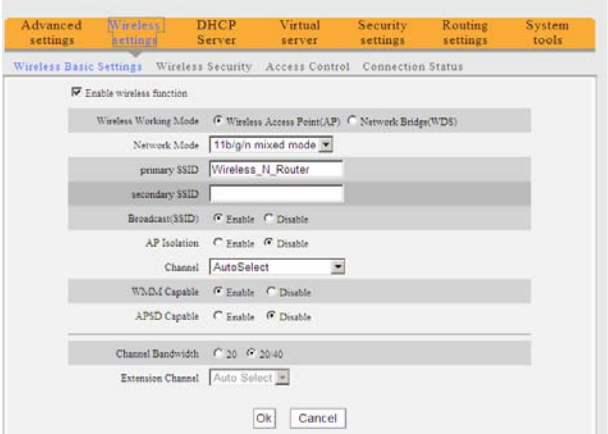
● AUTO
○ 10M HALF-duplex
○ 10M FULL-duplex
○ 100M HALF-duplex
○ 100M FULL-duplex

- **AUTO:** This is the default setting. In this mode, the router will select the best data speed for your network. Keep this selection unless you are experiencing connection and performance issues.
- **10M HALF-duplex:** This is the slowest data rate. Select this value if your router's WAN port does not function properly when connected to an Ethernet cable, which may be caused by degraded performance due to the cable's excessive length.
- **10M FULL-duplex:** Select this value to improve WAN port performance.
- **100M HALF-duplex:** Choose this selection it to set the router's WAN port to work at 100Mbps in half duplex mode.
- **100M FULL-duplex:** This is the fastest data rate. Select this value to force the WAN

port to work at maximum speed. This will result in lost a lost data if an error occurs. It is better to choose the AUTO option so that the router can dynamically react to fluctuations in signal strength and reliability.

Chapter 5 WLAN Settings

5.1 Wireless Basic Settings



☑ Enable wireless function

Wireless Working Mode	● Wireless Access Point(AP) ○ Network Bridge(WDS)
Network Mode	11b/g/n mixed mode
primary SSID	Wireless_N_Router
secondary SSID	
Broadcast(SSID)	● Enable ○ Disable
AP Isolation	○ Enable ● Disable
Channel	AutoSelect
WMM Capable	● Enable ○ Disable
APSD Capable	○ Enable ● Disable
Channel Bandwidth	○ 20 ● 20/40
Extension Channel	Auto Select

- **Enable wireless function:** When selected it enables the router's wireless features. When not selected, all wireless features and functions are disabled.
- **Wireless Working mode:** Select between the two possible wireless modes: **Wireless Access Point (AP)** and **Network Bridge (WDS)**.

Wireless Access Point (AP)

- **Network Mode:** Select one of the modes from the drop-down list:

  11b mode： Use this mode if you have only Wireless-B clients in your network.

  11g mode： Use this mode if you have only Wireless-G clients in your network.

  11b/g mixed mode: Use this mode if you have only Wireless-B and Wireless-G clients in your network.

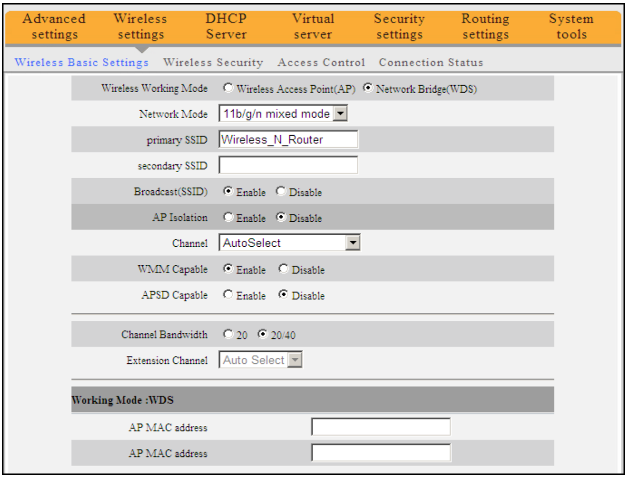
  11b/g/n mixed mode: Use this mode if you have Wireless-B, Wireless-G, and/or Wireless-N clients in your network.
- **Primary SSID:** This is a unique name used to identify the network and is required.
- **Secondary SSID:** This is another unique name, which must be different from the Primary SSID, and which serves as an alternative identifier. The Secondary SSID is optional.
- **Broadcast (SSID):** Select **Enable** to allow the router's SSID to be broadcast, which allows other wireless devices to find it by scanning. When disabled other wireless

devices must be manually configured to use the router's SSID. This is enabled by default.

- **AP Isolation:** This option is disabled by default, and it is recommended that you leave it disabled. When enabled, wireless clients connected via the primary SSID and wireless clients connected via secondary SSID are isolated and cannot communicate with each other. Enable this option only if you want to operate two completely separate wireless LANs, each with their own separate SSID.
- **Channel:** The channel currently used by the router. Select an effective channel, from 1 to 11, or AutoSelect.
- **WMM Capable:** The Wi-Fi MultiMedia mode allows the router to provide a steady bandwidth to high-priority data streams, such as Voice Over IP (VoIP), online gaming, and video streaming, by decreasing bandwidth to low priority streams, such as data downloads and email. This is enabled by default and should remain so to ensure proper QoS (Quality of Service) operation.
- **APSD Capable:** The Automatic Power Save Delivery option is used to put devices into sleep/doze status when not active and is only used with WMM. This is most useful for systems that consist almost entirely of Voice over IP (VoIP) applications. Otherwise it is best to leave this option disabled.
- **Channel bandwidth:** This option sets the appropriate bandwidth for the router and depends on the type of wireless connections in use. If the clients include systems using an 11n connection, select the 20/40M option. If the only clients are using 11b/g connections, then choose the 20M setting.
- **Extension Channel:** This setting determines the wireless channel on which your router will broadcast and receive data. You want to make sure that the router is not using the same channel as any other device in the same frequency range. If a conflict occurs it can cause interference and lost data packets. In most cases, setting this to **Auto Select** will ensure that no conflicts occur.

Network Bridge (WDS) Settings

WDS (Wireless Distribution System) is used to expand the wireless coverage area for an existing network.



Wireless Working Mode ○ Wireless Access Point(AP) ● Network Bridge(WDS)

Network Mode 11b/g/n mixed mode

primary SSID Wireless_N_Router

secondary SSID

Broadcast(SSID) ● Enable ○ Disable

AP Isolation ○ Enable ● Disable

Channel AutoSelect

WMM Capable ● Enable ○ Disable

APSD Capable ○ Enable ● Disable

Channel Bandwidth ○ 20 ● 20/40

Extension Channel Auto Select

Working Mode :WDS

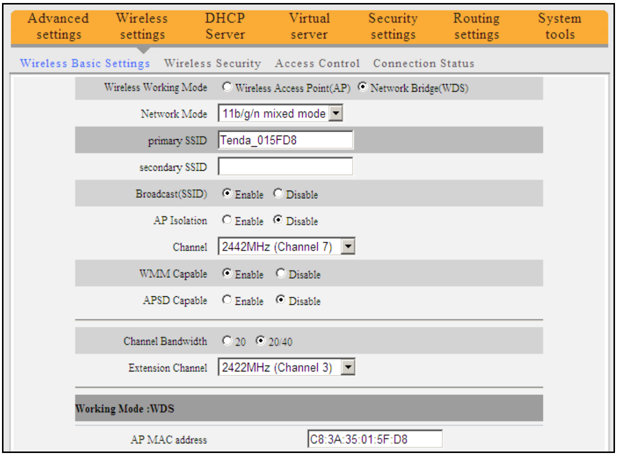
AP MAC address

AP MAC address

- **AP MAC address:** Input the MAC address of another (opposing) wireless router whose coverage you want to expand.

Example: This example bridges two W368R routers.

1. If you know the connecting router's MAC address, enter it into the AP MAC address field and click **Ok**.



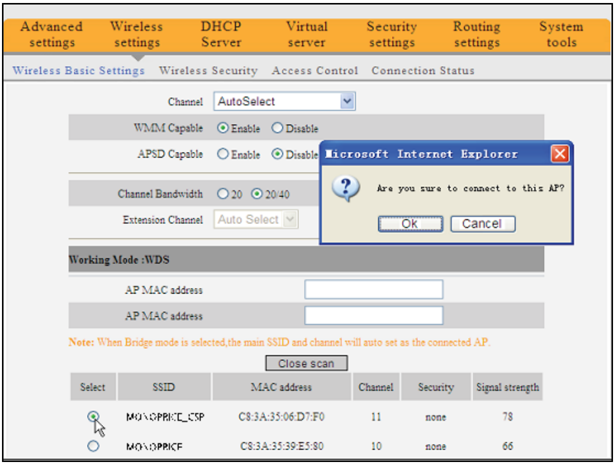
Wireless Working Mode	○ Wireless Access Point(AP) ● Network Bridge(WDS)
Network Mode	11b/g/n mixed mode
primary SSID	Tenda_015FD8
secondary SSID	
Broadcast(SSID)	● Enable ○ Disable
AP Isolation	○ Enable ● Disable
Channel	2442MHz (Channel 7)
WMM Capable	● Enable ○ Disable
APSD Capable	○ Enable ● Disable
Channel Bandwidth	○ 20 ● 20/40
Extension Channel	2422MHz (Channel 3)

Working Mode :WDS

AP MAC address: C8:3A:35:01:5F:D8

2. You can also obtain the MAC address by scanning for the router's signal.

a) Click **Open scan** to get a list of available routers. Select the router you want to connect to and click the **Ok** button on the dialog box. The corresponding wireless MAC address will be added to the AP MAC address field automatically.



Channel: AutoSelect

WMM Capable: ● Enable ○ Disable

APSD Capable: ○ Enable ● Disable

Channel Bandwidth: ○ 20 ● 20/40

Extension Channel: Auto Select

Working Mode :WDS

AP MAC address:

AP MAC address:

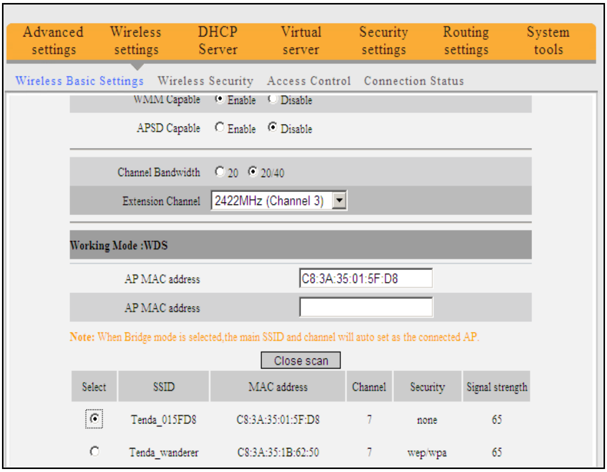
Note: When Bridge mode is selected,the main SSID and channel will auto set as the connected AP.

Microsoft Internet Explorer

Are you sure to connect to this AP?

Select	SSID	MAC address	Channel	Security	Signal strength
●	MONOPRICE_CSP	C8:3A:35:06:D7:F0	11	none	78
○	MONOPRICE	C8:3A:35:39:E5:80	10	none	66

b) After the MAC address is added, click **Ok**.



WMM Capable: ● Enable ○ Disable

APSD Capable: ○ Enable ● Disable

Channel Bandwidth: ○ 20 ● 20/40

Extension Channel: 2422MHz (Channel 3)

Working Mode :WDS

AP MAC address: C8:3A:35:01:5F:D8

AP MAC address:

Note: When Bridge mode is selected,the main SSID and channel will auto set as the connected AP.

Select	SSID	MAC address	Channel	Security	Signal strength
●	Tenda_015FD8	C8:3A:35:01:5F:D8	7	none	65
○	Tenda_wanderer	C8:3A:35:1B:62:50	7	wep/wpa	65

3. After completing the above steps, repeat the process with the other W368R router.

⚠**NOTE**:

The WDS feature requires that both routers support this function and that the SSID,

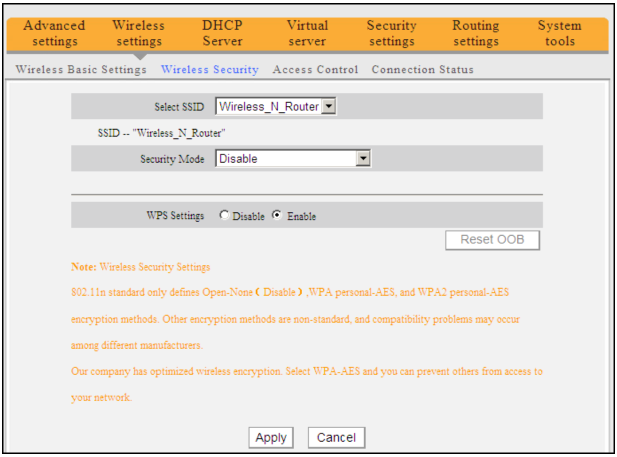
channel, encryption method, and password are the same on each connected router.

5.2 Wireless Security Settings

With the wireless security function, you can prevent others from connecting to your wireless network and using the network resources without your consent. Meanwhile, you can also block illegal users from intercepting or intruding into your wireless network.

5.2.1 WPS Settings

WPS (Wi-Fi Protected Setting) makes it quick and easy to establish a secure connection between the wireless clients and the router. You only need to enter a PIN code or press the WPS button on the back panel of the router to configure it without manually selecting an encryption method or setting a key.



Select SSID: Wireless_N_Router

SSID -- "Wireless_N_Router"

Security Mode: Disable

WPS Settings ○ Disable ● Enable

Note: Wireless Security Settings

802.11n standard only defines Open-None（Disable）,WPA personal-AES, and WPA2 personal-AES encryption methods. Other encryption methods are non-standard, and compatibility problems may occur among different manufacturers.

Our company has optimized wireless encryption. Select WPA-AES and you can prevent others from access to your network.

- **WPS settings**: To enable or disable WPS function. The default is **Enable**.
- **WPS mode:** Selects which of two methods to use: **PBC** (Push-Button Configuration) or **PIN** code.
  - **PBC:** Select **PBC** and click **Ok**, or press and hold the WPS button on the back panel of the device for about one second. The WPS LED indicator will be flashing for 2 minutes, which means the WPS is enabled. During this time (flashing WPS LED), you can enable the wireless client to implement the

WPS/PBC negotiation between them. When the WPS connection is completed, the LED indicator will be continuously lit. To add more clients, repeat the above steps.)

- **PIN:** If this option is enabled, you need to enter a wireless client's PIN code in the field and use the same code for the WPS client.

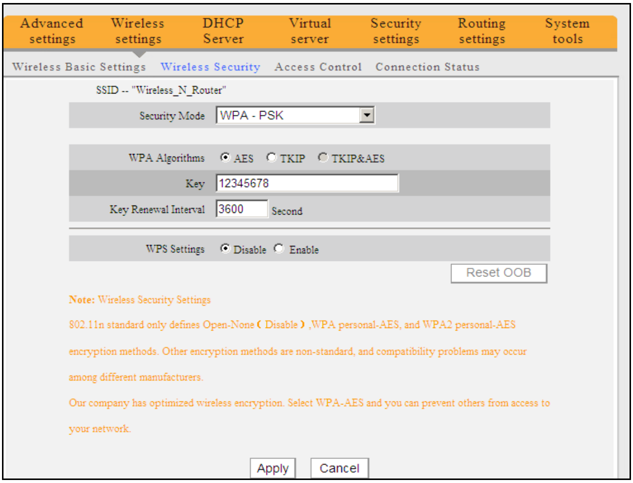
- **Reset OOB:** Press this button, the WPS client will be in an idle state, and the WPS indicator will turn off. The AP will not respond to the WPS client's connection request and will set the security mode as Open-None (Disable) mode.

⚠**NOTE**:

The use of the WPS function requires the use of wireless adapter.

5.2.2 WPA-PSK

The WPA (WiFi Protected Access) method guarantees protection of WLAN users' data and only the authorized network users can access the WLAN.



SSID -- "Wireless_N_Router"

Security Mode: WPA - PSK

WPA Algorithms: ● AES ○ TKIP ○ TKIP&AES

Key: 12345678

Key Renewal Interval: 3600 Second

WPS Settings: ● Disable ○ Enable

Reset OOB

Note: Wireless Security Settings

802.11n standard only defines Open-None (Disable) ,WPA personal-AES, and WPA2 personal-AES encryption methods. Other encryption methods are non-standard, and compatibility problems may occur among different manufacturers.

Our company has optimized wireless encryption. Select WPA-AES and you can prevent others from access to your network.

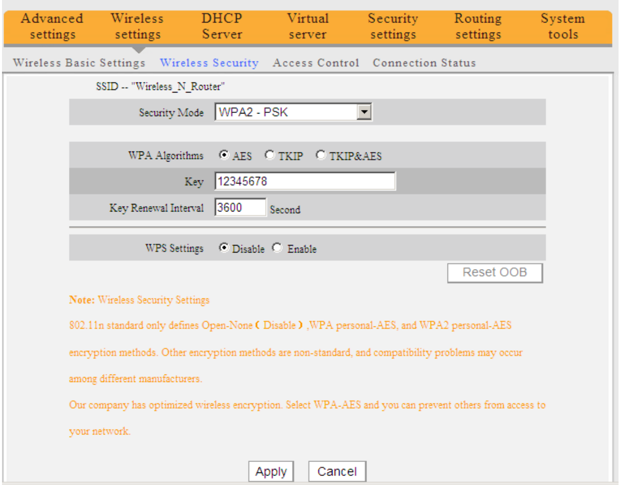
Apply Cancel

- **Security Mode:** Select the proper security mode from the drop-down menu.
- **WPA Algorithms:** Allows the use of TKIP (Temporal Key Integrity Protocol), AES (Advanced Encryption Standard), or both.
- **Key:** Enter a pass phrase that consists of 8-63 ASCII characters.
- **Key Renewal Interval:** Set the key's renewal period, which tells the device how

often it should change the dynamic keys.

5.2.3 WPA2-PSK

WPA2 (Wi-Fi Protected Access version 2) provides even higher security than the use of basic WPA.



SSID -- "Wireless_N_Router"

Security Mode WPA2 - PSK

WPA Algorithms ● AES ○ TKIP ○ TKIP&AES

Key 12345678

Key Renewal Interval 3600 Second

WPS Settings ● Disable ○ Enable

Note: Wireless Security Settings

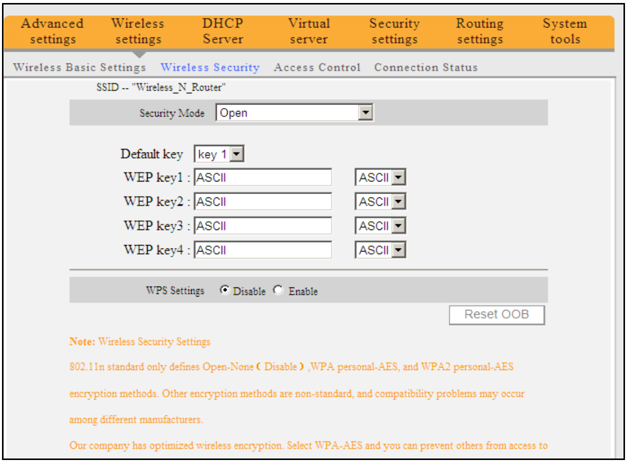
802.11n standard only defines Open-None（Disable）,WPA personal-AES, and WPA2 personal-AES encryption methods. Other encryption methods are non-standard, and compatibility problems may occur among different manufacturers.

Our company has optimized wireless encryption. Select WPA-AES and you can prevent others from access to your network.

- **WPA Algorithms:** Allows the use of TKIP (Temporal Key Integrity Protocol), AES (Advanced Encryption Standard), or both.
- **Key:** Enter a pass phrase that consists of 8-63 ASCII characters.
- **Key Renewal Interval:** Set the key's renewal period, which tells the device how often it should change the dynamic keys.

5.2.4 WEP

The WEP (Wired Equivalent Privacy) is an encryption method that encrypts the data transferred wirelessly between devices to prevent unauthorized users from intercepting or invading the wireless network. WEP security, based on RC4 data encryption technology, provides data confidentiality, integrity, and authentication for wireless communications.



SSID -- "Wireless_N_Router"

Security Mode: Open

Default key: key 1

WEP key1 : ASCII — ASCII

WEP key2 : ASCII — ASCII

WEP key3 : ASCII — ASCII

WEP key4 : ASCII — ASCII

WPS Settings ● Disable ○ Enable

Note: Wireless Security Settings

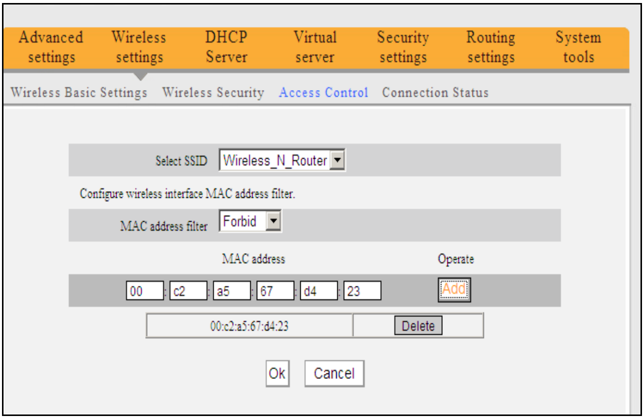
802.11n standard only defines Open-None（Disable）,WPA personal-AES, and WPA2 personal-AES encryption methods. Other encryption methods are non-standard, and compatibility problems may occur among different manufacturers.

Our company has optimized wireless encryption. Select WPA-AES and you can prevent others from access to

- **Security Mode:** Select the corresponding security mode from the drop-down menu. The **Open** option is more secure and is preferred over the **Shared** method.
- **WEP Key1~4:** Set the WEP keys using either ASCII or Hex format. ASCII codes use 5 or 13 ASCII characters (illegal characters such as "/" are not allowed). Hex keys use 10 or 26 hexadecimal characters (0-9 and A-F).
- **Default Key:** Select one of the four preset keys to use as the current default one.

5.3 Wireless Access Control

Wireless access control is based on the MAC address to permit or forbid specific clients' access to the wireless network.



Select SSID: Wireless_N_Router

Configure wireless interface MAC address filter.

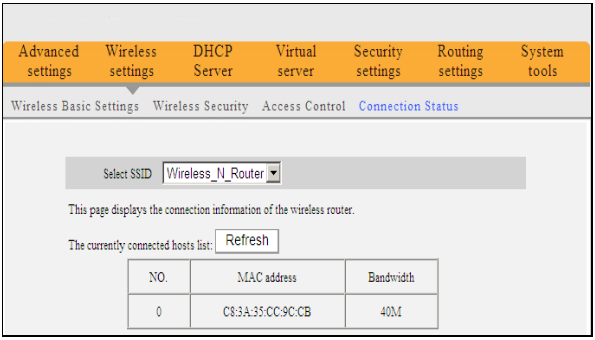
MAC address filter: Forbid

MAC address	Operate
00 : c2 : a5 : 67 : d4 : 23	Add
00:c2:a5:67:d4:23	Delete

- **MAC address filter:** The **Permit** option allows the specified clients in the list access to the wireless network, while the **Forbid** option prevents the specified clients in the list from accessing the wireless network.
- **Configure MAC address:** Input the MAC addresses of the wireless clients to implement the filter policy. Click **Add** to finish the MAC addition operation.
- **MAC Address list:** Displays the filtered MAC addresses. You can add or delete them individually.

5.4 Connection Status

This screen shows the wireless client's connection status, including the MAC address and channel bandwidth.



Select SSID Wireless_N_Router

This page displays the connection information of the wireless router.

The currently connected hosts list: Refresh

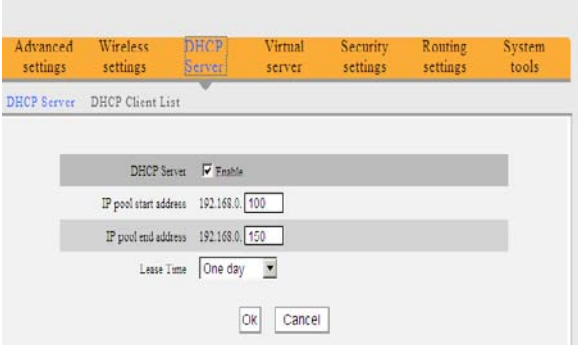
NO.	MAC address	Bandwidth
0	C8:3A:35:CC:9C:CB	40M

- **MAC address:** Shows the MAC addresses of the clients connected to the router.
- **Bandwidth:** Shows the channel bandwidth of the currently connected wireless clients.

Chapter 6 DHCP Server

6.1 DHCP Server

The DHCP (Dynamic Host Control Protocol) is used to assign an IP address to the computers on the LAN/private network. When you enable the DHCP Server, the DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address for the IP Address pool.

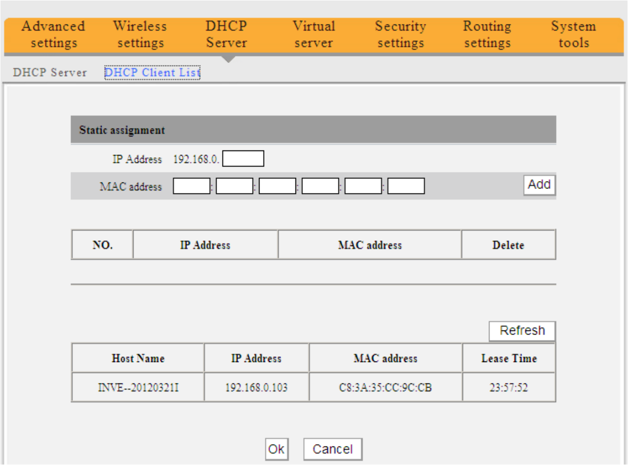


DHCP Server	☑ Enable
IP pool start address	192.168.0.100
IP pool end address	192.168.0.150
Lease Time	One day

- ➢ **DHCP server:** Check the **Enable** box to enable the DHCP server.
- ➢ **IP pool start/end address:** Enter the range of IP addresses for DHCP server distribution.
- ➢ **Lease time:** This indicates the length of time that a dynamic IP address may be assigned to a specific client by the DHCP server. During this time, the server will not attempt to assign the IP address to any other client computer.

6.2 DHCP Client List

The DHCP client list displays client computer IP addresses, MAC addresses, host names, and other information assigned by the DHCP server. You can manually enter the IP and MAC address to convert an IP into a static assignment for the specified client.



Static assignment

IP Address 192.168.0.

MAC address

NO.	IP Address	MAC address	Delete

Host Name	IP Address	MAC address	Lease Time
INVE--20120321I	192.168.0.103	C8:3A:35:CC:9C:CB	23:57:52

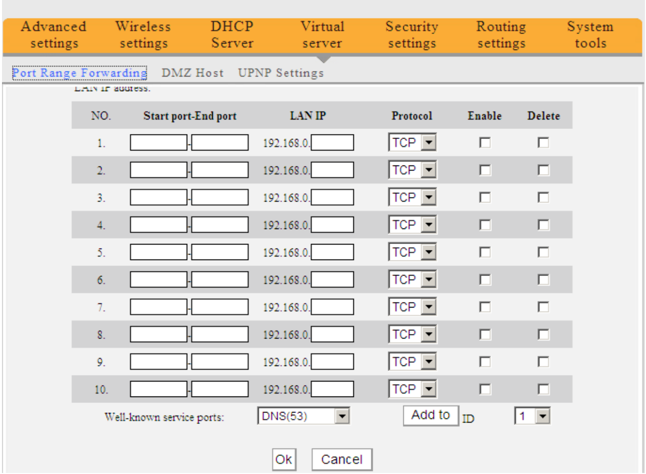
- **IP address:** You can specify an IP address for static binding.
- **MAC address:** Enter the MAC address of the computer you want to give static binding. Click **Add** to add the entry in the list.

- **Host Name:** Displays the name of the computer whose IP is allocated by the DHCP server.
- **IP Address:** Displays the IP address of the client computer.
- **MAC address:** Displays the MAC address of the client computer.
- **Lease time:** Displays the amount of time remaining on the client's IP address lease.

Chapter 7 Virtual Server

7.1 Port Range Forwarding

Port Range Forwarding allows you to specify which IP address is to receive incoming data over specific ports. This is useful when running an application that will receive data from the internet on a specific port, or port range, without having first sent out data to the internet on the same port (e.g., when running a web server, ftp host, etc.



LAN IP address.

NO.	Start port-End port	LAN IP	Protocol	Enable	Delete
1.	-	192.168.0.	TCP	□	□
2.	-	192.168.0.	TCP	□	□
3.	-	192.168.0.	TCP	□	□
4.	-	192.168.0.	TCP	□	□
5.	-	192.168.0.	TCP	□	□
6.	-	192.168.0.	TCP	□	□
7.	-	192.168.0.	TCP	□	□
8.	-	192.168.0.	TCP	□	□
9.	-	192.168.0.	TCP	□	□
10.	-	192.168.0.	TCP	□	□

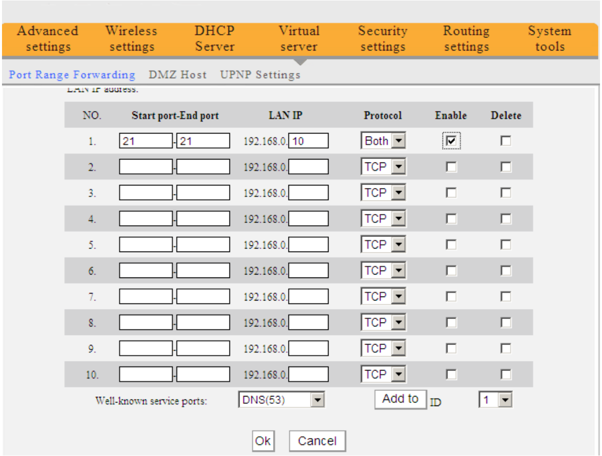
Well-known service ports: DNS(53) Add to ID 1

Ok Cancel

- **Start/End port:** Enter the starting and ending port numbers to be forwarded to the specific client computer.
- **LAN IP:** Enter the IP address of the client computer which will receive the data sent through the specified ports.
- **Protocol:** Select the protocol (TCP, UDP, or Both) for the application. If you are not clear about the protocol that will be used, select **Both**.
- **Enable:** Click the **Enable** checkbox to put the rule into effect.
- **Delete:** Clears all the settings of this line when the **Ok** button is clicked.
- **Well-known service port:** The well-known protocol ports are listed in the drop-down list. Select one and select a sequence number in the ID drop-down list and then click **Add to** and this port will be added automatically to the ID list. For other well known service ports that are not listed, you can manually add them to the list.
- **Add to:** Adds the selected well-known port to the policy ID.

For Example: You want to share some large files with your friends outside of your local area network. However, they are too big, and it's not convenient to physically transfer them. You can build a FTP server on your computer and set the router's port range forwarding to give your friends access to these files on your computer. For the purpose of this example, suppose that your FTP server (or your computer's static IP address) is 192.168.0.10 and you want your friends to access the server through the default port 21 using the TCP protocol. You would then perform the following steps:

1. Enter 21 in both the Start port and End port fields. Alternatively, you can select **FTP** from the well-known service port list and port 21 will be added to the corresponding fields automatically.
2. Enter 192.168.0.10 in the LAN IP column.
3. Select **Both** as the protocol.
4. Check the box under **Enable**.
5. Click the **Ok** button to put the rule into effect.



NO.	Start port-End port		LAN IP	Protocol	Enable	Delete
1.	21	21	192.168.0.10	Both	☑	□
2.			192.168.0.	TCP	□	□
3.			192.168.0.	TCP	□	□
4.			192.168.0.	TCP	□	□
5.			192.168.0.	TCP	□	□
6.			192.168.0.	TCP	□	□
7.			192.168.0.	TCP	□	□
8.			192.168.0.	TCP	□	□
9.			192.168.0.	TCP	□	□
10.			192.168.0.	TCP	□	□

Well-known service ports: DNS(53) Add to ID 1

Now, when your friends want to visit the FTP server, they only need to enter ftp://xxx.xxx.xxx.xxx:21 in the address field. Here, xxx.xxx.xxx.xxx is the router's WAN IP address. For example, when your router's WAN IP address is 172.16.102.89 your friends need to enter **ftp://172.16.102.89:21** in the address field.

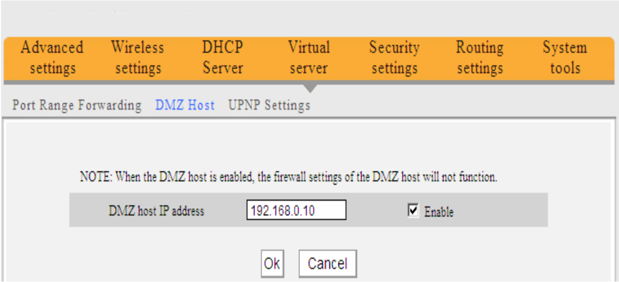
⚠**NOTE:**

If you set the service port of the virtual server to 80, you must set the Web

management port on the Remote Web Management screen to be any value except 80, e.g. 8080. Otherwise, there will be a conflict in disabling the virtual server.

7.2 DMZ Settings

The DMZ Settings screen allows one local computer to be exposed to the Internet for use by a special-purpose service, such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC.



NOTE: When the DMZ host is enabled, the firewall settings of the DMZ host will not function.

DMZ host IP address 192.168.0.10 ☑ Enable

- **DMZ Host IP Address:** The IP address of the client computer on the LAN, which you want to set as the DMZ host.
- **Enable:** Check to enable the DMZ host.

For example:

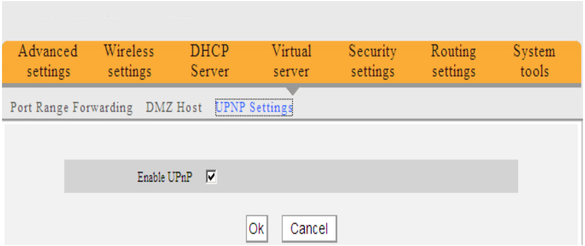
Set the computer at the IP address of 192.168.0.10 as DMZ host to connect to another host on the Internet for intercommunication.

⚠**NOTE:**

When the DMZ host is enabled, the firewall settings of the DMZ host will not function.

7.3 UPNP Settings

With the UPnP (Universal Plug and Play) function, the internal client computer can request the router to process some special port switching, so as to allow an external client to use the resources of the internal host.



Enable UPnP ☑

- **Enable UPnP:** Click the checkbox to enable the UPnP.

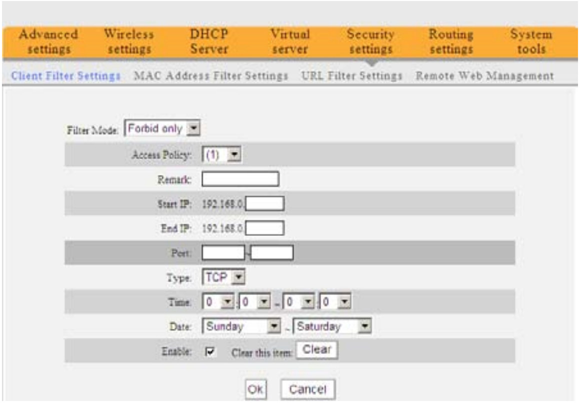
⚠**NOTE**:

This function is enabled with Windows XP, Windows ME, and later, when using Direct-X 9.0 or later. This function is also enabled when using software that supports UPnP.

Chapter 8 Security Settings

8.1 Client Filter Settings

You can enable client filtering to control a client computer's access to specific ports of the internet.



Filter Mode: Forbid only

Access Policy: (1)

Remark:

Start IP: 192.168.0.

End IP: 192.168.0.

Port: -

Type: TCP

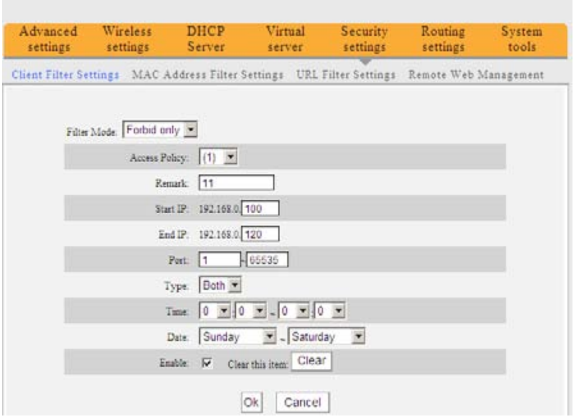
Time: 0 : 0 - 0 : 0

Date: Sunday - Saturday

Enable: ☑ Clear this item:

- ➤ **Filter Mode:** You can select either **Permit only** or **Forbid only**.
- ➤ **Access Policy:** Select an unused number from the drop-down list.
- ➤ **Remark:** Input a simple description of the configured filter rule (you may leave it blank if you wish).
- ➤ **Start/End IP:** Enter the Start IP and End IP address range.
- ➤ **Port:** Enter the range of ports to be controlled. The two values may be the same, indicating a single port rather than a range of ports.
- ➤ **Type:** Select a protocol type (TCP, UDP, or Both) from the drop-down list.
- ➤ **Time:** Select the starting and ending time range for the filter to be in effect.
- ➤ **Date:** Select the starting and ending day(s) to apply the access policy.
- ➤ **Enable:** Check the Enable box to apply the filter after clicking the **Ok** button.

Example 1: Prevent clients at IP addresses between 192.168.0.100 and 192.168.0.120 from accessing the Internet at any time.



Filter Mode: Forbid only

Access Policy: (1)

Remark: 11

Start IP: 192.168.0. 100

End IP: 192.168.0. 120

Port: 1 ~ 65535

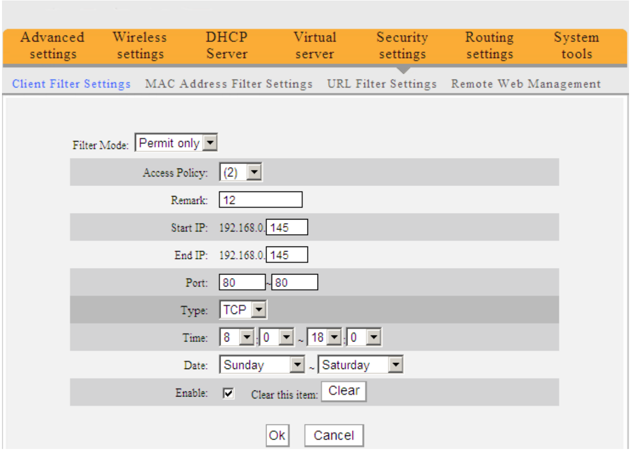
Type: Both

Time: 0 : 0 ~ 0 : 0

Date: Sunday ~ Saturday

Enable: ☑ Clear this item: Clear

Example 2: Allow the computer with the IP address of 192.168.0.145 to access websites only between the hours 8:00 (8 am) and 18:00 (6 pm) on any day of the week.



Filter Mode: Permit only

Access Policy: (2)

Remark: 12

Start IP: 192.168.0. 145

End IP: 192.168.0. 145

Port: 80 ~ 80

Type: TCP

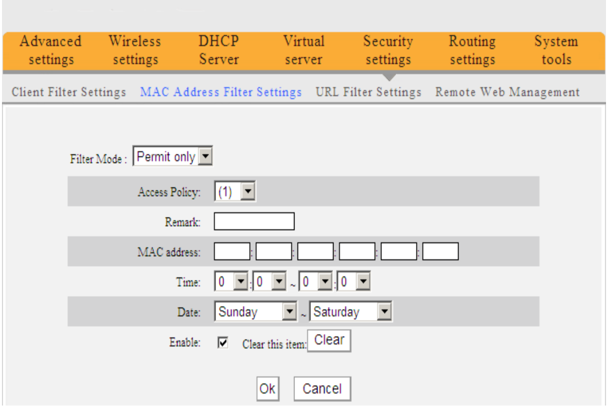
Time: 8 : 0 ~ 18 : 0

Date: Sunday ~ Saturday

Enable: ☑ Clear this item: Clear

8.2 MAC Address Filter

You can also limit the client access to the internet using the MAC Address Filter.



Filter Mode : Permit only

Access Policy: (1)

Remark:

MAC address: _ : _ : _ : _ : _ : _

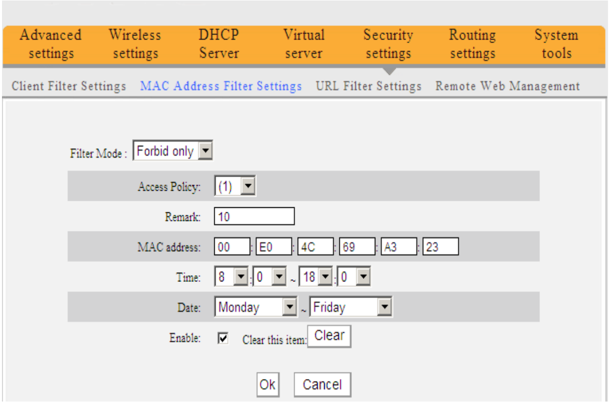
Time: 0 : 0 ~ 0 : 0

Date: Sunday ~ Saturday

Enable: ☑ Clear this item: Clear

- **Filter mode:** You can select either **Permit only** or **Forbid only**.
- **Access Policy:** Select an unused number from the drop-down list.
- **Remark:** Input a simple description of the configured filter rule (you may leave it blank if you wish).
- **MAC Address:** Enter the MAC address of the client to which you want to apply the filter.
- **Time:** Select the starting and ending time range for the filter to be in effect.
- **Date:** Select the starting and ending day(s) to apply the access policy.
- **Enable:** Check the Enable box to apply the filter after clicking the **Ok** button.

Example 1: Prevent the computer with the MAC address of 00:E0:4C:69:A3:23 from accessing the internet between 8:00 (8 am) to 18:00 (6 pm) from Monday to Friday.



Filter Mode : Forbid only

Access Policy: (1)

Remark: 10

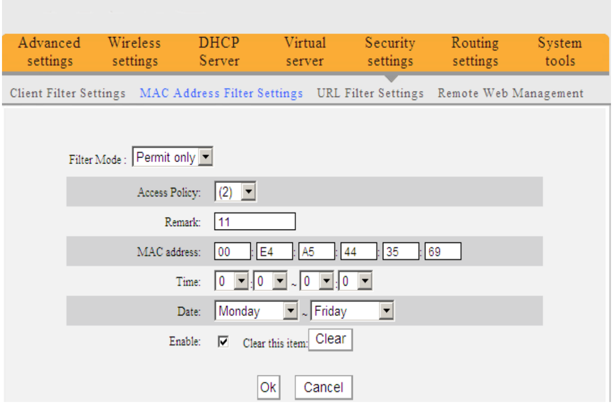
MAC address: 00 : E0 : 4C : 69 : A3 : 23

Time: 8 : 0 ~ 18 : 0

Date: Monday ~ Friday

Enable: ☑ Clear this item:

Example 2: Allow the computer with the MAC address of 00:E4:A5:44:35:69 to access internet at any time of day from Monday to Friday.



Filter Mode : Permit only

Access Policy: (2)

Remark: 11

MAC address: 00 : E4 : A5 : 44 : 35 : 69

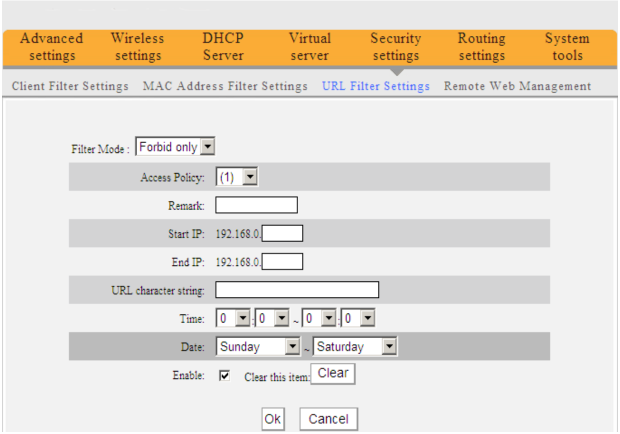
Time: 0 : 0 ~ 0 : 0

Date: Monday ~ Friday

Enable: ☑ Clear this item:

8.3 URL Filter Settings

You can use URL filtering to forbid client access to certain websites at a specified time and/or day of the week.



Filter Mode : Forbid only

Access Policy: (1)

Remark:

Start IP: 192.168.0.

End IP: 192.168.0.

URL character string:

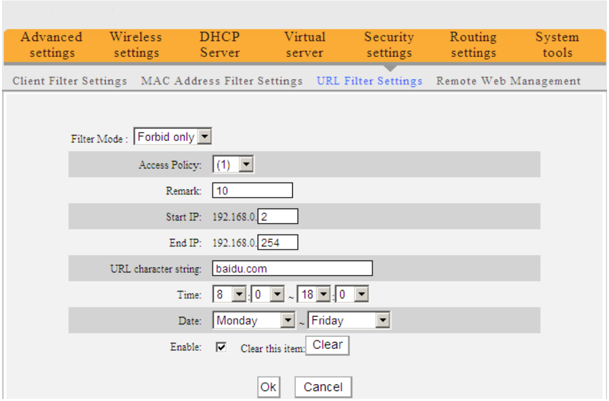
Time: 0 : 0 ~ 0 : 0

Date: Sunday ~ Saturday

Enable: ☑ Clear this item:

- **Filter Mode:** You can select either **Disable** or **Forbid only**.
- **Access Policy:** Select an unused number from the drop-down list.
- **Remark:** A simple description of the configured file. You can also leave it blank.
- **Start/End IP:** Enter the Start IP and End IP address range.
- **URL character string:** Enter text string(s) or keyword(s) that will be filtered.
- **Time:** Select the starting and ending time range for the filter to be in effect.
- **Date:** Select the starting and ending day(s) to apply the access policy.
- **Enable:** Check the Enable box to apply the filter after clicking the **Ok** button.

Example: Prevent all computers on LAN from accessing **baidu.com** between 8:00 (8 am) and 18:00 (6 pm) from Monday to Friday.



Filter Mode : Forbid only

Access Policy: (1)

Remark: 10

Start IP: 192.168.0.2

End IP: 192.168.0.254

URL character string: baidu.com

Time: 8 : 0 ~ 18 : 0

Date: Monday ~ Friday

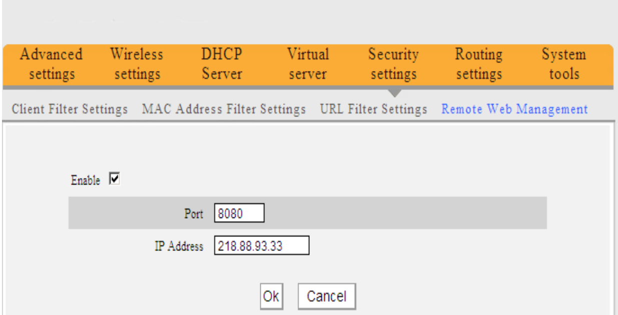
Enable: ☑ Clear this item:

⚠NOTE:

Each access policy can filter only one domain name. So, if you want to filter multiple domain names, you need to set multiple access policies.

8.4 Remote Web Management

This section allows the network administrator to manage the router remotely. If you want to access the router from outside of the local network, click the checkbox after **Enable**.



Enable ☑

Port 8080

IP Address 218.88.93.33

- **Enable:** Check to enable remote web management.
- **Port:** The management port open to outside access. The default value is 80.
- **IP Address:** Specify the range of the IP addresses of the computers on the internet to allow remote management of the router's settings.

⚠**NOTE:**

1. If you want to log in the device's Web-based Utility via port 8080, you need to use the format of WAN IP address:port (for example http://220.135.211.56:8080) to implement remote login.

2. If your WAN IP address starts and ends with 0.0.0.0, it means all computers on the Internet can perform remote web management. If you change the Internet IP address to 218.88.93.33 - 218.88.93.35, then only the computers at the IP addresses of 218.88.93.33, 218.88.93.34 and 218.88.93.35 can access the router to implement remote web management.

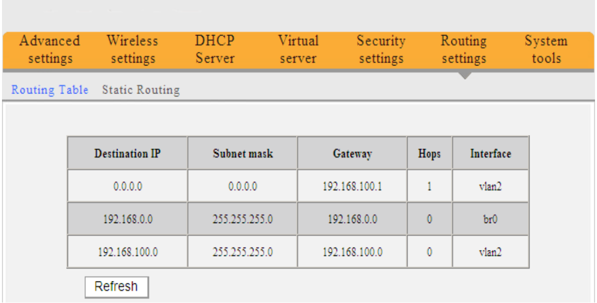
For example:

If you want to allow the computer at the IP address of 218.88.93.33 to access the router's web-based utility via port 8080, please set the parameters as shown in the example screenshot.

Chapter 9 Routing Settings

9.1 Routing Table

This page shows the router's core routing table.

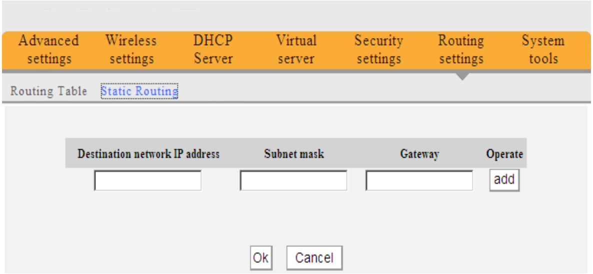


Destination IP	Subnet mask	Gateway	Hops	Interface
0.0.0.0	0.0.0.0	192.168.100.1	1	vlan2
192.168.0.0	255.255.255.0	192.168.0.0	0	br0
192.168.100.0	255.255.255.0	192.168.100.0	0	vlan2

The main duty of a router is to look for the best path for every data packet and transfer that data packet to its destination station. To fulfill this function, many transferring paths, i.e. routing table, are saved in the router, for use when needed.

9.2 Static Routing

This screen is used to set the router's static routing. A static route is a pre-determined pathway that network information must travel to reach a specific host or network.



- **Destination network IP address:** The destination host or IP segment you visit.
- **Subnet mask:** Enter the subnet mask, which is usually 255.255.255.0

- **Gateway:** The entry IP address of the next router.

⚠**NOTE:**

1. The gateway must be at the same net segment with the router's LAN IP.

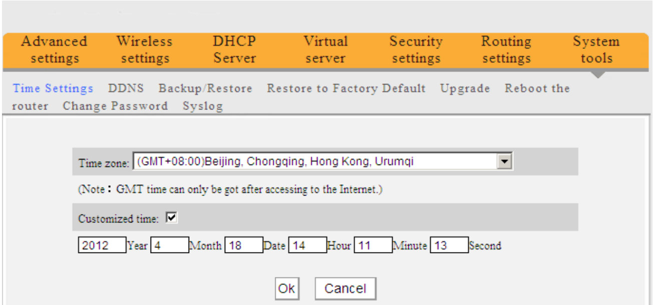
2. If the destination IP address is a client's address, then the subnet mask must be 255.255.255.255.

3. If the destination IP address is an IP segment, then it must match the subnet mask. For example, if the destination IP is 10.0.0.0 then the subnet mask must be 255.0.0.0

Chapter 10 System Tools

10.1 Time Settings

This section is used to the router's internal clock. You can set it manually or obtain the GMT time from the Internet.



Time zone: (GMT+08:00)Beijing, Chongqing, Hong Kong, Urumqi

(Note：GMT time can only be got after accessing to the Internet.)

Customized time: ☑

2012 Year 4 Month 18 Date 14 Hour 11 Minute 13 Second

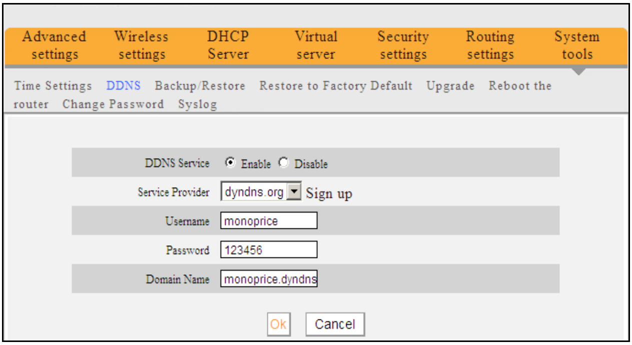
- **Time zone:** Select the time zone in which you are operating the router from the drop-down list.
- **Customized time:** Check this box to enable manual time setting, then enter the date and time in the appropriate fields.

⚠**NOTE:**

When the Router is powered off, the time settings will be lost. The router will obtain the GMT time automatically the next time it accesses the internet. Only when you connect to the internet and obtain the GMT time or set the time on this screen, can the time settings in other functions (e.g. security settings) take effect.

10.2 DDNS

If you want outside users to be able to access your system from the internet, they can do so using either your gateway's router IP address or a Domain Name. However, unless you have a static IP address from your ISP, your IP address will change and the resolution of your Domain Name will be broken. To solve this, you can sign up for a Dynamic Domain Name System, which will ensure that the fixed Domain Name you have selected can always be resolved with whatever IP address is currently assigned to your connection. This router can be setup to communicate with the DDNS server to keep it informed of your current IP address.



DDNS Service ● Enable ○ Disable

Service Provider: dyndns.org ▾ Sign up

Username: monoprice

Password: 123456

Domain Name: monoprice.dyndns

- ➢ **DDNS:** Click the radio button to **Enable** or **Disable** the DDNS service.
- ➢ **Service provider:** Select one of the available service providers from the drop-down list. If you haven't already registered with this service, click **Sign up** for registration.
- ➢ **Username:** Enter the Username for login to the DDNS provider.
- ➢ **Password:** Enter the password for login to the DDNS provider.
- ➢ **Domain name:** Enter the effective registered Domain Name.

For example:

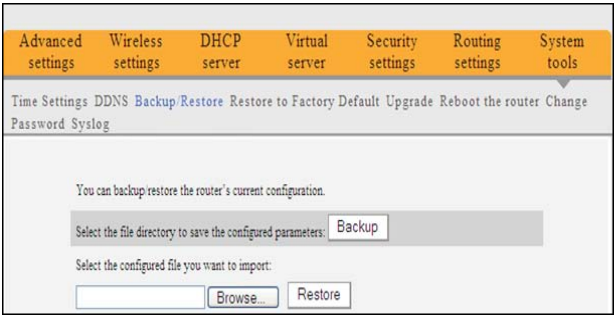
Establish a Web server in the local host 192.168.0.10 and register in dyn.net as follows:

Username	monoprice
Password	123456
Domain Name	monoprice.dyndns.org

After mapping the port in the virtual server, and setting up the account information on the DDNS server, you can then access the web page by entering http://monoprice.dyndns.org in the address field.

10.3 Backup/Restore

This screen allows you to backup the router's current settings or restore any previously saved settings.



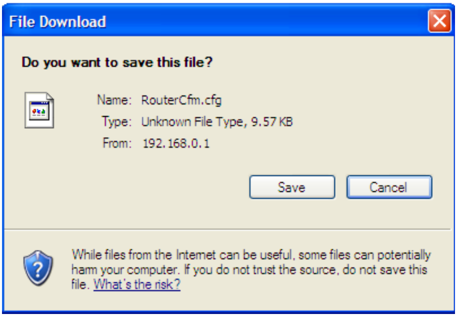
You can backup/restore the router's current configuration.

Select the file directory to save the configured parameters:

Select the configured file you want to import:

- ➢ **Backup Setting:**

Click the **Backup** button to back up the Router's settings. You will be prompted to select a path in which to save the configuration file.



Do you want to save this file?

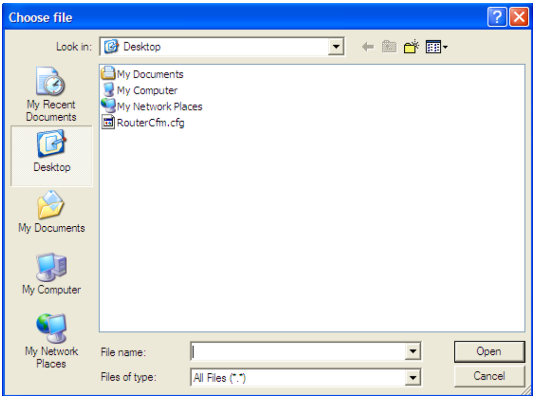
Name: RouterCfm.cfg
Type: Unknown File Type, 9.57 KB
From: 192.168.0.1

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not save this file. What's the risk?

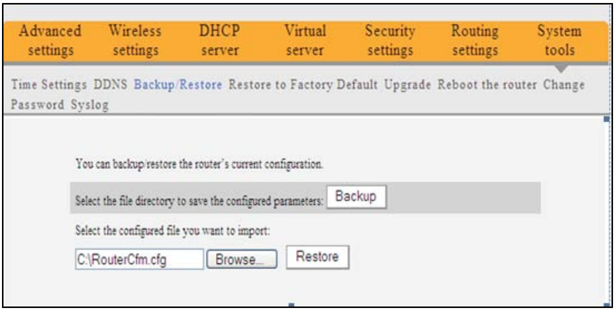
Click the **Save** button to save the configuration files.

- ➢ **Restore Setting:**

Click the **Browse** button to select the configuration file you wish to restore.



Click the "**Restore"** button to restore previous settings.



You can backup/restore the router's current configuration.

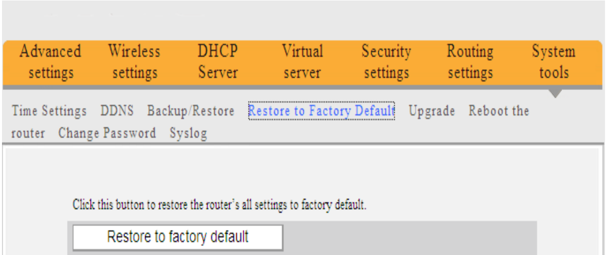
Select the file directory to save the configured parameters:

Select the configured file you want to import:

C:\RouterCfm.cfg

10.4 Restore to Factory Default

This screen allows you to restore all settings to the factory default values.



Advanced settings
Wireless settings
DHCP Server
Virtual server
Security settings
Routing settings
System tools
Time Settings DDNS Backup/Restore Restore to Factory Default Upgrade Reboot the router Change Password Syslog

Click this button to restore the router's all settings to factory default.

Restore to factory default

- **Restore:** Click this button to restore to default settings.
- **Factory default settings:**

  Password: NULL (the default password displays as null)

  IP address: 192.168.0.1

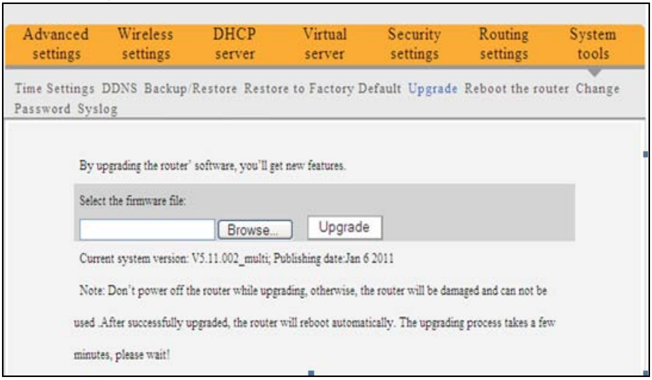
  Subnet mask: 255.255.255.0

⚠NOTE:

After restoring to default settings, please restart the router to make the default settings effective.

10.5 Upgrade

When updated firmware is available, you can upgrade the router's internal software to obtain improved performance and functionality. You can check for firmware updates at the http://www.monoprice.com website.



Advanced settings
Wireless settings
DHCP server
Virtual server
Security settings
Routing settings
System tools
Time Settings DDNS Backup/Restore Restore to Factory Default Upgrade Reboot the router Change Password Syslog

By upgrading the router' software, you'll get new features.

Select the firmware file:

Current system version: V5.11.002_multi; Publishing date:Jan 6 2011

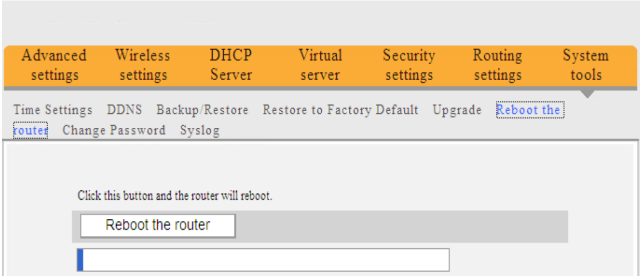
Note: Don't power off the router while upgrading, otherwise, the router will be damaged and can not be used .After successfully upgraded, the router will reboot automatically. The upgrading process takes a few minutes, please wait!

- **Browse:** Click this button to select the upgrade file.
- **Upgrade:** Click this button to start the update process. After the upgrade is

completed, the router will reboot automatically.

10.6 Reboot the Router

Reboot the router to make a configuration take effect. The router will cut its WAN connection automatically after rebooting.



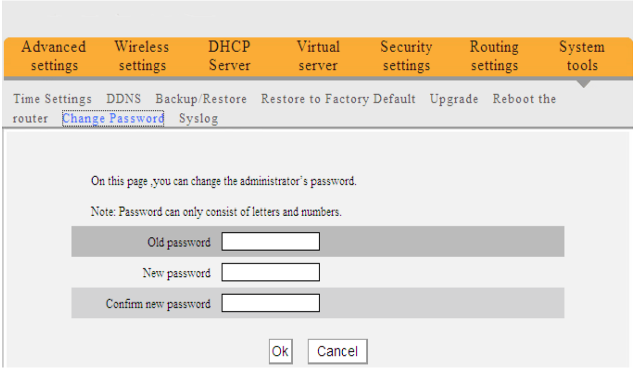
Click this button and the router will reboot.

Reboot the router

- **Reboot the router:** Click this button to reboot the router.

10.7 Password Change

On this screen you can set a new password for the router. Changing passwords periodically is a good security practice.



On this page ,you can change the administrator's password.

Note: Password can only consist of letters and numbers.

Old password	
New password	
Confirm new password	

Ok Cancel

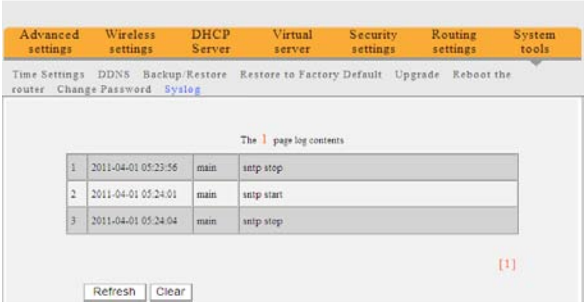
- **Old password:** Enter the old password.
- **New password:** Enter a new password.
- **Confirm new password:** Re-enter to confirm the new password.

⚠**NOTE:**

The default password displays as null, users can log into the web-based utility without any authentication. To secure the router and your network, it is highly recommended that you change the initial password.

10.8 Syslog

This screen allows you to review the system log. You can view various conditions appearing after system start and check to see if there has been an attack on the network. The log can record up to 150 entries.



The 1 page log contents

```
1  2011-04-01 05:23:56  main  sntp stop
2  2011-04-01 05:24:01  main  sntp start
3  2011-04-01 05:24:04  main  sntp stop
```

- **Refresh:** Click this button to update the log.
- **Clear:** Click this button to clear the currently displayed log.

Appendix 1 Glossary

IP: Internet Protocol. An IP address is a numeric identifier assigned to computers on both LANs and WANs. It is used to direct data traffic to the specific computer or LAN.

WAN: Wide Area Network. A WAN is a large network that provides data and intercommunications between multiple smaller LANs. In most cases, the WAN is the internet, though businesses and government institutions often maintain their own private WANs.

LAN: Local Area Network. A LAN is a small network, which accesses a WAN through a Gateway. In most cases, the LAN is the network of computers in your home, which access the internet (WAN) through a router configured as a Gateway.

MAC: Media Access Control. A MAC address is a unique identifier assigned to network interface devices. Each Network Interface Card (NIC), for example, has a unique MAC address. While a computer's IP address may change frequently, its MAC address will remain the same, unless it undergoes a physical change in hardware.

DNS: Domain Name System. The DNS is a system of alphanumeric names to identify locations on the internet, rather than forcing users to use the raw IP address. Since an IP can change, the DNS system allows users to continue to access a particular domain, even if its IP has changed.

Channel: Because many wireless devices use the same frequency a system of channels is used to separate the different transmissions, thereby eliminating interference and crosstalk. This is the same functional concept as the use of channels on a TV to separate the different transmissions coming in over the single RF cable.

SSID: SSID (Service Set Identifier) is the network name shared by all devices in a wireless network. Your network's SSID should be unique to your network and all devices within the network must use the same SSID. It is case-sensitive and limited to a maximum of 20 characters. You may use any of the characters on the keyboard.

DHCP: Dynamic Host Configuration Protocol. The DHCP is a system for configuring computers connected to IP networks. It eliminates much of the manual work that would have to be done by a network administrator. It also maintains a central database of all the devices connected to a network and eliminates duplicate resource assignments.

Appendix 2 Product Features

- Supports IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, IEEE 802.3, and IEEE 802.3u standards.
- High gain omni-directional antenna, with strong signals and long transmission distance.
- Wireless transmission rates up to 150 Mbps or 300 Mbps.
- Provides one 10/100 Mbps auto-negotiation Ethernet WAN port to connect to the Wide Area Network.
- Provides four 10/100 Mbps auto-negotiation Ethernet LAN ports to connect to the Local Area Network.
- Supports Auto MDI/MDIX.
- Supports xDSL/Cable modems with either static or dynamic IPs in a community broadband networking.
- Includes router, wireless access point, four-port switch, and firewall functions.
- Supports WPA-PSK, WPA2-PSK, and WPA-PSK/WPA2-PSK mixed security modes.
- Includes a WPS button to initiate the WPS function.
- Supports hidden SSID function and MAC address-based access control.
- Supports WMM for improved multimedia and VoIP performance.
- Supports SNTP.
- Supports UPnP and DDNS.
- Supports WDS to extend wireless network coverage.
- Supports wireless WAN functionality and allows access to ISP's wireless hotspots to share Internet access with multiple computers.
- Supports virtual server and DMZ hosting.
- Provides a system log to record the important router events.

Appendix 3 FAQ

This section provides some possible solutions to common problems, which may occur during the router's installation or use. The instructions below may help you deal with the problems. If your problem is not in the list, please log into our website www.monoprice.com or send an E-mail to support@monoprice.com, and we will reply to you at the earliest time.

1. I am unable to access the router's Web-based Utility after entering the IP address in the address field of my browser.

Step 1: Check to see if the router is powered on and working correctly. After the device is powered on for a few seconds, the SYS indicator on the front panel should illuminate. If it is not lit, please contact us.
Step 2: Check that the network cables are connected correctly and that the corresponding LED indicator illuminates. Sometimes, the indicator illuminates, but it does not mean it is functioning.
Step 3: Run the "Ping" command and check to see if it can ping the router's LAN IP address 192.168.0.1. To do this, open your system's "Command Prompt" and type **Ping 192.168.0.1** and then press Enter. If the ping is successful, please make sure your browser does not access the Internet through a proxy server. If the ping fails, press the **RESET** button on the router for at least 7 seconds to restore to default settings, then repeat the ping operation. If it still does not work, please contact us.

2. I forgot the login password and cannot enter the Web-based Utility.
Press the **RESET** button for at least 7 seconds to restore the router to its default settings.

3. The computer connected with the router shows IP address conflict.
Check if there are other DHCP servers in the LAN. If so, disable them. The default IP address of the router is 192.168.0.1, so make sure the address is not being used by any other device. If there are two computers with the same IP address, change one of them.

4. I cannot use E-mail and access the Internet.
This sometimes happens with ADSL connections and Dynamic IP users. You may need to modify the default MTU value (1492). To do this, open the **WAN Setting** screen and modify the MTU value to a recommended value, such as 1450 or 1400.

5.How can I share my computer's resource with other users on the internet?
If you want Internet users to access the internal server via the router, such as an e-mail server, Web server, FTP server, etc., you can configure a **Virtual Server**, as follows:
Step 1: Create your internal server. Make sure the LAN users can access these servers and that you know the related service port. For example, a web server's port is 80, FTP is 21, SMTP is 25, and POP3 is 110.
Step 2: In the router's web utility, click **Virtual Server** and select **Port Range Forwarding**.
Step 3: Input the service port used by the application (i.e. the external port) for mapping the internal and external network, for example 80 for a web server. Input the same value for both the **Start port** and **End port** fields
Step 4: Input the internal server's IP address. For example, if your Web server's IP address

is 192.168.0.10, input 10 in the IP address field.

Step 5: Select the communication protocol used by your internal host: TCP, UDP, or Both.

Step 7: Click **Ok** to activate the settings.

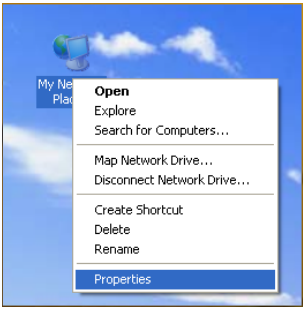
The following table lists some well-known applications and their respective service ports:

Server	Protocol	Service Port
WEB Server	TCP	80
FTP Server	TCP	21
Telnet	TCP	23
NetMeeting	TCP	1503, 1720
MSN Messenger	TCP/UDP	File Send: 6891-6900 (TCP) Voice: 1863, 6901 (TCP) Voice: 1863, 5190 (UDP)
PPTP VPN	TCP	1723
Vonage VoIP	TCP	5060-5070 10000-25000
SMTP	TCP	25
POP3	TCP	110

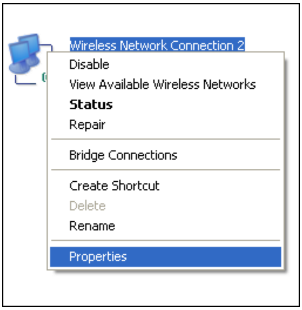
Appendix 4 Deleting the Wireless Configuration File

Deleting the wireless configuration file under Windows XP:

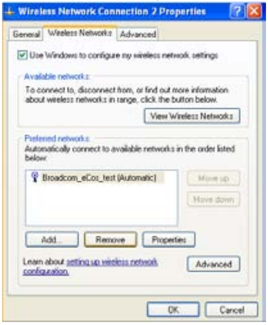
1. Right click **My Network Places** on your computer's desktop and select **Properties**.



2. Right click **Wireless Network Connections** and select **Properties**.



3. Click **Wireless Networks**, select the network configuration in **Preferred networks**, then click the **Remove** button, as shown in the example below.



☑ Use Windows to configure my wireless network settings

Available networks:

To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

Preferred networks:

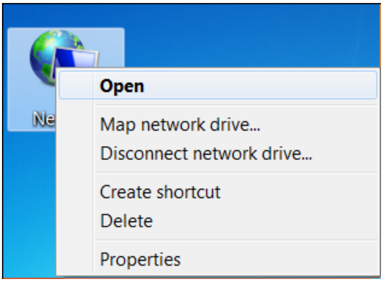
Automatically connect to available networks in the order listed below:

Broadcom_eCos_test (Automatic)

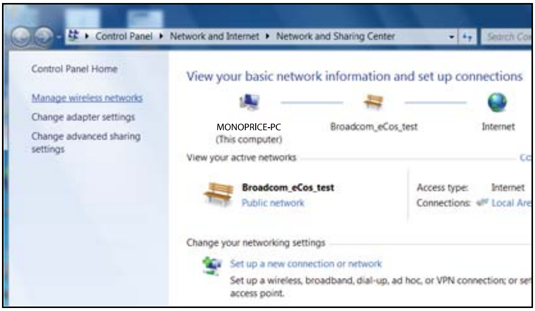
Learn about setting up wireless network configuration.

Deleting the wireless configuration file under windows 7

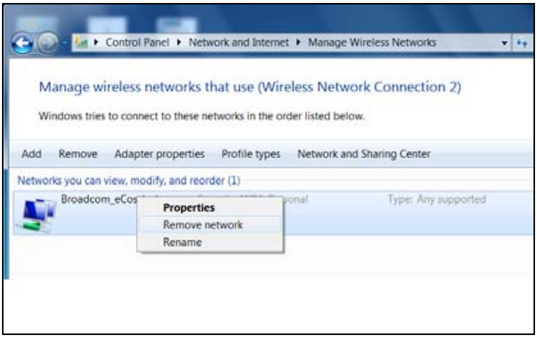
1. Right click **Network** and click **Properties**.



2. Click **Manage wireless networks** on the left side of the window.


Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search Co
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
MONOPRICE-PC
(This computer)
Broadcom_eCos_test
Internet
View your active networks
Broadcom_eCos_test
Public network
Access type: Internet
Connections: Local Are
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or se
access point.

3. Select the corresponding configuration file, right click it, then select **Remove network** in the pop-up menu.


Control Panel ▸ Network and Internet ▸ Manage Wireless Networks
Manage wireless networks that use (Wireless Network Connection 2)
Windows tries to connect to these networks in the order listed below.
Add
Remove
Adapter properties
Profile types
Network and Sharing Center
Networks you can view, modify, and reorder (1)
Broadcom_eCos
onal
Type: Any supported
Properties
Remove network
Rename

Appendix 5 Regulatory Information

EU Declaration or Declaration of Conformity

Hereby, Monoprice declares that this Wireless Broadband Router is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

FCC Statement

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

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

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example: use only shielded interface cables when connecting to computer or peripheral devices).

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with the minimum distance of 20 cm. Operation is subject to the following two conditions:

1) This device may not cause interference, and
2) This device must accept any interference, including interference that may cause undesired operation of the device.

Caution!

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user authority to operate the equipment.