iball Baton®

150M Wireless-N Broadband Router

Model No.: iB-WRB150N

User Manual

Ver.: 1.0.0

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 pro-vide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not in-stalled 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.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference.

2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

CE Mark Warning

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Table of Contents

Table of Contents **3**

Chapter 1 Product Overview **5**

1.1 Package Contents 5
1.2 Panel Overview 6

Chapter 2 Installation **8**

Chapter 3 Internet Connection Setup **10**

3.1 Configure your PC's TCP/IP Settings 10
3.2 Login to Router 15
3.3 Quick Internet Connection Setup 16
3.4 Quick Encryption 17

Chapter 4 Network Settings **18**

4.1 Status Info 18
4.2 WAN 19
4.2.1 PPPoE 19
4.2.2 Static IP 21
4.2.3 Dynamic IP 21
4.3 LAN 24
4.4 MAC Clone 25
4.5 DNS 26
4.6 Bandwidth Control 27
4.7 Traffic Statistics 29
4.9 WAN Speed 30

Chapter 5 Wireless Settings **32**

5.1 Wireless Basic Settings 32
5.2 Wireless Security 37
5.2.1 WPS Settings 37
5.2.2 WPA-PSK 38
5.2.3 WPA2-PSK 39
5.2.4 WEP 39
5.3 MAC Filtering 39
5.4 Connection Status 42

Chapter 6 DHCP **43**

6.1 DHCP Settings 43
6.2 DHCP Clients & Address Reservation 44

Chapter 7 Virtual Server 45

7.1 Port Forwarding 45
7.2 DMZ.....47
7.3 UPnP 48

Chapter 8 Security Settings 49

8.1 IP Address Filtering 49
8.2 MAC Address Filtering.....50
8.3 URL Filtering 53
8.4 Remote Management.....54

Chapter 9 Routing Settings 56

9.1 Routing Table 56
9.2 Static Routing.....56

Chapter 10 Maintenance.....58

10.1 Time Settings 58
10.2 DDNS 58
10.3 Backup/Restore 60
10.4 Factory Default.....61
10.5 Firmware Upgrade 62
10.6 Restart 62
10.7 Password 63
10.8 SysLog.....64

Appendix 1: Glossary 65

Appendix 2: Features..... Error! Bookmark not defined.

Appendix 3: Troubleshooting..... 66

Appendix 4: Contact Information..... Error! Bookmark not defined.

Chapter 1 Product Overview

iBall Baton 150M Wireless-N Broadband Router complies with IEEE 802.11 b/g/n wireless standards.

Enhanced Wireless Transmission speed up to 150Mbps

Integrates 4- 10/100Mbps LAN ports & 1 - WAN port.

With Firewall security features as IP/MAC Filter and URL Filtering, NAT-Router and Wireless AP

Package Contents

The following items should be found in your package:

- 150M Wireless-N Broadband Router
- DC Power Adapter
- RJ45 Patch Cord
- Resource CD for 150M Wireless-N Router, including:
  Easy Setup Wizard, Other Helpful Information

Product Feature:

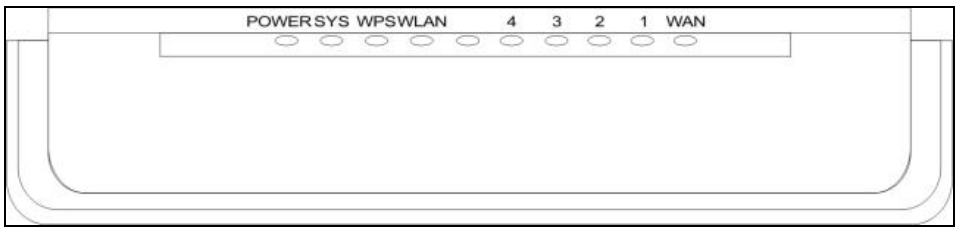
- Complies with IEEE802.11b/g/n, IEEE802.3 & IEEE802.3u standards
- 4 -10/100M LAN ports, 1- WAN port & Wireless-N AP
- Operation Mode: AP Router / WDS
- Broadband Internet: PPPoE, Static IP, Dynamic IP connection type
- With Security feature such as IP, MAC and domain filtering
- With WEP, WPA-PSK, WPA2-PSK encryption security
- Built-in NAT, DHCP Server , Virtual server, DMZ and UPnP
- Web-based management
- 5dBi Omni-Directional Antenna
- Power Adapter: 9V DC, 0.6A

Conventions

The Router or iB-WRB150N mentioned in this guide stands for iBall Baton 150M Wireless-N Broadband Router without any explanation.

1.2 Panel Overview

LED overview:



LED	Status	Colour	Description
PWR	Blinking	Orange Led	Router is ON & functioning properly
SYS	Flashing	Green Led	Indicates as functioning properly
WPS	Blinking	Green Led	System is functioning properly
WLAN	Blinking	Orange Led	System is functioning properly
LAN	Blinking	Green Led	System is functioning properly
WAN	Blinking	Orange Led	System is functioning properly

Port/Button Overview：

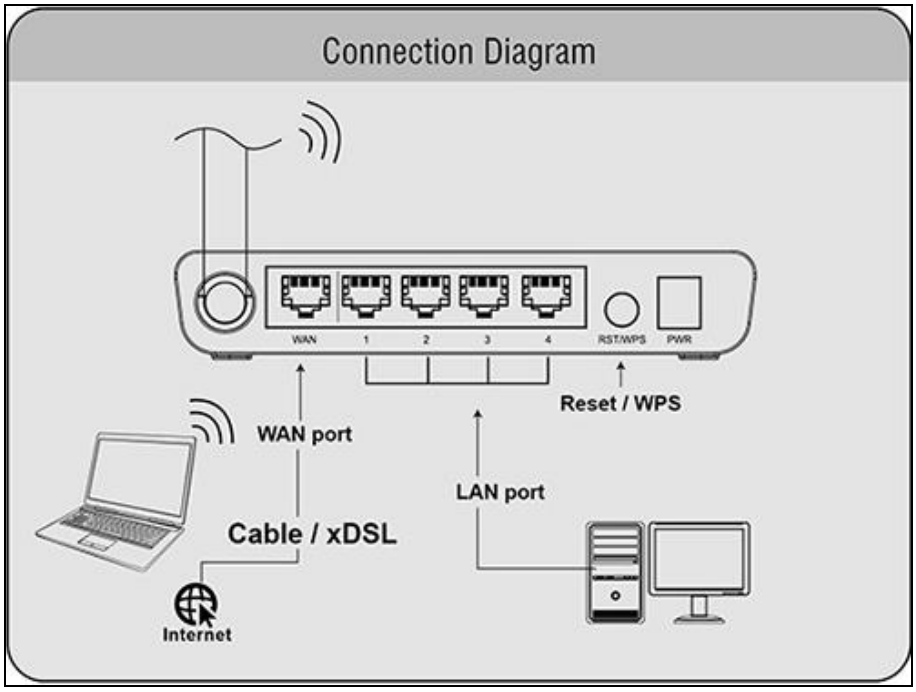
Port/Button	Description
WAN	Internet port connecting to a DSL/Cable modem or ISP directly.
LAN	For connection to a computer or router.
RESET	Pressing this button for 7 seconds restores the device to factory default settings.
PWR	Power Adapter. Do not use a different power adapter than the included one.

Chapter 2 Installation

1. Connect one end of the included power adapter to the router and then plug the other end into a wall outlet nearby.

2. Connect the LAN port on the Router to the NIC port on your PC using an Ethernet cable.

3. Connect the WAN port on the Router to an Internet-enabled Cable/xDSL modem using an Ethernet cable.



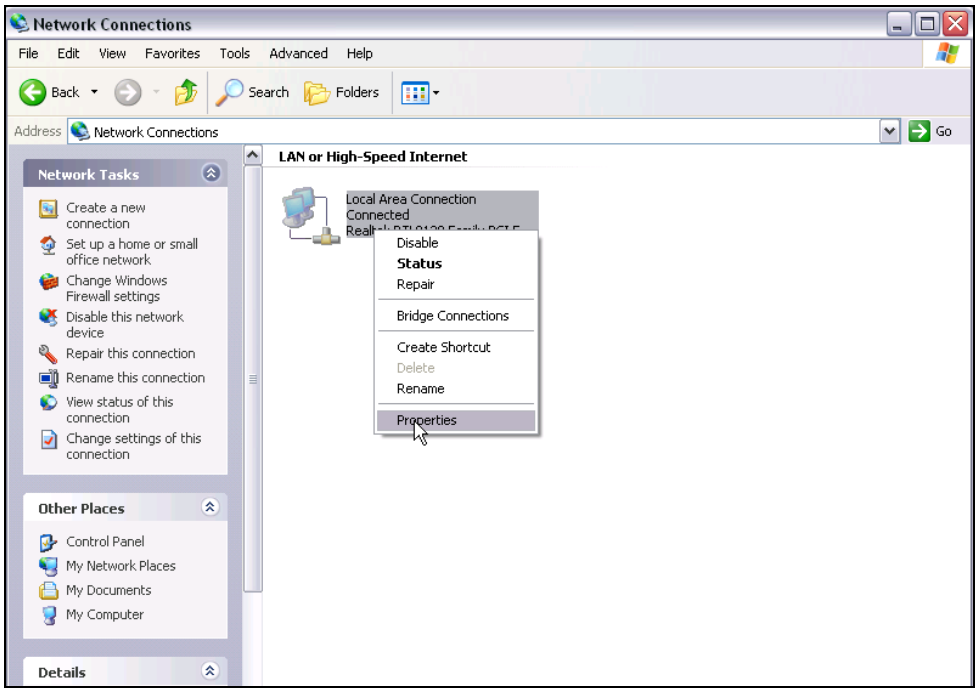
4. Insert the included “Easy Setup Wizard” CD-ROM into your PC’s drive, click “Setup. exe” if the program does not run automatically and follow onscreen instructions to complete settings. Or directly launch a web browser and configure the router on web based utility (For details, refer to chapter 3).

Chapter 3 Internet Connection Setup

3.1 Configure your PC's TCP/IP Settings

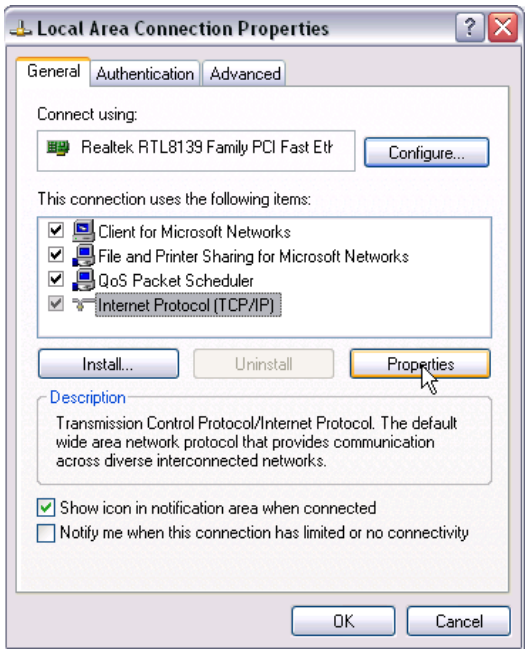
If you are using Windows XP operating system, do as follows.
1. Right click "My Network Places" and select "Properties".

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



3. Select "Internet Protocol (TCP/IP)" on the appearing window and

click “Properties” button.



4. Select “Use the following IP address”

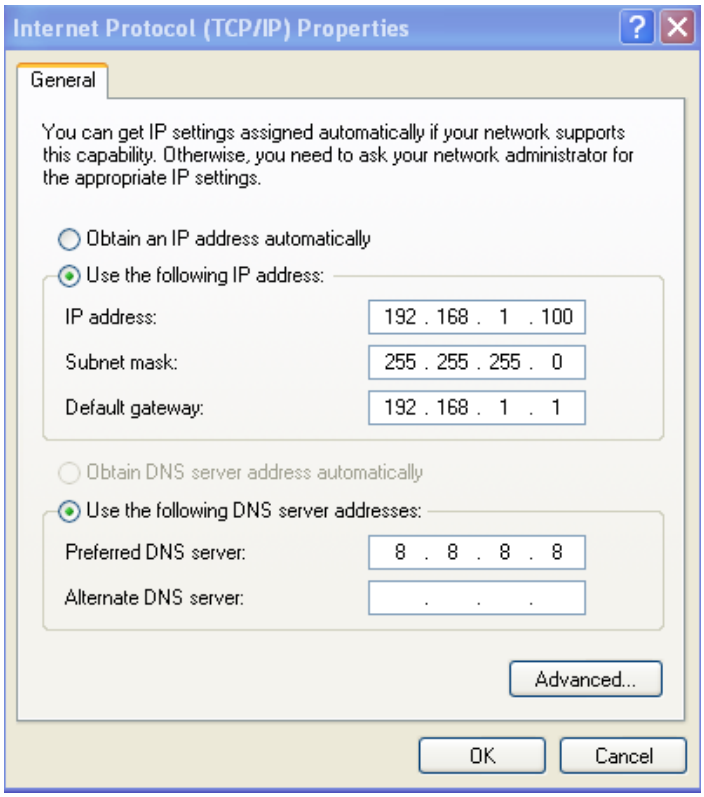
● **IP address**: Enter 192.168.1.xxx (xxx can be any value from 2~254).

● **Subnet mask**: Enter 255.255.255.0.

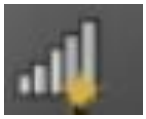
● **Default gateway**: Enter 192.168.1.1.

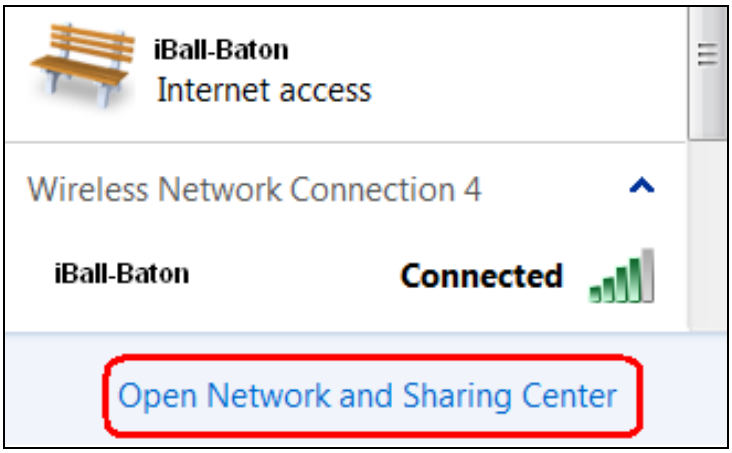
● **Preferred DNS server**: Enter 192.168.1.1 in case that you don’t know the local DNS server address (Or contact your ISP for help).

At last, click OK to save your settings.

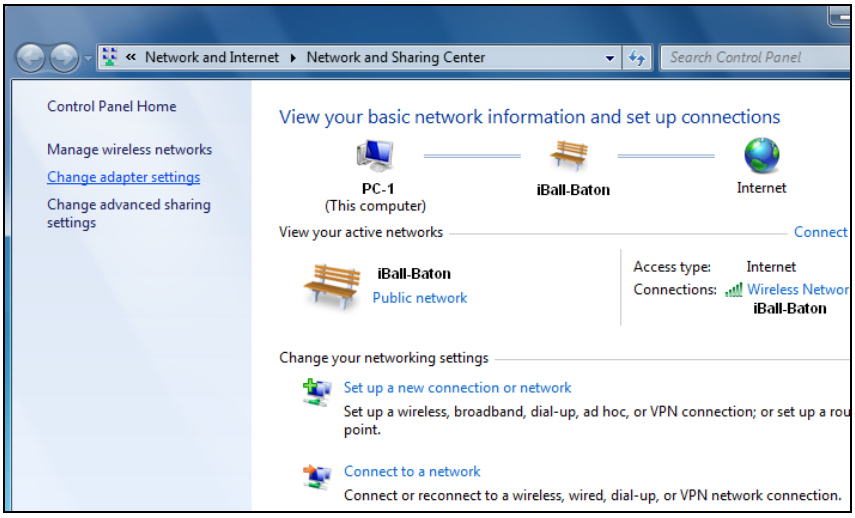


If you are using Windows 7 operating system, do as follows:

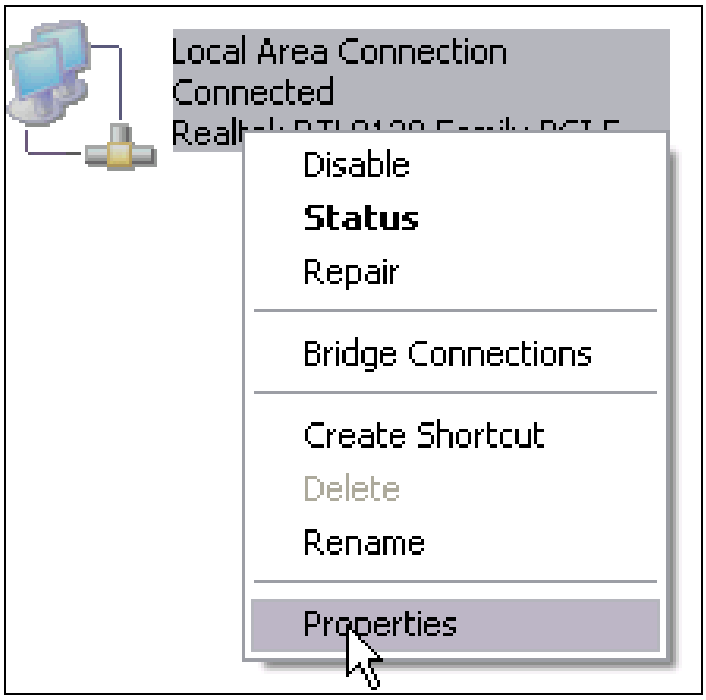
1. Right click network icon  on your desktop and then click the "Open Network and Sharing Center".



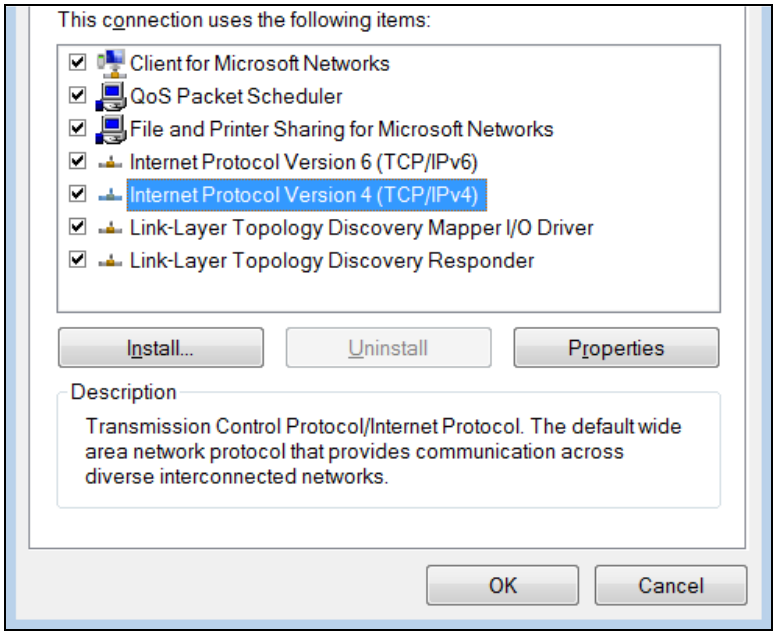
2. Click “Change adapter settings”.



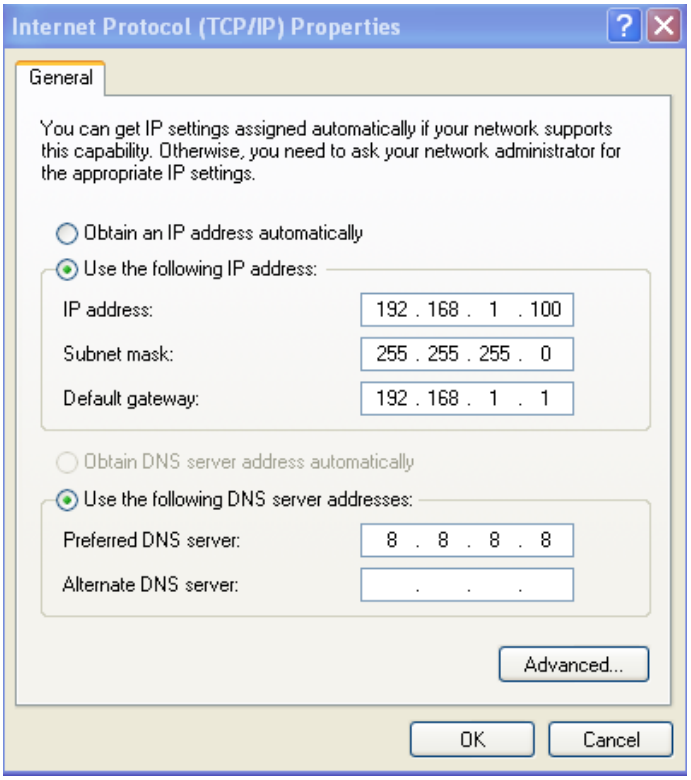
3. Right click “Local Area Connection” and select “Properties””



4. Select “Internet Protocol (TCP/IP)” on the appearing window and click “Properties” button.



5. Select “Use the following IP address”



- **IP address**: Enter 192.168.1.xxx (xxx can be any value from 2~254).
- **Subnet mask**: Enter 255.255.255.0.
- **Default gateway**: Enter 192.168.1.1.
- **Preferred DNS server**: Enter 192.168.1.1 in case that you don't know the local DNS server address (Or contact your ISP for help).

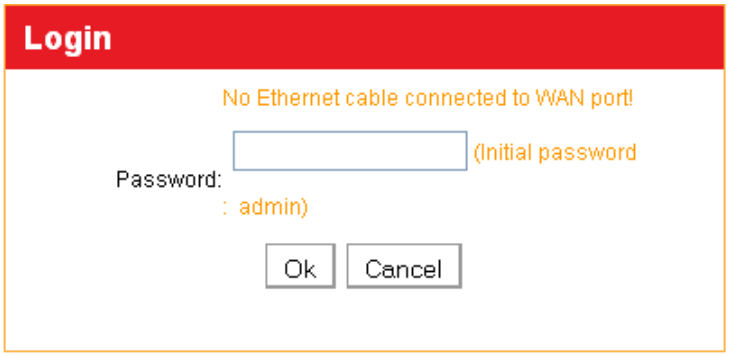
At last, click OK to save your settings.

3.2 Login to Router

1. With a Web-based utility, it is easy to configure and manage the iB-WRB150N 150Mbps Wireless -N Router.

To access the configuration utility, open a web-browser and type in the default address http:// 192.168.1.1 in the address bar

1. 



Type password "**admin**" and then click ok to go to interface below:

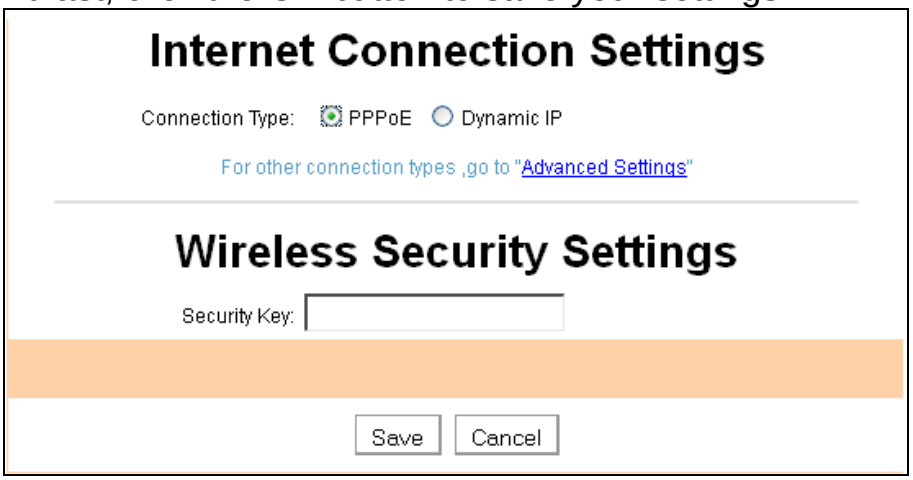
Note: Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser, such as Microsoft Internet Explorer 8.0 / 9.0 (Suggested) & Mozilla Firefox.

3.3 Quick Internet Connection Setup

There are 2 Internet connection types on this screen, ADSL dialup (PPPoE) and Dynamic IP (DHCP).

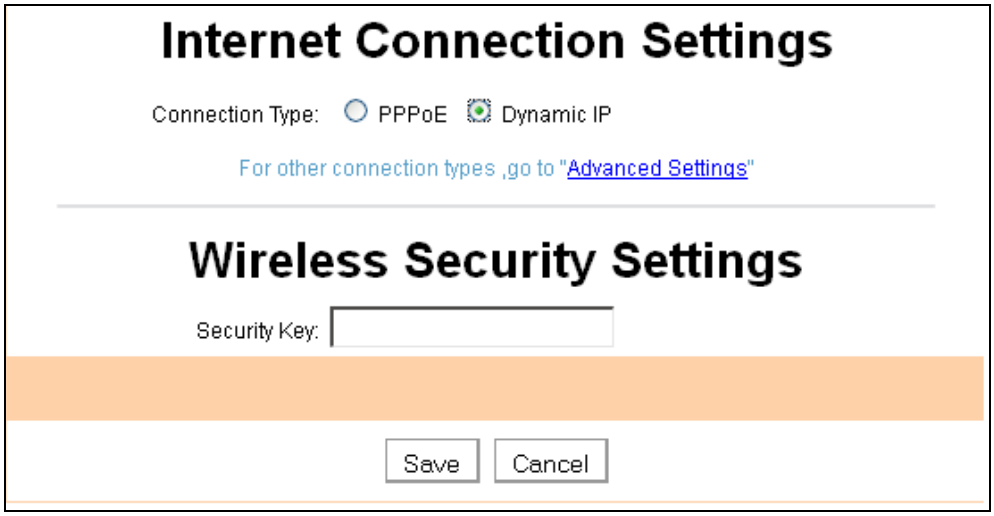
PPPoE

Select PPPoE, if your ISP are using a PPPoE connection and enter the PPPoE user name and password provided by your ISP. Then setup a wireless security key on the interface below to secure your wireless network. At last, click the OK button to save your settings.



Dynamic IP

Select Dynamic IP as per your ISP details provided.
We recommend you to setup a wireless security key on this interface to protect your wireless network from undesired access.
Then click the OK button to save your settings.



● The default Internet connection type is PPPoE. Contact your ISP if you are not clear about the PPPoE user name and password.

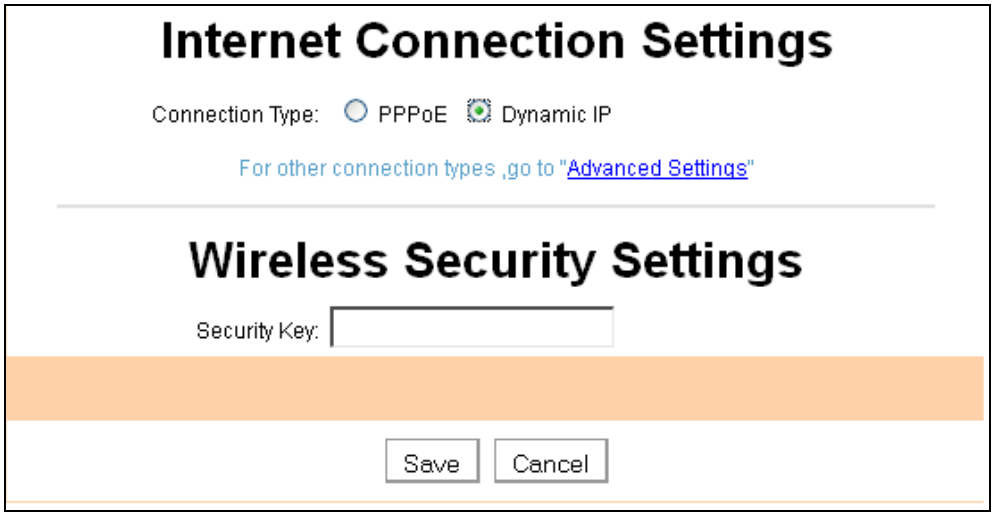
● Go to Chapter4 > WAN Settings, if you are using an Internet connection type other than the above- mentioned.

3.4 Quick Wizard

Click the quick wizard to configure the quickly the WAN settings & Wireless key.

- WAN Setup > you can configure PPPoE or Dynamic IP settings (Check for more settings as provided from ISP)

- Wireless > you can configure the WPA2-PSK Wireless security key to secure wireless connection.

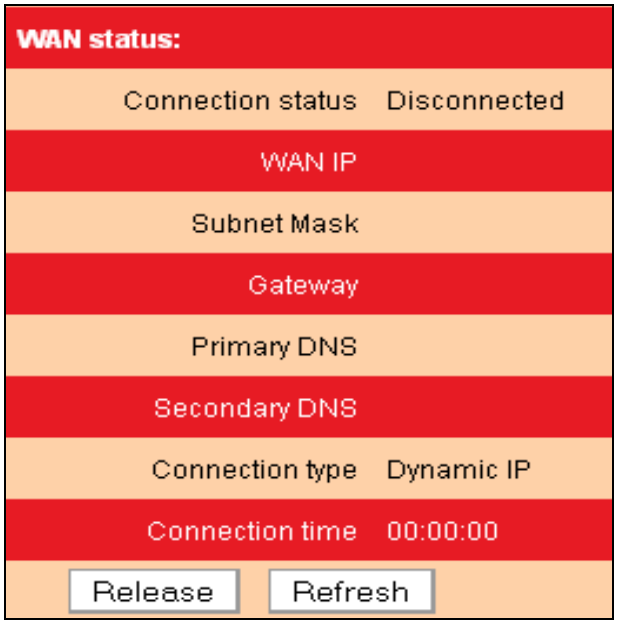


For more settings you can use the standard menu of advanced setup

Chapter 4 Network Settings

4.1 Status Info

This section allows you to view the router's WAN and system information.



● **Connection Status**: Displays WAN connection status: Disconnected, Connecting or Connected.

Disconnected: Indicates that the Ethernet cable from your ISP side is not connected to the WAN port / connection problem of cable line.

Connecting: Indicates that the WAN port is correctly connected and is requesting an IP address from your ISP.

Connected: Indicates WAN port has been connected to your ISP.

● **WAN IP**: Displays WAN IP address.

● **Subnet Mask**: Displays WAN subnet mask.

● **Gateway**: Displays WAN gateway address.

● **Primary DNS**: Displays WAN primary DNS address.

● **Secondary DNS**: Displays WAN secondary DNS address.

● **Connection Type**: Displays current Internet connection type.

System status:	
LAN MAC address	XX:XX:XX:XX:XX:XX
WAN MAC address	XX:XX:XX:XX:XX:XX
System time	2011-04-01 00:55:44
Running time	00:55:44
Connected client	1
Firmware Version	V1.0.0
Hardware version	V3.0

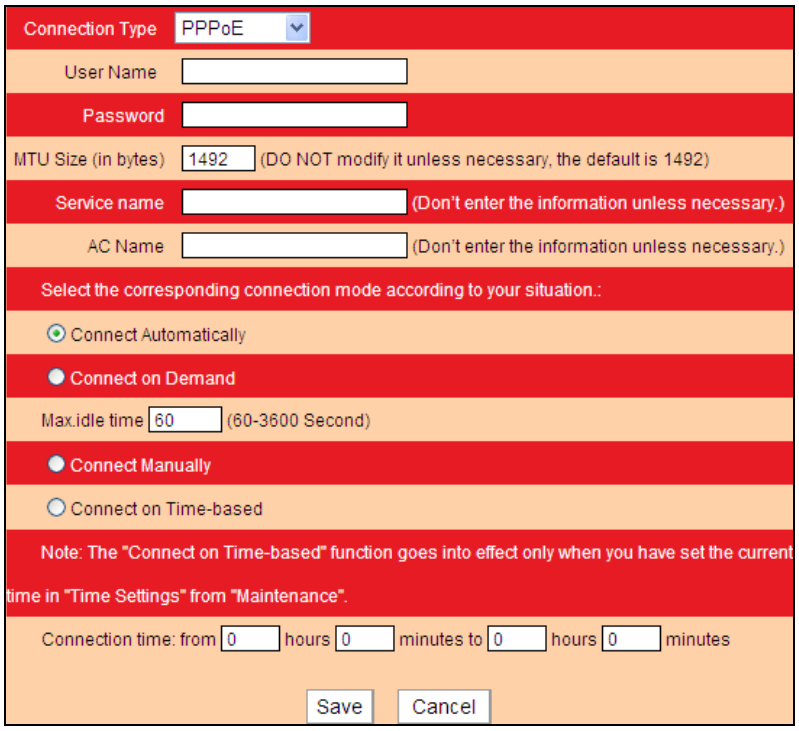
- **LAN MAC Address**: Displays router's LAN MAC address.
- **WAN MAC Address**: Displays router's WAN MAC address.
- **System Time**: Displays the time when system is updated.
- **Connected client**: Displays the number of connected computers (which obtains IP addresses from the device' DHCP server).
- **Software Version**: Displays router's firmware version.
- **Hardware Version**: Displays router's hardware version.

4.2 WAN

There are 5 Internet connection types available for your selection: PPPoE, Static IP，Dynamic IP，PPTP and L2TP. Select your Internet connection type and follow corresponding instructions below:

4.2.1 PPPoE

Select PPPoE, if your ISP are using a PPPoE connection and provide you with PPPoE user name and password information.

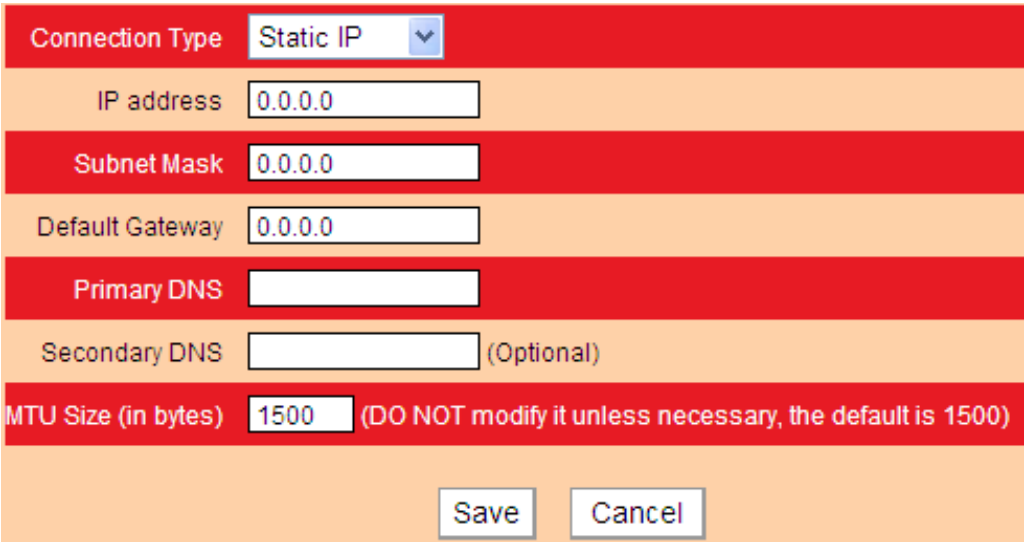


● **Connection Type**: Displays current Internet connection type.
● **User Name**: Enter the user name provided by your ISP.
● **Password**: Enter the password provided by your ISP.
● **MTU**: Maximum Transmission Unit. DO NOT change it from the factory default of 1492 unless necessary. You may need to change it for optimal performance with some specific websites or application software that cannot be opened or enabled; in this case, try 1450, 1400, etc.
● **Service Name**: Description of PPPoE connection. Leave blank unless necessary.
● **AC Name**: Description of server. Leave blank unless necessary.
● **Connect Automatically**: Connects automatically to the Internet upon device startup or disconnection from the Internet.
● **Connect Manually**: Users need to connect the device to Internet manually upon disconnection from the Internet.
● **Connect on Demand**: Connects to Internet automatically upon traffic present.
● **Connect on Fixed Time**: Connects to Internet automatically within the specified time length.

⚠**Note:**
To activate the “Connect on Fixed Time" feature, you must first configure current time on the "Time Settings” screen under "System Tools" menu.

4.2.2 Static IP

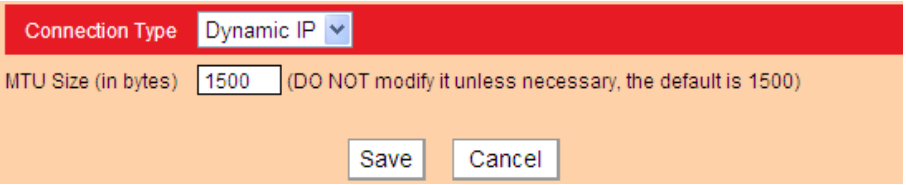
If your ISP offer you static IP Internet connection type, select “Static IP" from Mode drop-down menu and then enter IP address, subnet mask, Primary DNS and secondary DNS information provided by your ISP into corresponding fields.



● **Connection Type**: Displays the current Internet connection type.
● **IP Address**: Enter the WAN IP address provided by your ISP. Inquire your ISP if you are not clear.
● **Subnet Mask**: Enter WAN Subnet Mask provided by your ISP. The default is 255.255.255.0.
● **Default Gateway**: Enter the WAN Gateway provided by your ISP.
● **Primary DNS**: Enter the necessary DNS address provided by your ISP.
● **Secondary DNS**: Enter the secondary DNS address if your ISP provides, and it is optional.
● **MTU**: Maximum Transmission Unit. DO NOT change it from the factory default of 1500 unless necessary. You may need to change it for optimal performance with some specific websites or application software that cannot be opened or enabled.

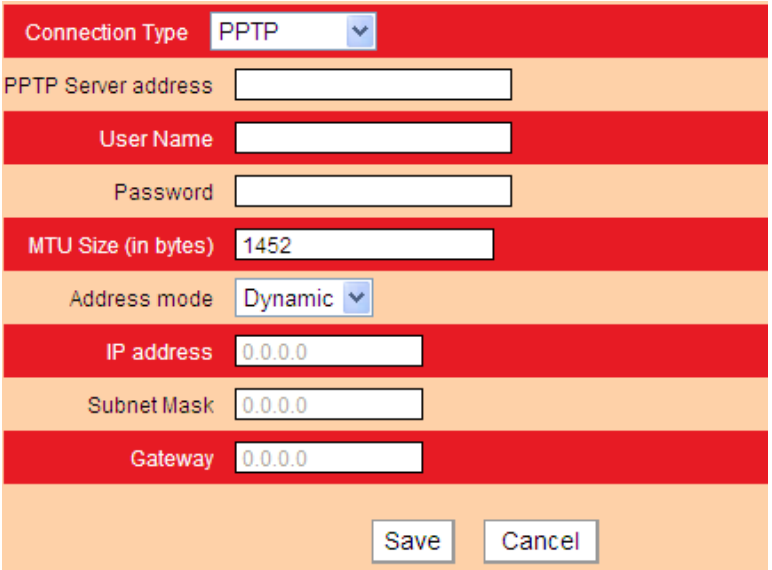
4.2.3 Dynamic IP

Select this option if your ISP does not give you any IP information or account information. You don’t need to configure any settings for this connection.



● **MTU**: Maximum Transmission Unit. DO NOT change it from the factory default of 1500 unless necessary. You may need to change it for optimal performance with some specific websites or application software that cannot be opened or enabled.

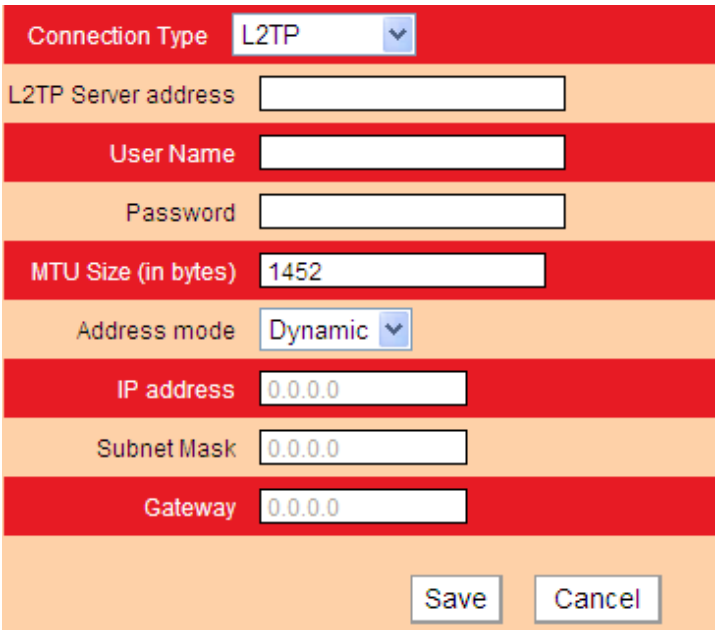
4.2.4 PPTP:



● **Connection Type**: Displays the current Internet connection type.
● **PPTP Server address**: Enter the IP address of a PPTP server.
● **Username/Password**: Enter Username/Password given by the PPTP server.
● **MTU**: Maximum Transmission Unit. DO NOT change factory default value unless necessary. However you may need to change it for optimal performance with some specific websites or application software that cannot be opened or enabled; in this case, try 1450, 1400, etc.

● **Address mode**: Select “Dynamic” if you don’t get any IP information from the PPTP server, otherwise select “Static”.
● **IP address**: Enter the IP address information provided by your ISP (PPTP server). Inquire your local ISP if you are not clear (Static IP address mode only).
● **Subnet mask**: Enter the subnet mask provided by your ISP, normally, 255.255.255.0 (Static IP address mode only).
● **Gateway**: Enter the gateway provided by your ISP (Static IP address mode only). Inquire your local ISP if you are not clear.

4.2.5 L2TP

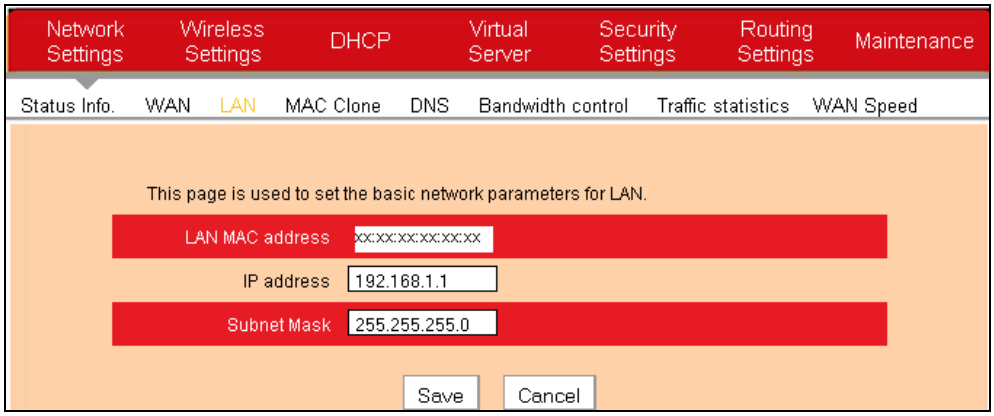


● **Connection Type**: Displays the current Internet connection type.
● **L2TP Server address**: Enter the IP address of a L2TP server.
● **Username/Password**: Enter Username/Password specified by the PPTP server.
● **Address mode**: Enter the IP address information provided by your ISP (PPTP server). Inquire your local ISP if you are not clear (Static IP address mode only).
● **IP address**: Enter the IP address information provided by your ISP (PPTP server). Inquire your local ISP if you are not clear (Static IP address mode only).

● **Subnet mask**: Enter the subnet mask provided by your ISP, normally, 255.255.255.0 (Static IP address mode only).
● **Gateway**: Enter the gateway provided by your ISP (Static IP address mode only). Inquire your local ISP if you are not clear.

4.3 LAN

Click “Advanced Settings”----“LAN Settings” to enter the interface below.



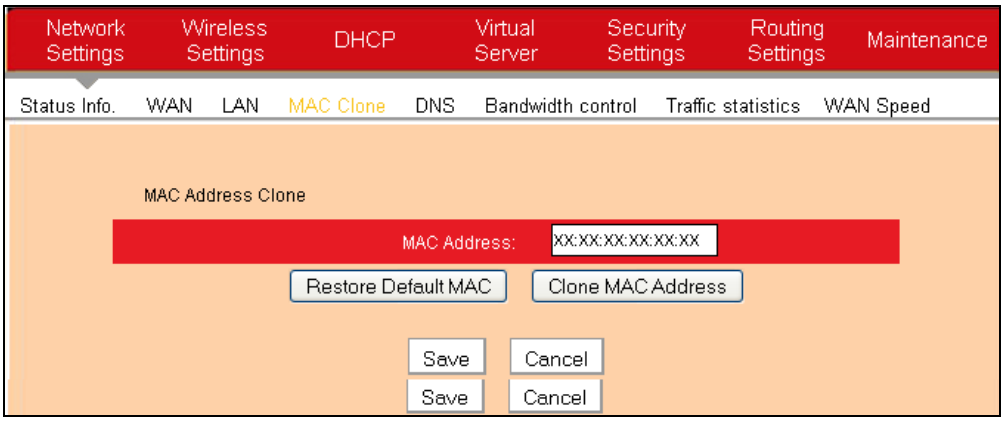
● **LAN MAC Address**: Displays the router’s LAN MAC address, which cannot be changed.
● **IP Address**: The default LAN IP address for this router is 192.168.1.1. You can change it according to your need.
● **Subnet Mask**: Enter the Router’s LAN subnet mask. The default value is 255.255.255.0.

⚠ **Note:**

If you change the device’s LAN IP address, you must enter the new one in your browser to get back to the web-based configuration utility. And LAN PCs’ gateway must be set to this new IP for successful Internet connection.

4.4 MAC Clone

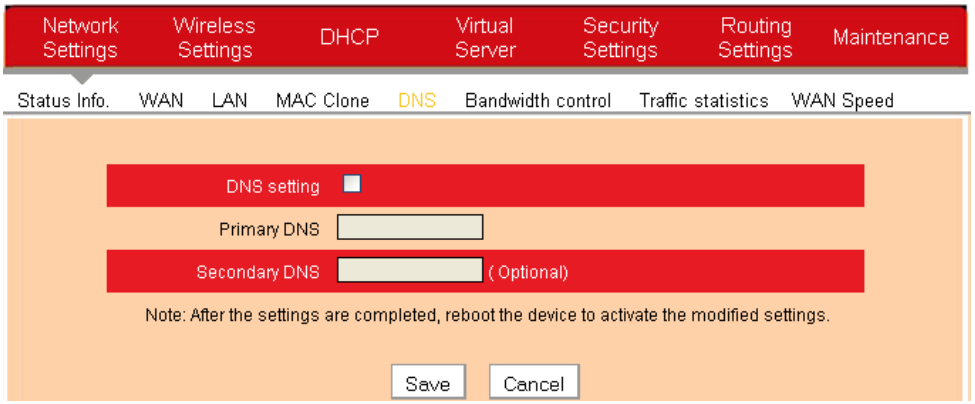
This section allows you to configure router's WAN MAC address. Some ISP may require binding an accepted MAC address for communication. If the bound MAC address differs from your router's predefined WAN MAC address, then you need to replace the router's WAN MAC with the bound MAC for achieving valid communication with your ISP.



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

4.5 DNS

The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It functions just as the "phone book" for the Internet by translating human-friendly domain names into numerical identifiers of IP addresses for the purpose of locating and addressing these devices worldwide.



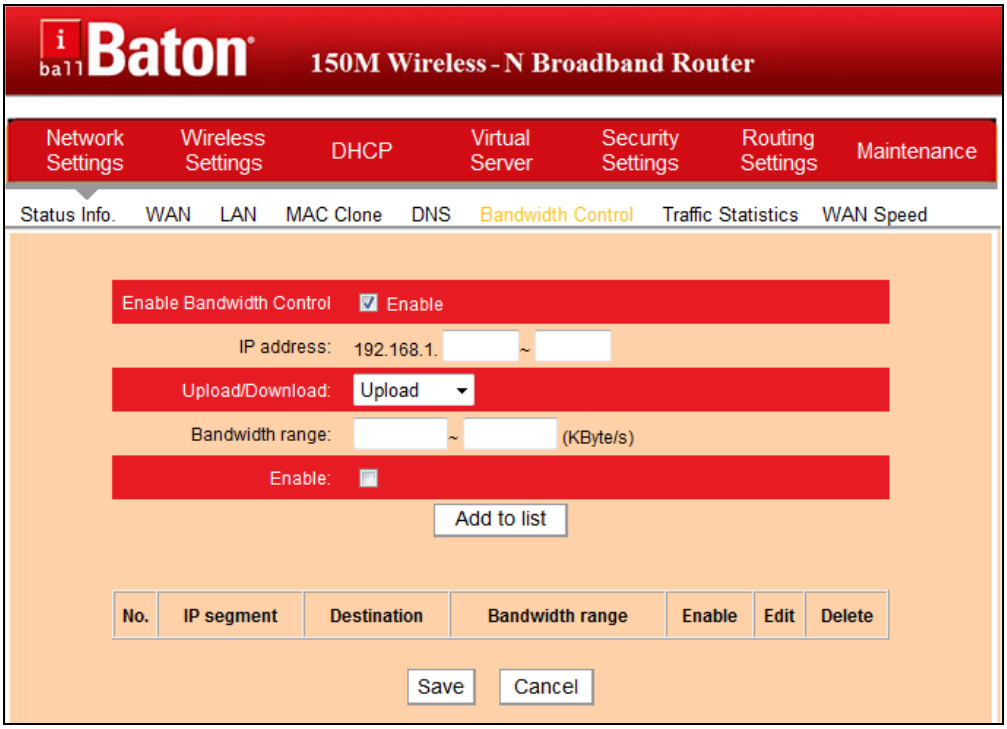
- **DNS Setting**: Check the box to enable DNS settings.
- **Primary DNS**: Enter the DNS server address provided by your ISP.
- **Secondary DNS**: Enter the secondary DNS address if your ISP offers you 2 DNS addresses (Optional).

⚠ **Note:**

1. Wrong DNS server addresses will lead to failure in accessing websites.
2. To activate the new settings, reboot the device.

4.6 Bandwidth Control

The bandwidth control feature can be used to simultaneously regulate traffic of up to 254 computers on your LAN network. It allows you to regulate a group of PCs' traffic by specifying a range of IP addresses.

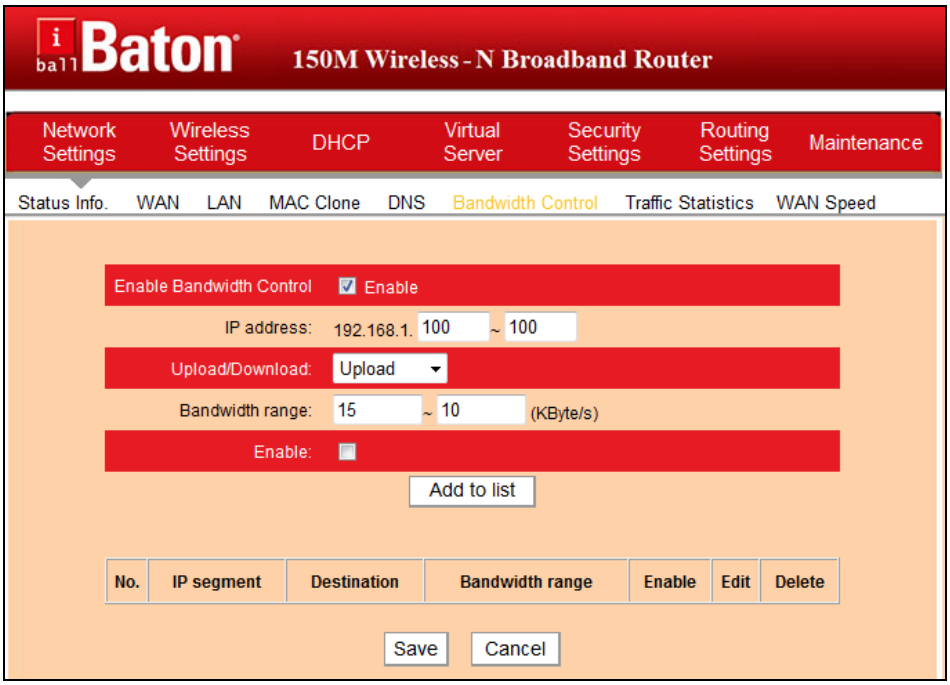


● **Enable Bandwidth Control**: Check/uncheck the box to enable/disable bandwidth control. It is disabled by default.
● **IP Address**: Enter an IP address (same number in both boxes) or a range of IP addresses (different numbers in two boxes) of the PCs whose traffic you want to regulate.
● **Upload /Download**: You can select either to limit Uplink or Downlink Bandwidth of PCs within the specified IP range.
● **Bandwidth Range**: Maximum and minimum data flow which is permitted to be uploaded/downloaded by computers within a specified IP range. Unit is Kbytes/s. (For WAN bandwidth range, consult your ISP.)
● **Enable**: Check the box to enable current rule. The existing rule will not take effect when left unchecked.
● **Add to List**: Click it to add currently edited bandwidth control rule to the list.

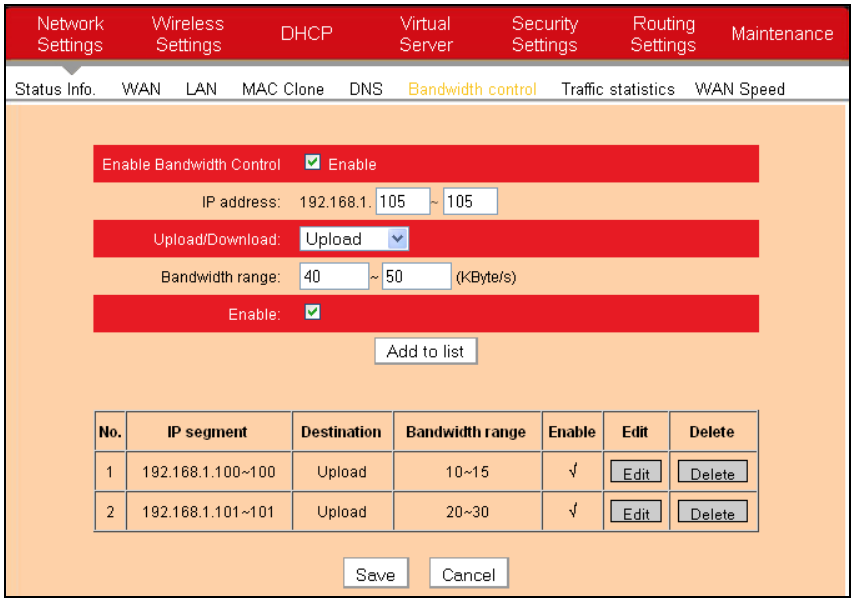
For example: Suppose that you have a 2M WAN connection, then maximum

download and upload rates in theory will be 2Mbps=256KByte/s and 512kbps=64KByte/s respectively. And you want the PC at the IP address of 192.168.1.100 to have 10-15KByte/s upload and 80-90KByte/s download rates.

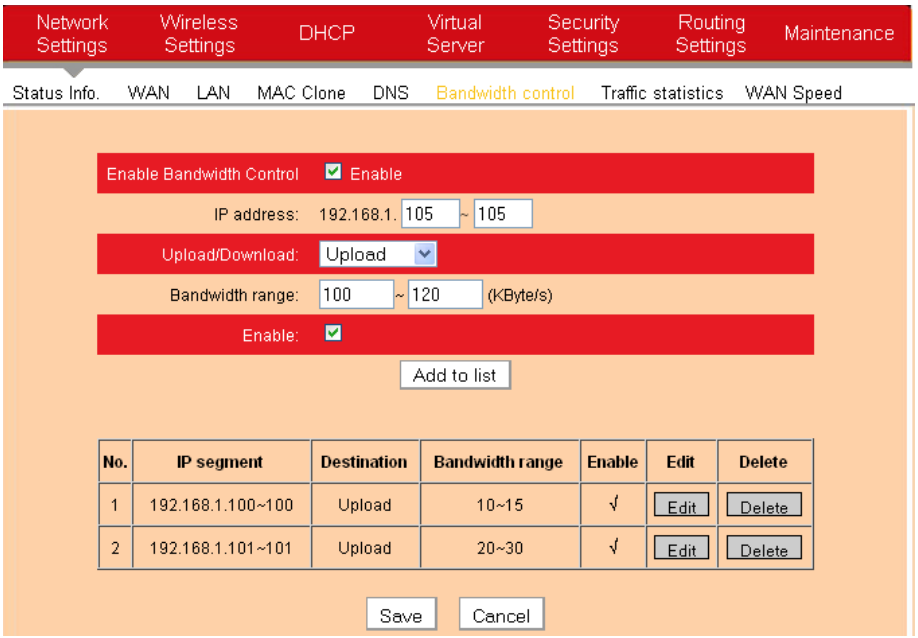
Follow below step:



Step1. Enter 192.168.1.100 in IP address boxes.
Step2. Select Upload from the corresponding drop-down menu.
Step3. Enter 10~15 in bandwidth range box
Step4. Check the “Enable” box.
Step5. Click “Add to List”.
Step6. Click “OK” to finish settings.
Then, follow steps above to add a download rule.

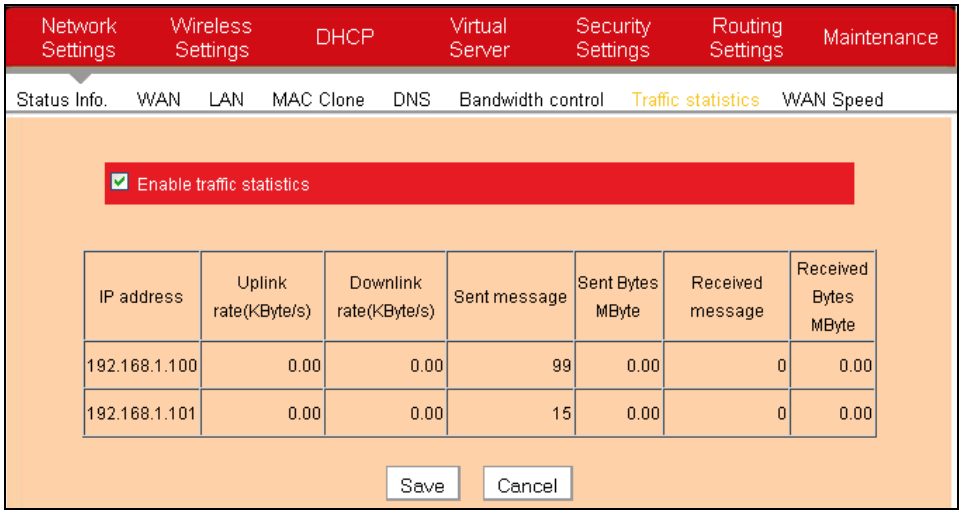


For example: Supposing that you want PCs within the IP range of 192.168.1.2--192.168.1.254 to have 100-120KByte/s download rate and 20-30KByte/s upload rate, then repeat same settings shown on below screenshot on your router:



4.7 Traffic Statistics

Statistics dynamically displays bandwidth usage by PCs on your LAN.



● **Enable Traffic Statistics**: Check the box to gather bandwidth usage by PCs on your LAN. It is disabled by default. Disabling this option may boost router's packet processing capacity. When enabled, system will dynamically renew statistics information every 5 seconds.

● **IP Address**: Displays IP address information of a corresponding statistics item.

● **Uplink Rate**: Displays how many Kbytes of data have been transmitted per second.

● **Downlink Rate**: Displays how many Kbytes of data have been received per second.

● **Sent Message (TX Packets)**: Displays the total number of packets transmitted by a corresponding IP address through the router.

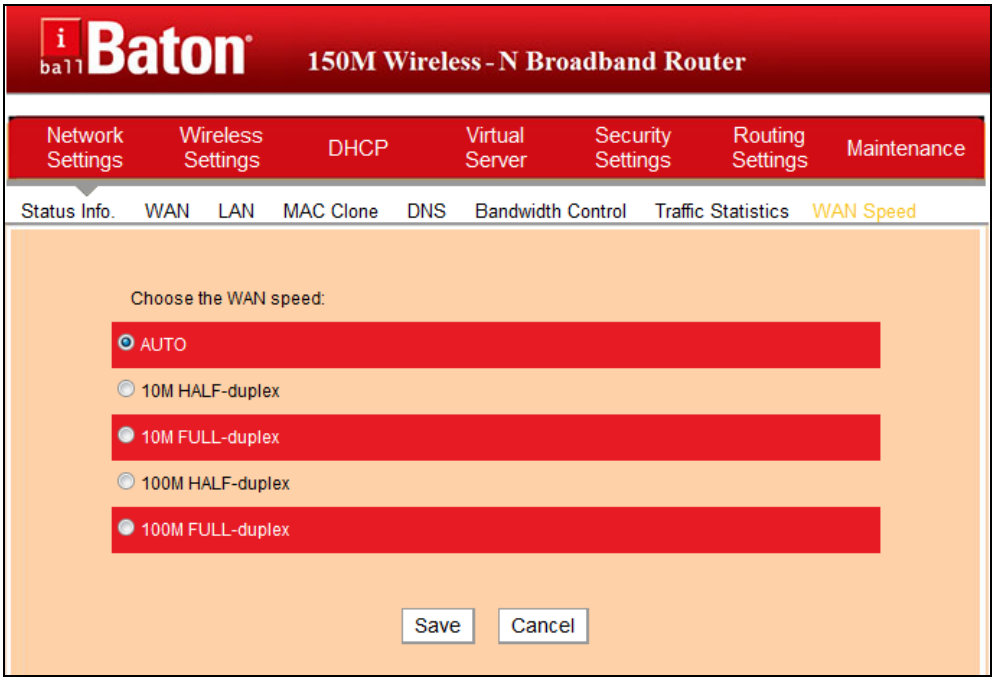
Sent Bytes: Displays how many Mbytes of data have been transmitted by a corresponding IP address through the router.

Received Message (RX Packets): Displays the total number of packets received by a corresponding IP address from the router.

● **Received Bytes**: Displays how many Mbytes of data have been received by a corresponding IP address from the router.

4.9 WAN Speed

This section allows you to configure WAN speed. Default settings are recommended.



● **AUTO**: DO NOT change this default setting unless you are connecting an excessively long Ethernet cable from your ISP, which may degrade drive capability, to the router's WAN port.

● **10M HALF-duplex**: Select it if your router's WAN port does not function properly when connected to an Ethernet cable from your ISP; excessive length of the cable may degrade drive capacity of the WAN port.

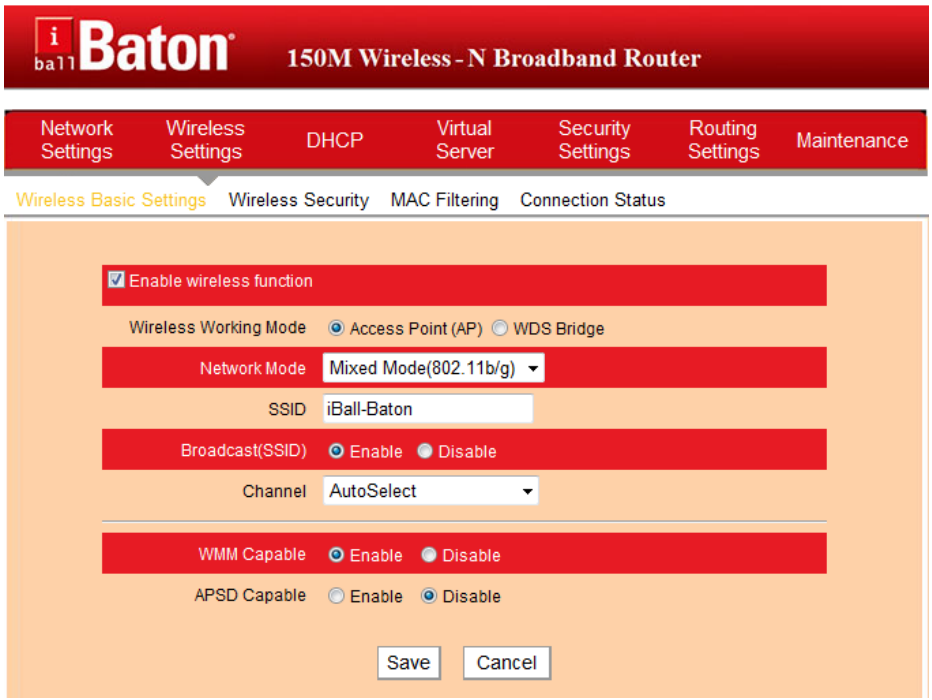
● **10M FULL -duplex**: Select it to set router's WAN port to work at 10Mbps in full duplex mode, improving WAN port drive capacity.

● **100M HALF-duplex**: Select it to set router's WAN port to work at 100Mbps in half duplex mode.

● **100M FULL-duplex**: Select it to set router's WAN port to work at 100Mbps in full duplex mode.

Chapter 5 Wireless Settings

5.1 Wireless Basic Settings



●**Enable Wireless function**: Check/uncheck to enable/disable the wireless feature. When disabled, all wireless related features will be disabled automatically

●**Wireless working Mode**: Select AP or WDS by clicking the corresponding radio button.

● **Network Mode**: Network Mode: Select a right mode according to your wireless client. The default mode is 11b/g/n mixed.

● **11Mbps 802.11b mode**: Select it if you have only Wireless-B clients in your wireless network.

● **54Mbps 802.11g mode**: Select it if you have only Wireless-G clients in your wireless network.

● **Mixed 802.11b/g mode**: Select it if you have only Wireless-B and Wireless-G clients in your wireless network.

● **Automatic 11b/g/n mixed mode**: Select it if you have Wireless-B, Wireless-G and Wireless-N clients in your wireless network.

● **SSID**: A SSID (Service Set Identifier) is the unique name of a wireless network. The primary SSID is changeable and compulsory.

● **Broadcast (SSID)**: Select “Disable” to hide your SSID. When disabled, no wireless clients will be able to see your wireless network when they

perform a scan to see what's available. If they want to connect to your router, they will have to first know this SSID and then manually enter it on their devices. By default, this option is enabled.

● **Channel**: The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. From the drop-down list，you can select a most effective channel, which ranges from 1 to 11. You can also select "Auto Select" to let system detect and choose one that best fits your network.

● **WMM-Capable**: Enabling this option may boost transmission capacity of wireless multimedia data (such as online video play).

● **ASPD Capable**: Auto power saving mode for WMM feature, disabled by default.

● **Channel Bandwidth**: Select a proper channel bandwidth to enhance wireless performance. When there are 11b/g and 11n wireless clients, please select the 802.11n mode of 20/40M frequency band; when there are only non-11n wireless clients, select 20M frequency band mode; when the wireless network mode is 11n mode, please select 20/40 frequency band to boost its throughput.

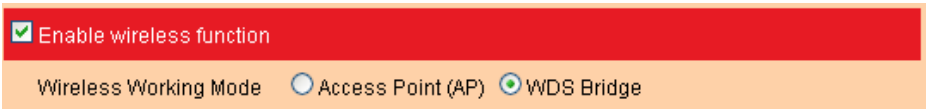
● **Extension Channel**：Indicates the working network frequency range for 11n mode.

● **WDS Mode**: To extend your existing wireless network coverage, select the WDS (Wireless Distribution System) feature.

● **AP MAC Address**: Enter the MAC address of a wireless link partner or populate this field using the Open Scan option.

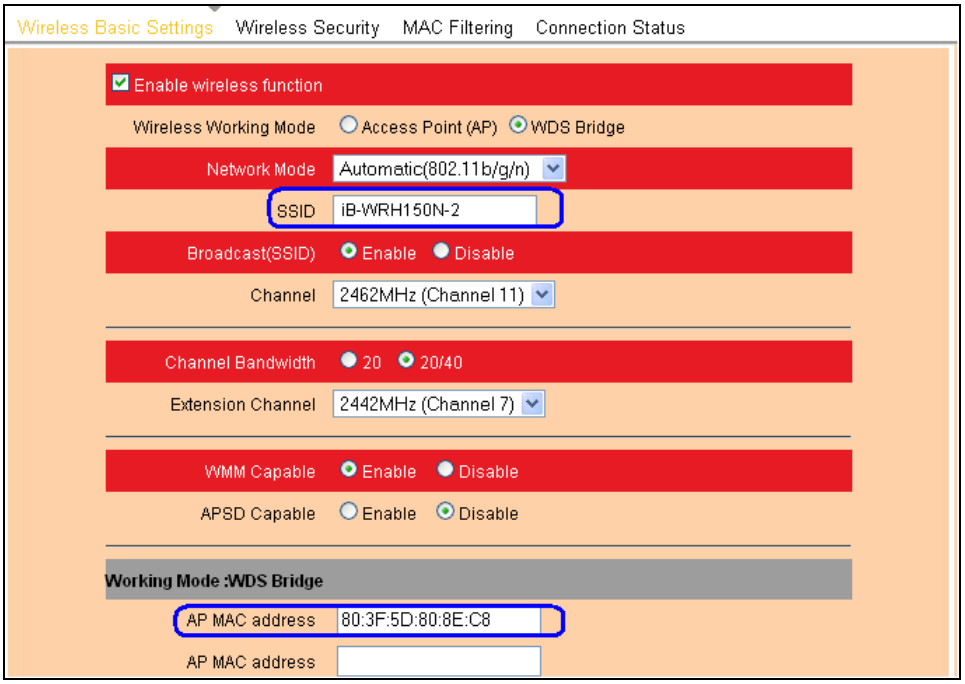
Application example: Implement the WDS feature using 2 iB-WRB150N wireless router labeled iB-WRB150N-1 and iB-WRB150N-2.

1. Change the default wireless working mode of AP on iB-WRB150N to WDS as shown in the figure below:



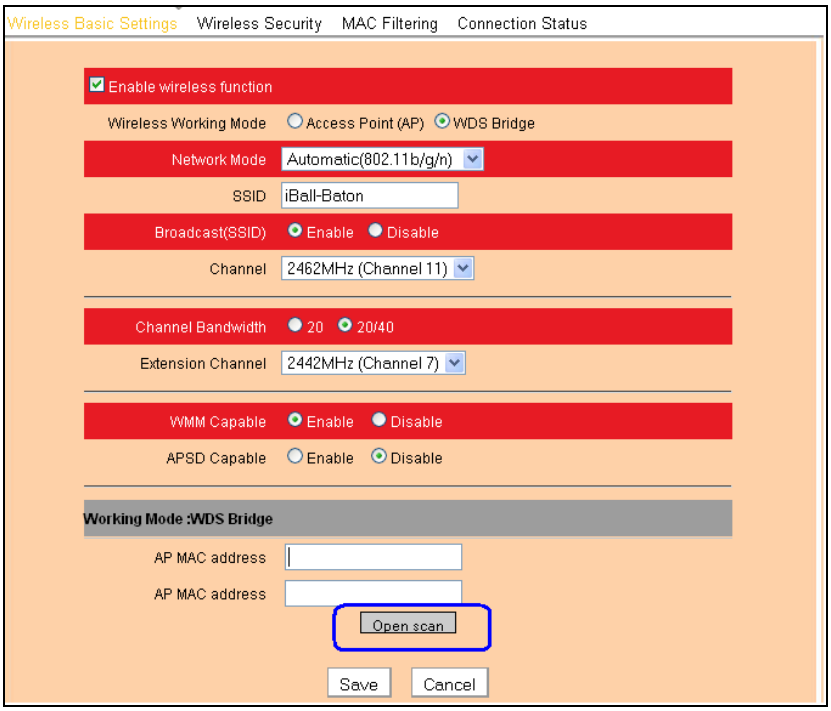
2. Add iB-WRH150N-2's MAC address to iB-WRH150N-1 and change iB-WRH150N-1's SSID and channel respectively to those of iB-WRH150N-2. (Assuming that iB-WRH150N-2's SSID is changed to OFFICE)

a. If you already know iB-WRH150N-2's MAC address, SSID and channel settings, then you can manually configure the same settings on iB-WRB150N-1.



b. Or you can use the Open Scan option.

1) Click the “Open Scan” button to display a list of available wireless networks.



2) Select the iB-WRH150N-2's SSID from the list and click OK on the appearing dialogue box; iB-WRH150N-2's MAC address, SSID and channel settings will be automatically added to the iBl-WRH150N-1

3) Click OK to save your settings.

4) Configure wireless security settings. For this step, refer to section 5.2 hereof.

5) Repeat steps 1-4 on iB-WRH150N-2. After the 2 routers have added each other's MAC address and share the same SSID, channel, security settings and security key, the WDS feature can be implemented.

⚠ **Note:**

1. WDS feature can be implemented only between 2 wireless devices that both support the WDS feature. Plus, SSID, channel, security settings and security key must be the same on both devices. Using the Open Scan option and selecting link partner from the scan list automatically change the router's existing SSID and channel settings respectively to those of link partner as well as add link partner's MAC address. So we recommend you to use this Open Scan option for easy WDS settings.

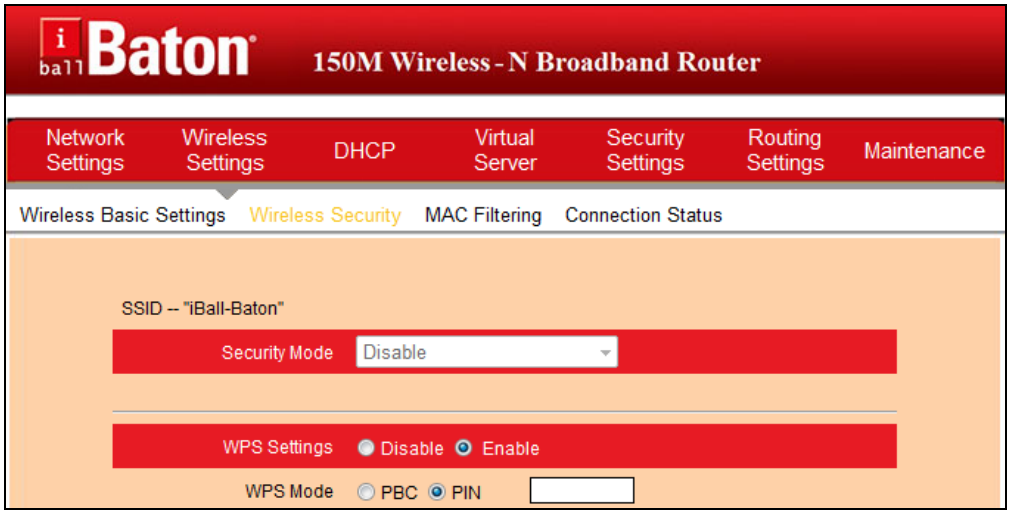
2. Using WEP encryption improves WDS compatibility. For this reason, we recommend you to encrypt your wireless network with WEP when using the WDS feature.

5.2 Wireless Security

This section allows you to configure wireless security settings to block unauthorized access to your wireless network and prevent malicious packet sniffing. You have 4 ways to encrypt your wireless data: WPS, WEP, WPA-PSK and WPA2-PSK.

5.2.1 WPS Settings

Wi-Fi Protected Setup makes it easy for home users who know little of wireless security to establish a secure wireless home network, as well as to add new devices to an existing network without entering long passphrases or configuring complicated settings. Simply enter a PIN code or press the software PBC button or hardware WPS button (if any) and a secure wireless connection is established.



● **WPS Settings**: Select to enable/disable the WPS encryption. It is enabled by default.
● **WPS Mode**: Select PBC (Push-Button Configuration) or PIN.
● **PBC**: Click this software button or directly press the hardware WPS button on both your router and the new wireless client device (that you want to connect to your router wirelessly) for 1 second to establish an easy and secure wireless connection.
● **PIN**: To use this option you must know the PIN code from the wireless client. Simply click the PIN radio button and enter client's PIN code while using the same PIN code on client side for secure connection.
● **Reset OOB**: When clicked, the WPS LED will display a solid light; the WPS function will be disabled automatically; WPS server on the Router enters idle mode and will not respond to client's WPS connection request.

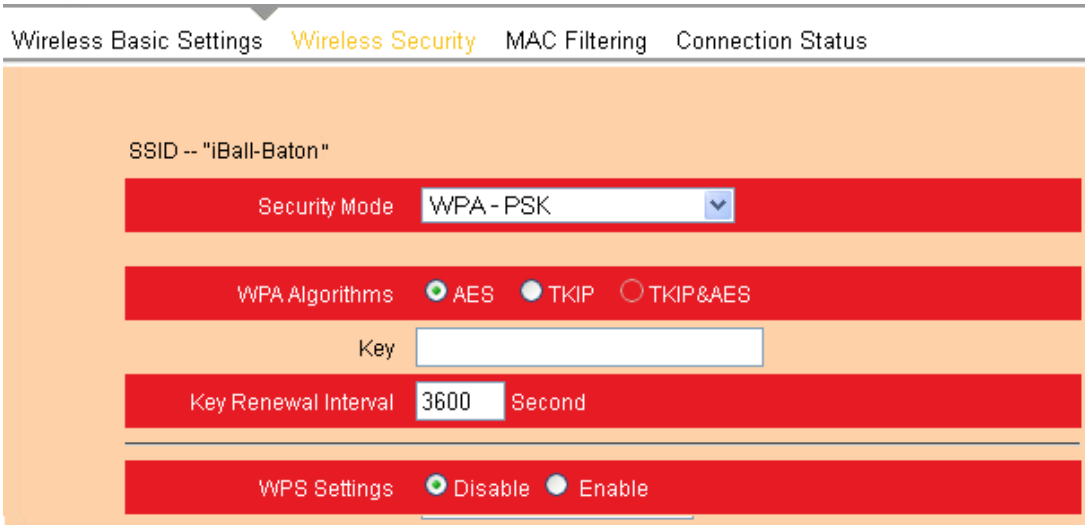
⚠ **Note**:

1. If you find the WPS LED blinking for 2 minutes after you select and apply the PBC mode, it means that the PBC encryption method is successfully enabled. And an authentication will be performed between your router and the WPS/PBC-enabled wireless client device during this time; if it succeeds, the wireless client device connects to your device, and the WPS LED displays a solid light thereafter. Repeat steps mentioned above if you want to connect more wireless client devices to your router.

2. The WPS function can be implemented only between your Router and another WPS-enabled device.

5.2.2 WPA-PSK

The WPA protocol implements the majority of the IEEE 802.11i standard. It enhances data encryption through the Temporal Key Integrity Protocol (TKIP) which is a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet. WPA also includes a message integrity check feature to prevent data packets from being hampered with. Only authorized network users can access the wireless network.



● **Security Mode**: Select a proper mode, which is also supported by your wireless clients, from the drop-down menu.

● **WPA Algorithms**: Select either AES (advanced encryption standard) or TKIP (temporary key integrity protocol) type.

● **Key**: Enter a security key，which must be between 8-63 ASCII characters.

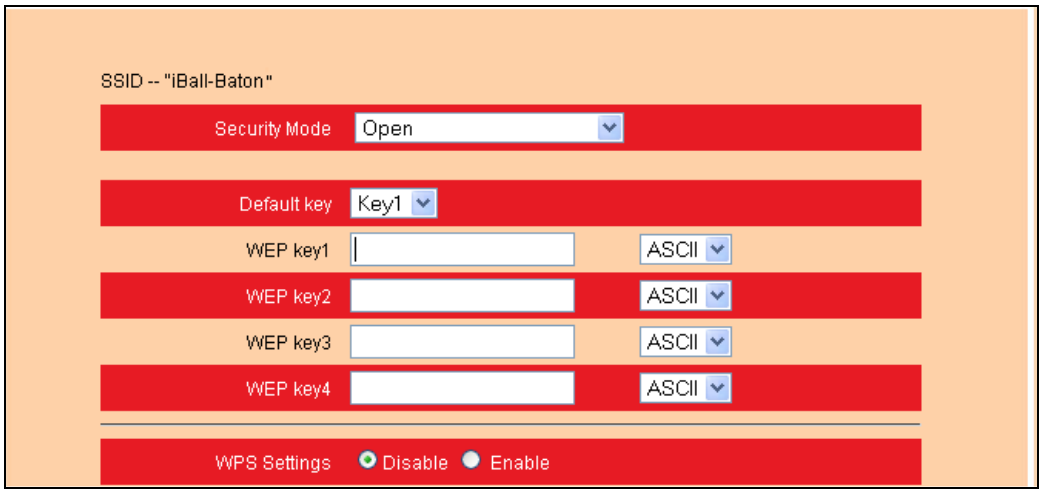
● **Key Renewal Interval**: Enter a valid time period for the key.

5.2.3 WPA2-PSK

The later WPA2 protocol features compliance with the full IEEE 802.11i standard and uses Advanced Encryption Standard (AES) in addition to TKIP encryption protocol to guarantee better security than that provided by WEP or WPA.

5.2.4 WEP

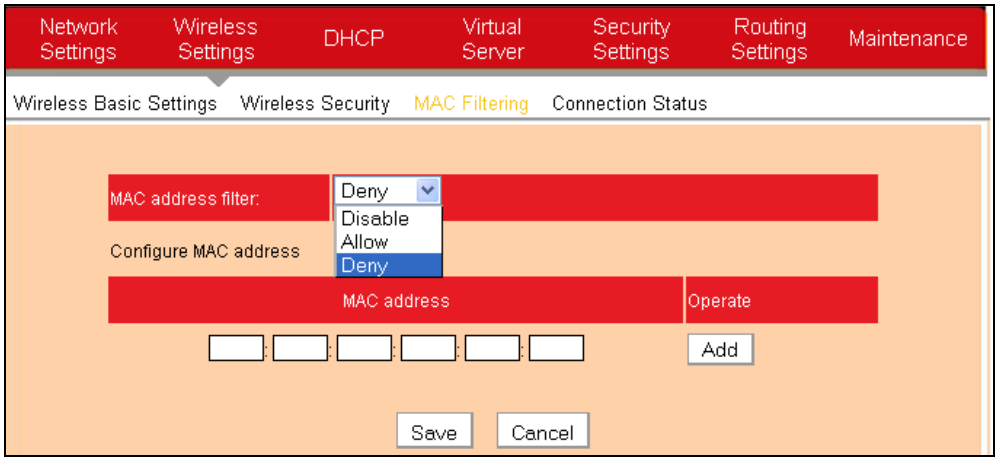
WEP is intended to provide data confidentiality comparable to that of a traditional wired network. Two methods of authentication can be used with WEP: Open System authentication and Shared Key authentication.



● **WEP Key**: You can select either ASCII or Hexadecimal from the drop-down menu.
Note: If you select ASCII, enter 5 or 13 valid ASCII characters; or if you select Hexadecimal, enter 10 or 26 Hexadecimal characters.
● **Default Key**: Select one key from the 4 preset keys.

5.3 MAC Filtering

The MAC filtering feature can be used to allow or disallow clients to connect to your wireless network.



● **MAC Address Filter**: "Permit" means to permit PCs at specified MAC addresses to connect to your wireless network while "Forbid" means to block PCs at specified MAC addresses from connecting to your wireless network.

● **MAC Address**: Enter the MAC addresses of a wireless client and click "Add".

● **MAC Address List**: Displays the MAC addresses added by you. You can delete any entry by clicking on the "Delete" button nearby.

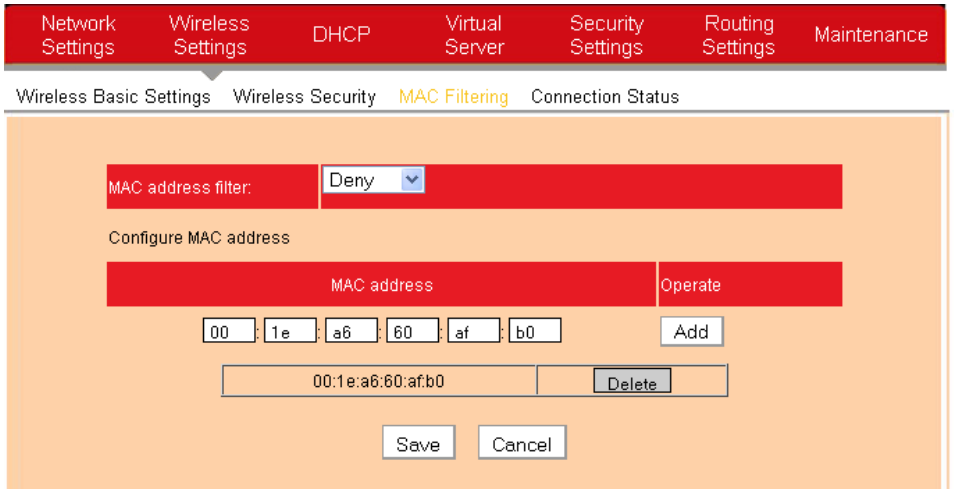
Example 1:

To allow only a PC at the MAC address of 00:1e:a6:a4:56:75 to connect to your wireless network, do as follows:

Step1. Select "Permit" from MAC Address Filter drop-down menu.

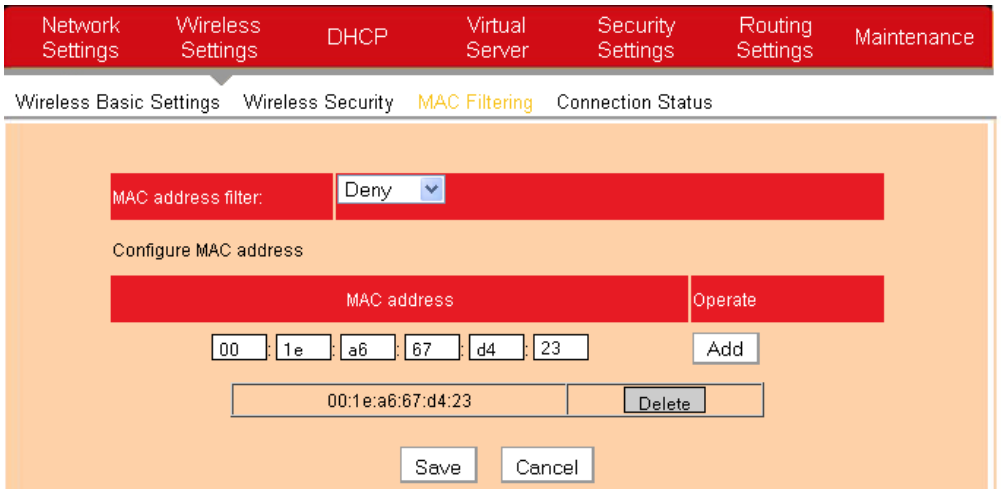
Step2. Enter 00:1e:a6:a4:56:75 in the MAC address box.

Step3. Click the "OK" button to save your settings and you can add more MAC addresses, if you like, simply repeating the follow steps.



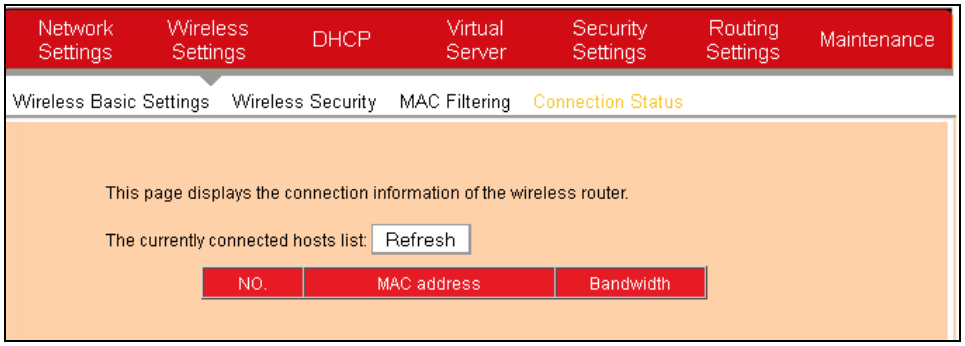
Example 2:

To prohibit only a PC at the MAC address of 00:1e:a6:67:d4:23 from connecting to your wireless network, follow steps above and make a few necessary changes as shown follow.



5.4 Connection Status

This interface displays the information of currently connected wireless clients including MAC addresses and bandwidth.



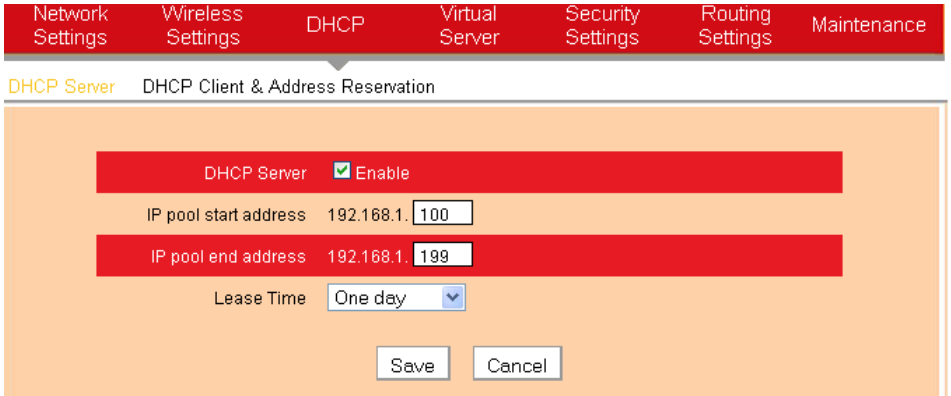
● **MAC Address**: Displays the MAC addresses of the PCs that have been wirelessly connected to your router.
● **Bandwidth**: Displays the channel bandwidth used by the currently connected hosts (connected wireless clients).

⚠ **Note:** "Bandwidth" refers to the wireless channel bandwidth instead of wireless connection rate.

Chapter 6 DHCP

6.1 DHCP Settings

The Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used on IP networks. If you enable the built-in DHCP server on the device, it will automatically configure the parameters of TCP/IP protocol for all your LAN computers (including IP address, subnet mask, gateway and DNS etc), eliminating the need for manual intervention. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to “Obtain an IP Address Automatically”. When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the device.

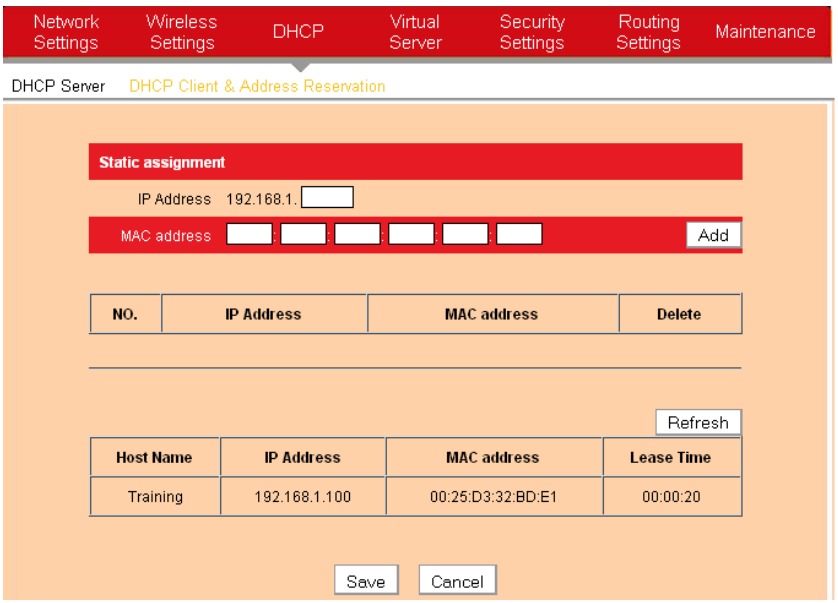


● **DHCP Server**: Check or uncheck the box to enable or disable the device’s DHCP server feature.
● **IP pool start address**: Enter the starting IP address for the DHCP server’s IP assignment.
● **IP pool end address**: Enter the ending IP address for the DHCP server’s IP assignment.
● **Lease Time**: The length of time for the IP address lease. Configuring a proper lease time improves the efficiency for the DHCP server to reclaim disused IP addresses.

6.2 DHCP Clients & Address Reservation

This section not only displays a DHCP dynamic client list but also includes a configurable Static DHCP assignment feature.

The DHCP client list displays IP addresses assigned by the built-in DHCP server, MAC addresses, host names and lease time. If you would like some devices on your network to always have fixed IP addresses, you can manually add a static DHCP assignment entry for each such device. You can manually add an IP address and a MAC address, and then whenever a host with this MAC address connects to the router, it will always get the same IP address (the one you just added). According to the connected computer's MAC address, the router checks relevant entries in its DHCP reservation list and decides what IP address to assign to this host (an unused IP from DHCP IP address pool, or a reserved one): If it fails in finding a reserved IP address for this MAC address in the list, it will immediately assign an unused IP from its DHCP IP address pool; and if such IP is found, it will be assigned to this host so as to ensure that host with a static DHCP assignment always get this reserved IP address.

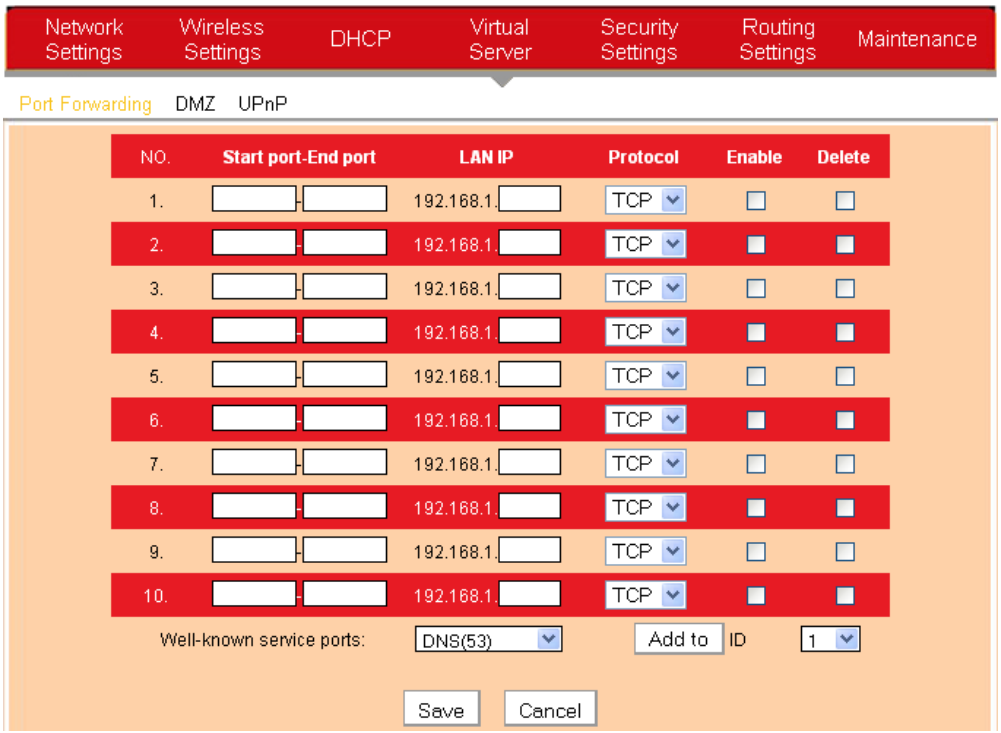


● **IP Address**: Enter the IP address for static DHCP assignment.
● **MAC Address**: Enter the MAC address of a computer to always receive the same IP address (the IP you just entered above).
● **Host name**: Displays the name of a computer (DHCP client).

● **Lease Time**: Remaining time for the corresponding IP address lease.

Chapter 7 Virtual Server

7.1 Port Forwarding



● **Start/End Port**: Enter the service port range provided by the mapped host in internal network.
● **LAN IP**: The IP address of the computer which is used as a server in LAN.
● **Protocol**: Includes TCP, UDP and Both. Select “Both” when you are not sure about which protocol to use.
● **Enable**: Check the “Enable” option to activate the corresponding rule.
● **Delete**: Check the “Delete” option to delete the corresponding rule.

For example:

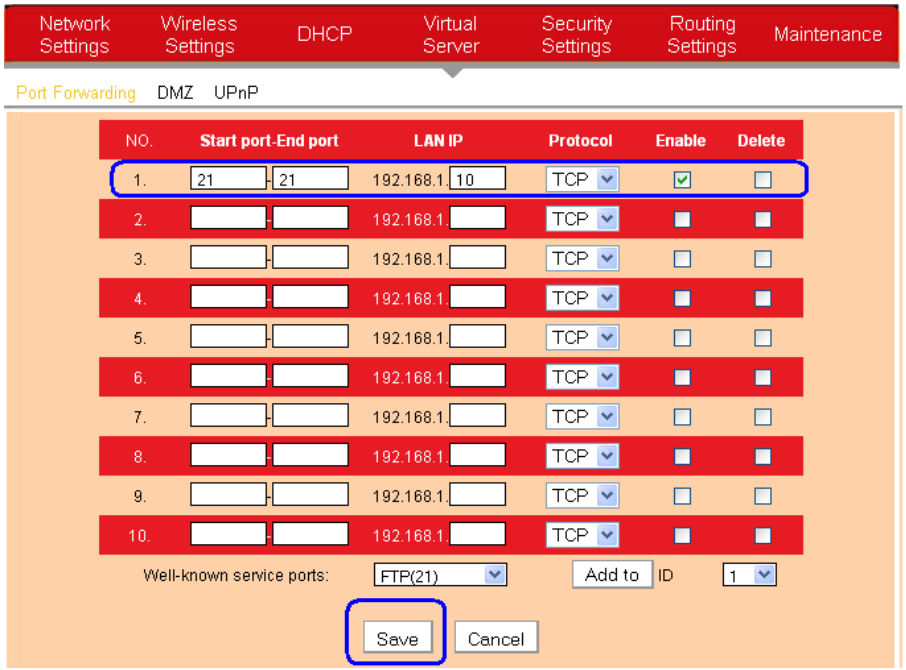
You want to share some large files with your friends who are not in your LAN; however it is not convenient to transfer such large files. Then, you can set up your own PC as a FTP server and use the port range forwarding feature to let your friends access these files. Provided that the static IP address of the FTP server (Namely, your PC) is 192.168.1.10 and

you want your friends to access this FTP server through default port 21 and TCP protocol, then you can follow the steps below for configurations.

1. Enter 21 for both the start and end port in ID 1, or select "FTP" from “Well-Known Service Port” and port 21 will be added automatically to ID 1.

2. Enter 192.168.1.10 for the "IP Address", select "TCP" and then select "Enable'.

3. The screenshot below displays the above settings.



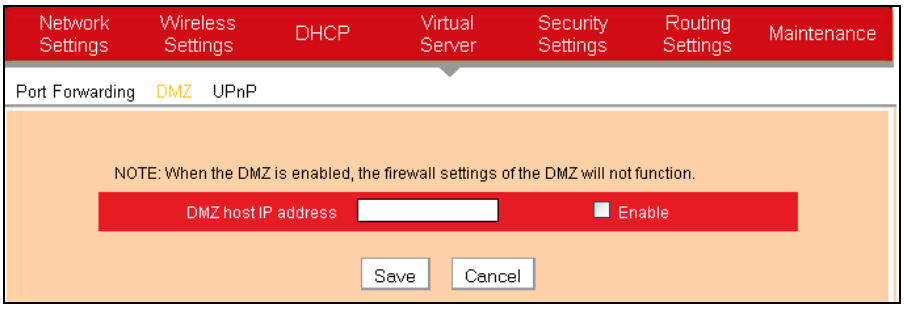
4. Click "OK".

Now, your friends only need to enter ftp://xxx.xxx.xxx.xxx:21 in their browsers to access your FTP server. xxx.xxx.xxx.xxx is the device's WAN IP address. For example, if it is 172.16.102.89, then your friends only need to enter "ftp://172.16.102.89: 21" in their browsers.

⚠ **Note:** If you include port 80 on this section, you must set the port on remote (web-based) management section to a different number than 80, such as 8080, otherwise the virtual server feature may not take effect.

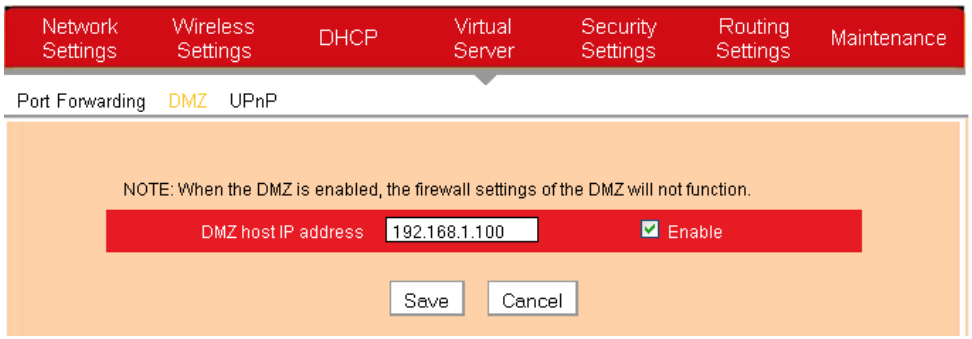
7.2 DMZ

In some cases, we need to set a computer to be completely exposed to extranet for implementation of a 2-way communication. To do so, we set it as a DMZ host.



● **DMZ Host IP Address**: Enter the IP address of a LAN computer which you want to set to a DMZ host.
● **Enable**: Check/uncheck to enable/disable the DMZ host.

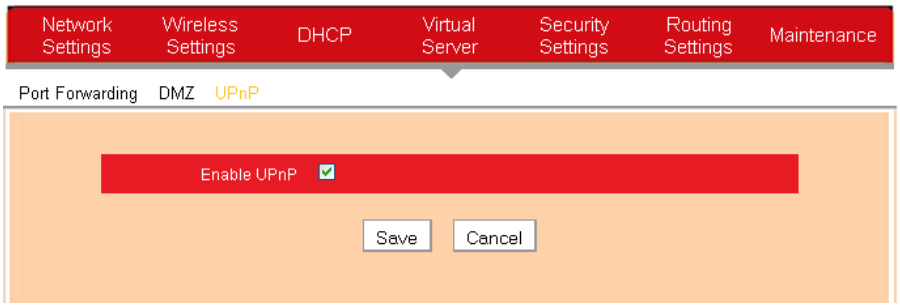
For example: You can set a LAN computer at the IP address of 192.168.1.10 as a DMZ Host to intercommunicate with another host on the Internet.



⚠ **Note:** If you set a PC to a DMZ host, it will be completely exposed to extranet and gains no more protection from the device firewall.

7.3 UPnP

UPnP (Universal Plug and Play) allows a network device to discover and connect to other devices on the network. With this feature enabled, hosts in LAN can request the device to perform special port forwarding so as to enable external hosts to access resources on internal hosts.



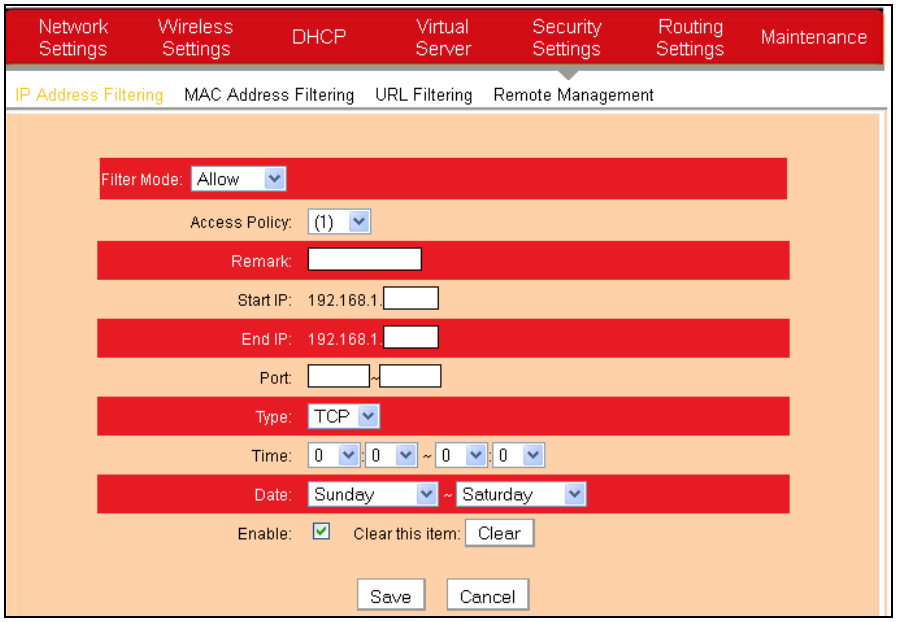
● **Enable UPnP**: Check/uncheck to enable/disable the UPnP feature.

⚠ **Note:** UPnP works in Windows XP, Windows ME or later (NOTE: Operational system needs to be integrated with or installed with Directx 9.0) or in an environment with installed application software that supports UPnP.

Chapter 8 Security Settings

8.1 IP Address Filtering

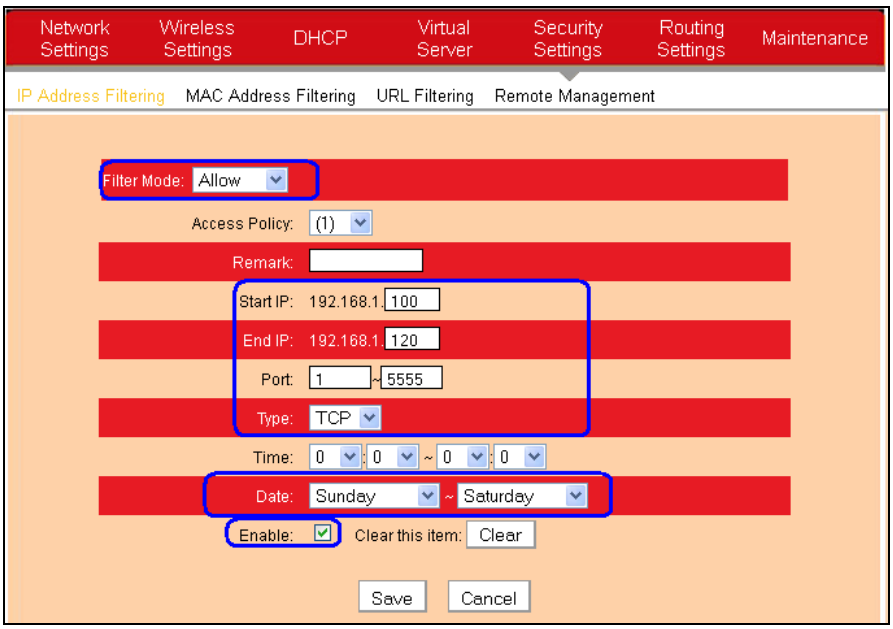
To better manage the computers in LAN, you can regulate LAN computers' access to certain ports on Internet using Client Filter functionality.



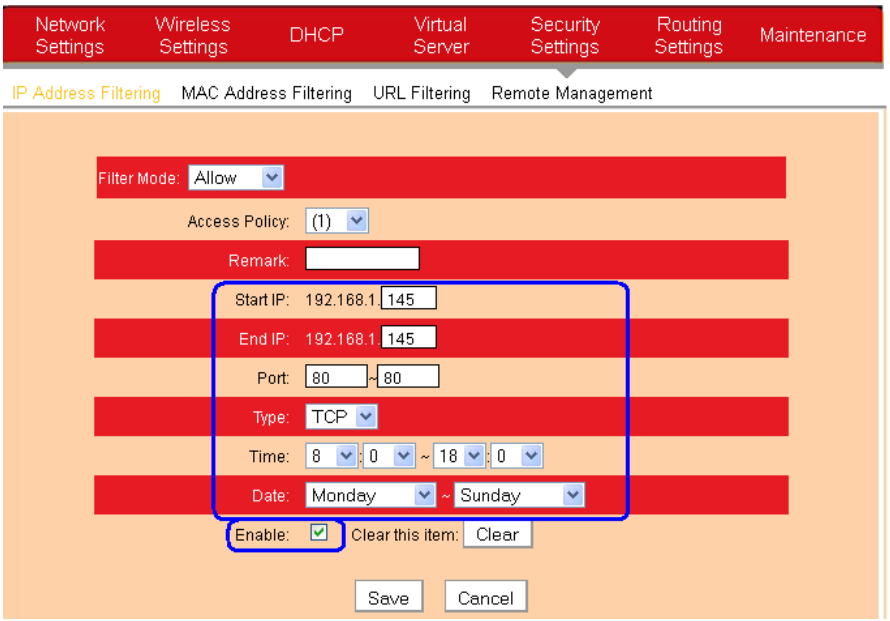
● **Filter Mode**: Select Forbid only or Permit only according to your own needs.
● **Access Policy**: Select a number (indicating a filter rule) from the drop-down menu.
● **Remark**: Enter a meaningful name to yourself for a new filter rule.
● **Start /End IP Address**: Enter a starting/ending IP address.
● **Port**: Enter TCP/UDP protocol port number (s); it can be a range of ports or a single port.
● **Type**: Select a protocol or protocols for the traffic (TCP/UDP/Both).
● **Time**: Select a time range for the rule to take effect.
● **Day**: Select a day or several days for the rule to take effect.
● **Enable**: Check to enable or uncheck to disable a corresponding filter rule (allow/disallow matched packets to pass through router).

Example 1: To prohibit PCs within the IP address range of 192.168.1.100 -- 192.168.1.120 from accessing Internet from Monday to Friday, do as

follows:



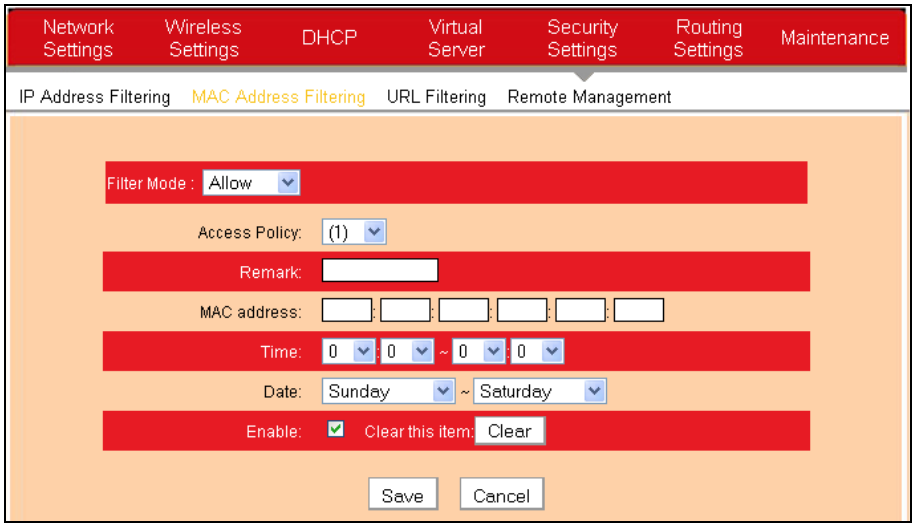
● **Example 2**: To allow only the computer at an IP address of 192.168.1.145 to access Internet from 8:00 to 18:00 without restricting other computers in LAN, do as follow



8.2 MAC Address Filtering

To better manage the computers in LAN, you can use the MAC

Address Filter function to control the computer's access to Internet.



● **Filter Mode**: Select Forbid only or Permit only according to your own needs.

● **Access Policy**: Select a number (indicating a filter rule) from the drop-down menu.

● **Remark**: Enter a meaningful name to you for a new filter rule.

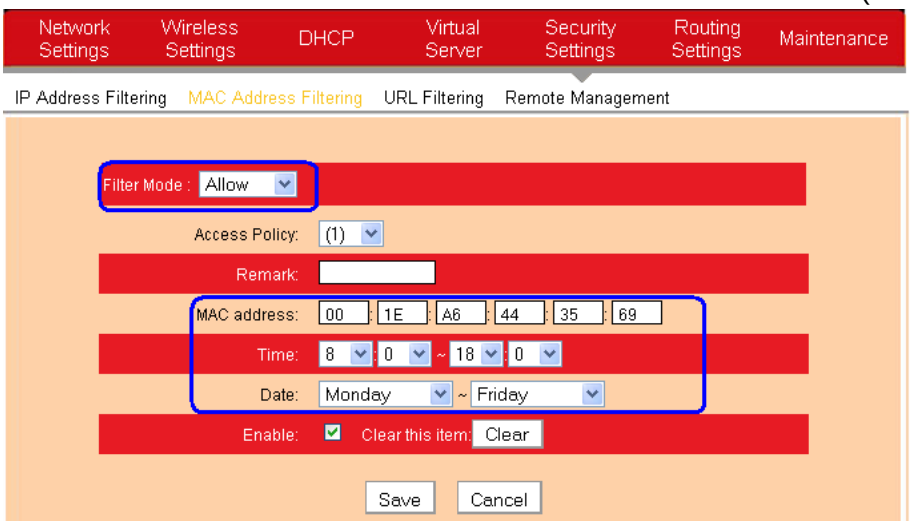
MAC address: Enter the computer's MAC address that you want to filter out in the MAC address field.

● **Time**: Select a time range for the new MAC address filter rule to take effect.

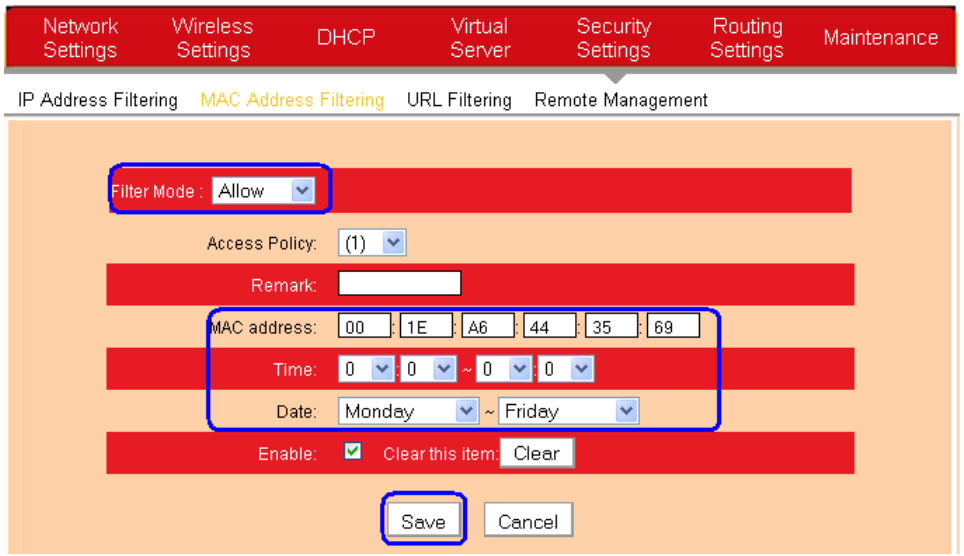
● **Day**: Select a day or several days for the new MAC address filter rule to take effect.

● **Enable**: Check to enable or uncheck to disable a corresponding filter rule (allow/disallow matched packets to pass through router).

Example1: To prevent a PC at the MAC address of 00:E0:4C:69:A3:23 from accessing Internet within the time range of 8:00-18:00 from Monday to Friday, do as follows:

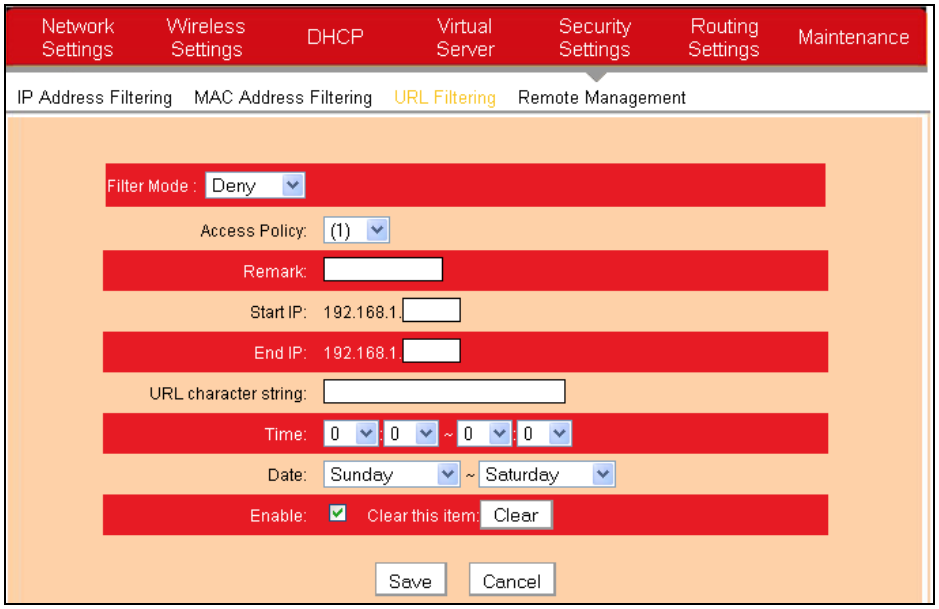


Example2: To allow only the PC at a MAC address of 00:1E:A6:44:35:69 to access Internet from Monday to Friday, do as follows:



8.3 URL Filtering

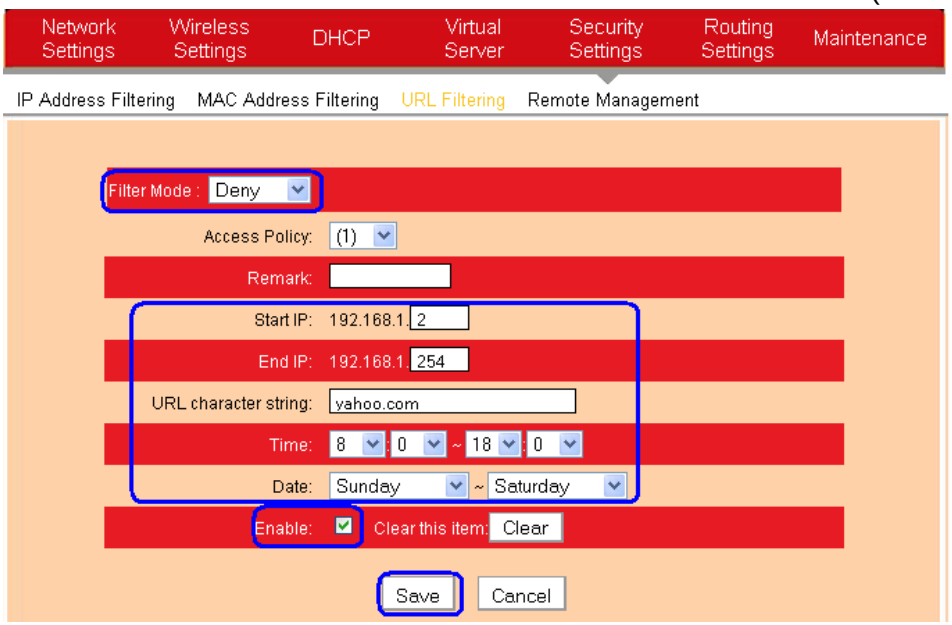
To better control the LAN computers' access to websites, you can use URL filtering to allow or disallow their access to certain websites within a specified time range.



● **Filter Mode**: Select Disable or Forbid only according to your own needs.
● **Access Policy**: Select a number (indicating a filter rule) from the drop-down menu.
● **Remark**: Enter a meaningful name to you for a new filter rule.
● **Start/End IP Address**: Enter the starting/ending IP address.
● **URL character string**: Enter domain names or a part of a domain name that needs to be filtered.
● **Time**: Select a time range for the new URL filter rule to take effect.
● **Day**: Select a day or several days for the new MAC address filter rule to take effect.
● **Enable**: Check to enable or uncheck to disable a corresponding filter rule (allow/disallow matched packets to pass through router).

For example:

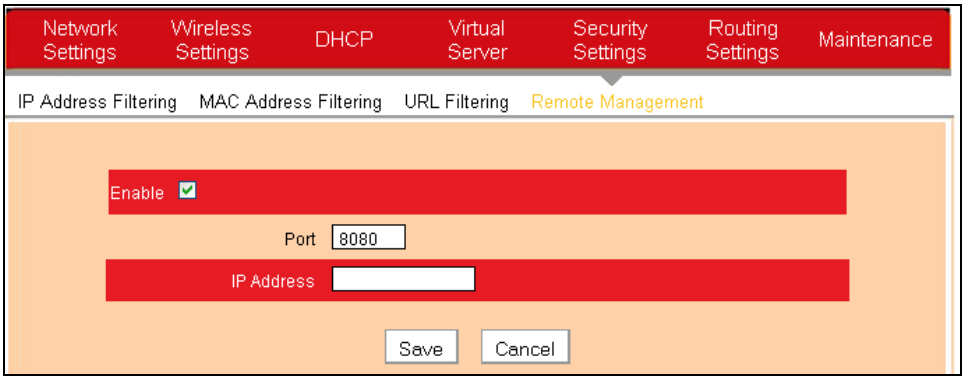
If you want to disallow all computers on your LAN to access "yahoo.com" at the time range of 8：00-18：00 from Monday to Friday, then do as follow.



⚠ **Note:** Each URL character string entry can corresponded to only a domain name. So you need to set multiple rules if you want to filter out multiple domain names**.**

8.4 Remote Management

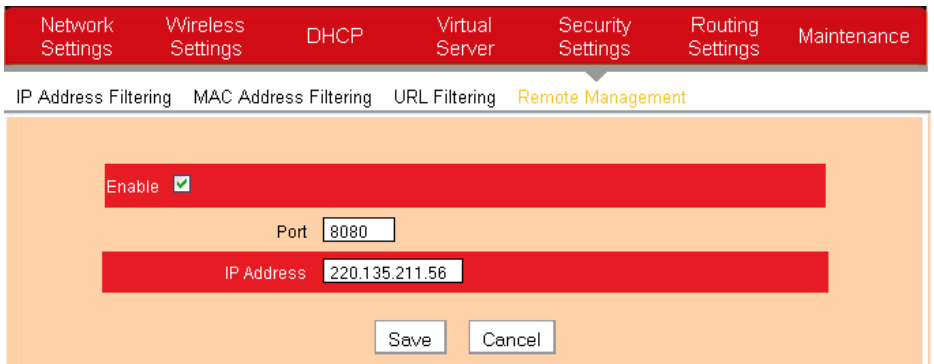
The Remote Web-based Management feature allows users to configure your router from Internet via a web browser.



● **Enable**: Check or uncheck to enable or disable the remote web-based management feature.
● **Port**: Enter a port number for remote web-based management.
● **IP Address**: Enter the IP address of a PC on Internet authorized to access and manage your router's web-based utility remotely.

⚠ **Note:** If you enter 0.0.0.0 in the IP address box, then all PCs on Internet can access your router's Web-based utility to view or change your settings remotely once you enable the remote Web-based management feature**.**

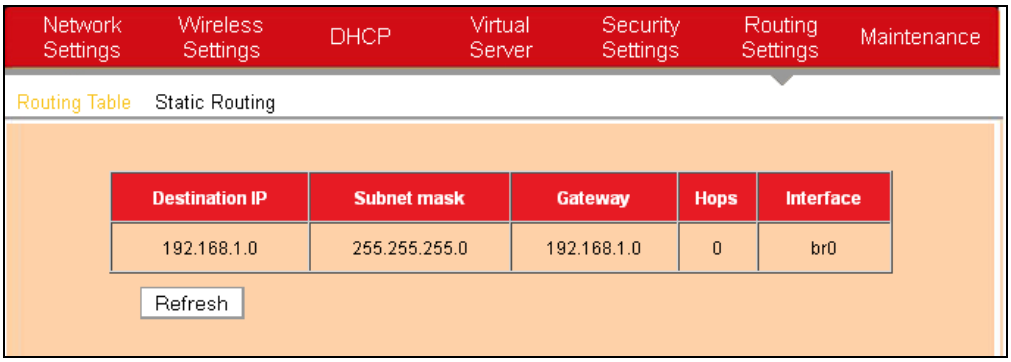
For example: If you want to allow only a PC at the IP address of 218.88.93.33 to access your router's web-based utility from Internet via port: 8080, you need to configure same settings shown in the diagram above on your router. And what this IP user needs to do is to simply launch a browser and enter http://220.135.211.56:8080 (provided that your router's WAN IP address is 220.135.211.56).



Chapter 9 Routing Settings

9.1 Routing Table

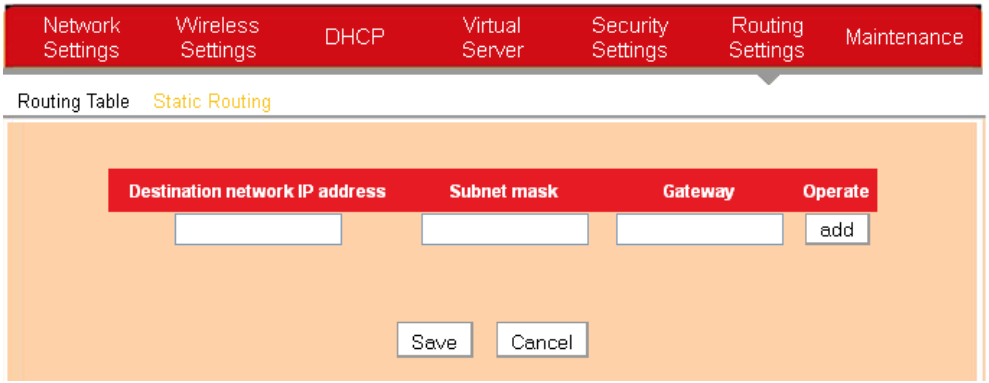
This page displays the router's core routing table which lists destination IP address, subnet mask, gateway, hop count and interface.



The principal task for a router is to look for an optimal transfer path for each data packet passing through it, and transfer it to the specified destination. So, it's essential for the router to select an optimal path, i.e. routing algorithm. To complete this work, the router stores related data of various transfer paths, i.e. establishing a routing table, for future route selection.

9.2 Static Routing

You can use this section to set up router's static routing feature.



● **Destination Network IP Address**: Enter a destination IP address or subnet.

● **Subnet Mask**: Enter a Subnet Mask that corresponds to destination IP address or subnet you entered.

● **Gateway**: Next-hop IP address.

⚠ **Note:**

1. Gateway IP address must be on the same subnet with the router's LAN/WAN IP address.

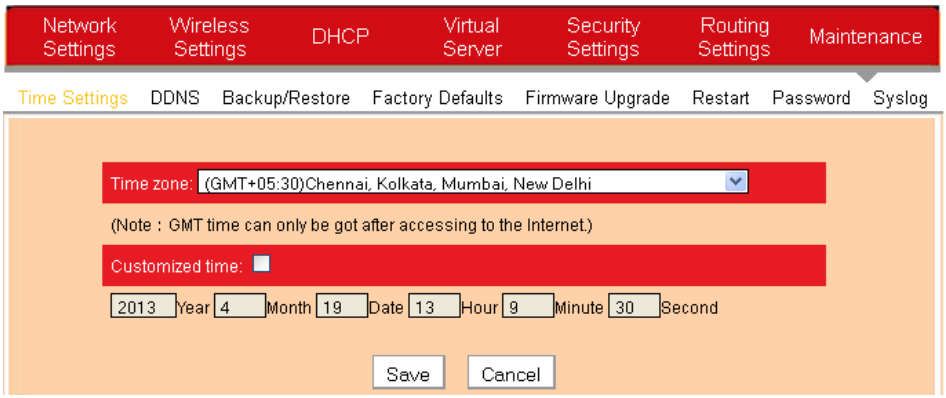
2. If you want destination network to be a single host, then you must enter an IP address thereof and 255.255.255.255 respectively in Destination Network IP Address and Subnet Mask boxes.

3. If you want destination network to be a network, then you must enter an IP address and a corresponding subnet mask value respectively in Destination Network IP Address and Subnet Mask boxes. For example, if you enter 10.0.0.0 in the IP address box, then corresponding subnet mask should be 255.0.0.0.

Chapter 10 Maintenance

10.1 Time Settings

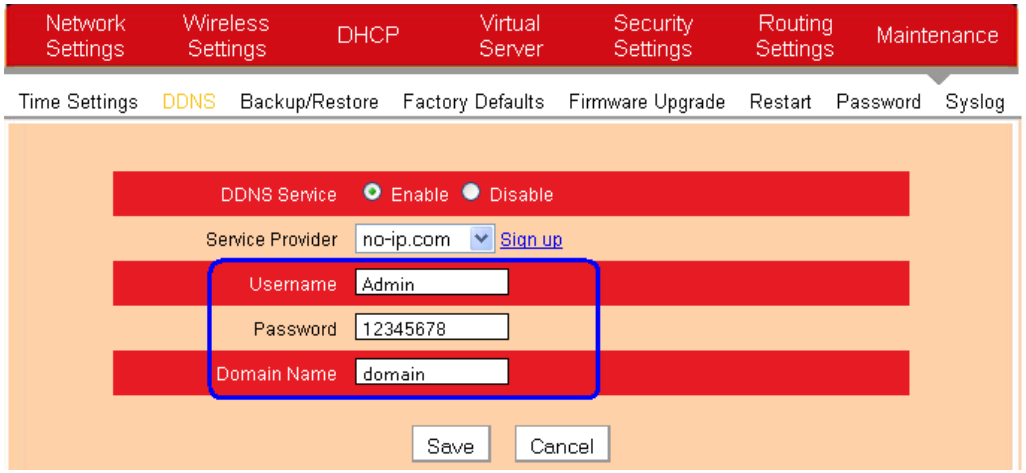
This section assists you in setting the device's system time; you can either select to set the time and date manually or automatically obtain the GMT time from Internet.



⚠ **Note**: The configured time settings lose once the router is powered off. But it obtains the GMT time automatically when you connect it to the Internet. Features/functions based on time (e.g. security settings) take effect only after time settings are configured manually or updated automatically from Internet.

10.2 **DDNS**

Dynamic DNS or DDNS is a term used for the updating in real time of Internet Domain Name System (DNS) name servers. We use a numeric IP address allocated by Internet Service Provider (ISP) to connect to Internet; the address may either be stable ("static"), or may change from one session on the Internet to the next ("dynamic"). However, a numeric address is inconvenient to remember; an address which changes unpredictably makes connection impossible. The DDNS provider allocates a static hostname to the user; whenever the user is allocated a new IP address this is communicated to the DDNS provider by software running on a computer or network device at that address; the provider distributes the association between the hostname and the address to the Internet's DNS servers so that they may resolve DNS queries. Thus, uninterrupted access to devices and services whose numeric IP address may change is maintained.



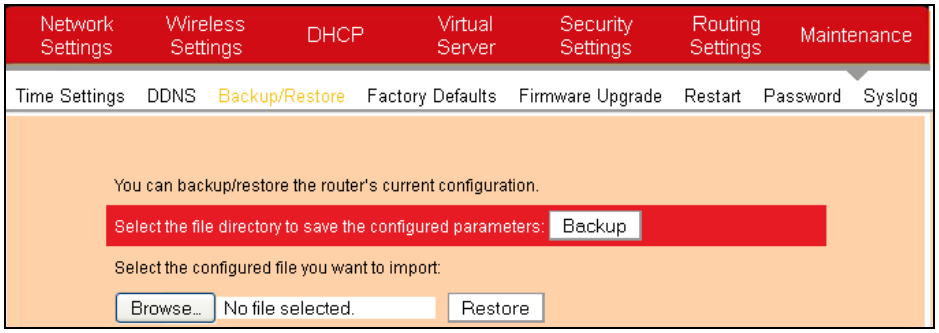
● **DDNS Service**: Click Enable or Disable radio button to enable/disable the DDNS feature.
● **Service Provider**: Select your DDNS service provider from the drop-down menu (Dyndns or no-ip).
● **Username**: Enter the DDNS username provided by your DDNS service provider.
● **Password**: Enter the DDNS password provided by your DDNS service provider.
● **Domain Name**: Enter the DDNS domain name distributed by your DDNS service provider.

Username	Admin
Password	12345678
Domain Name	domain.no-ip.com

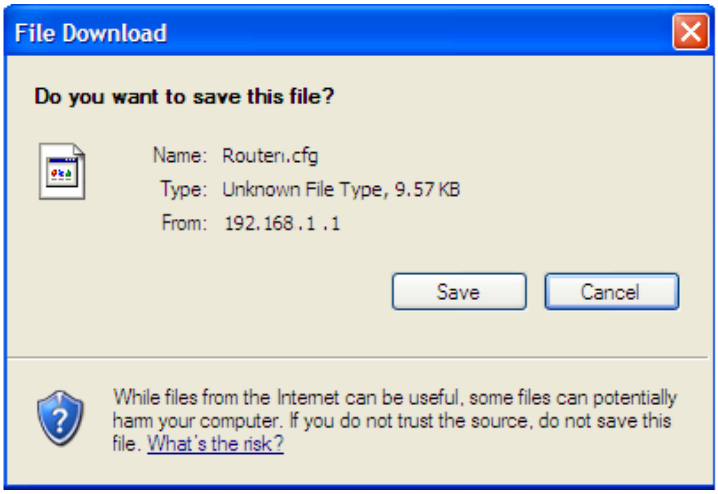
For example: If you have registered a DDNS service in no-ip.com and are allocated with domain, 12345678, domain.no-ip.com respectively as username, password and domain name for a web server on your PC at 192.168.1.10, then configure port settings on port range forwarding interface under virtual server menu and enter this information on the above DDNS interface. Others can access your web server by simply entering http://domain. no-ip.com in their browser address bar.

10.3 Backup/Restore

This section allows you to backup current settings or to restore the previous settings configured on the device.

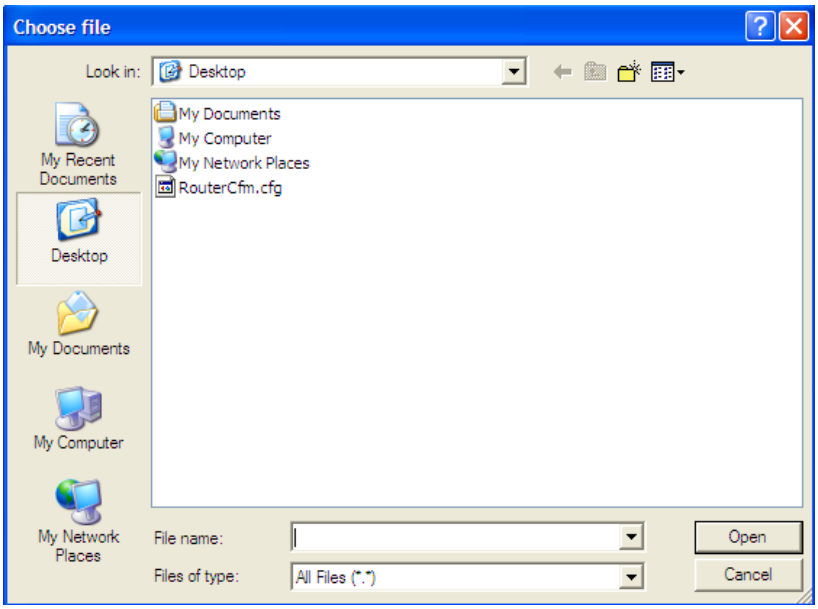


● **Backup** : Once you have configured the device the way you want it, you can save these settings to a configuration file on your local hard drive that can later be imported to your device in case that the device is restored to factory default settings. To do this, click the “Backup” button next to where it says “Select the file directory to save the configured parameters” on the screen above.

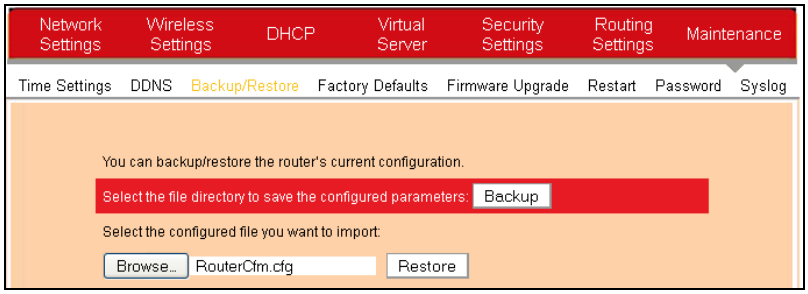


And then，click the “Save” button on the appearing screen above to store it under the selected path.

● **Restore** : Click the "Browse" button to locate and select a configuration file that is saved previously to your local hard drive.

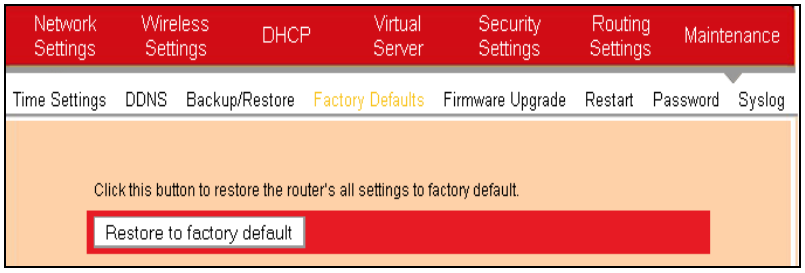


And then click the "Restore" button to reset your device to previous settings.



10.4 Factory Default

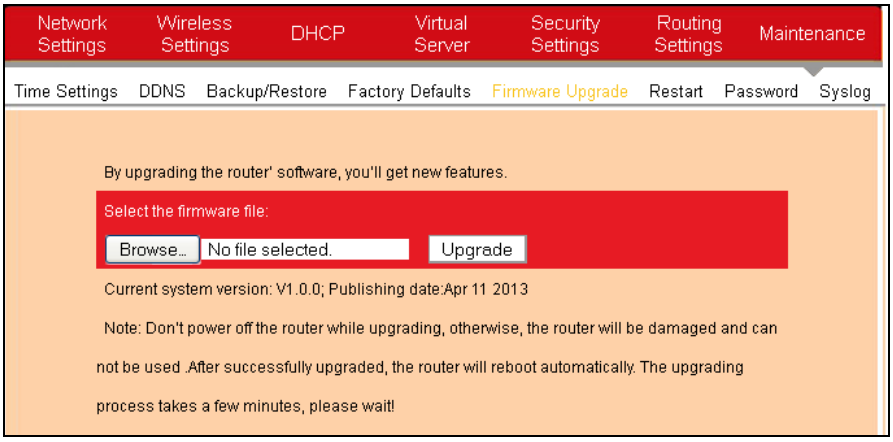
To restore all settings to the device's factory default values, click the "Restore to Factory Default" button on the interface below:



⚠ **Note:** To activate your settings, reboot the device after you reset it.

10.5 Firmware Upgrade

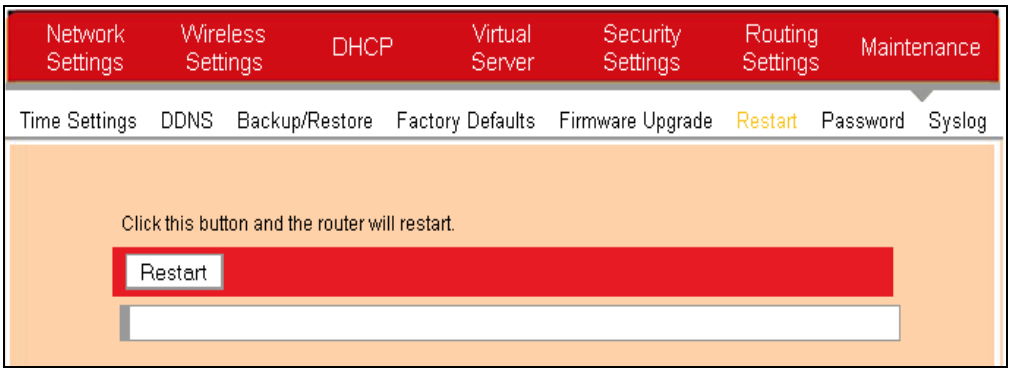
Firmware upgrade is released periodically to improve the functionality of your device and also to add new features. If you run into a problem with a specific feature of the device, log on to our website（www.iBallBaton.com）to download the latest firmware to update your device.



● **Browse**: Click this button to select an upgrade file.
● **Upgrade**: Click this button to start an upgrading process. After the upgrade is completed, the Router will reboot automatically.

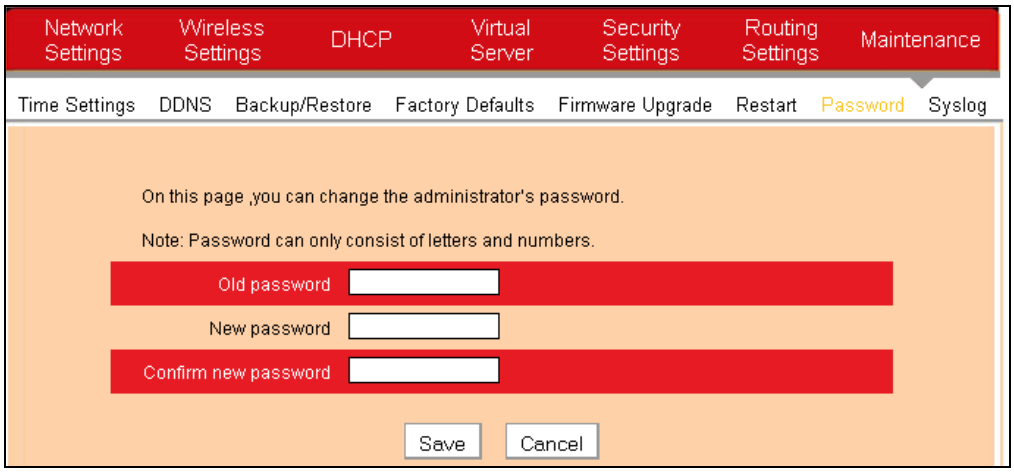
10.6 Restart

By Rebooting the device，new settings can be brought into effect. And WAN connection will be cut automatically during this process.



10.7 Password

This section allows you to change login password for accessing device's Web-based interface.

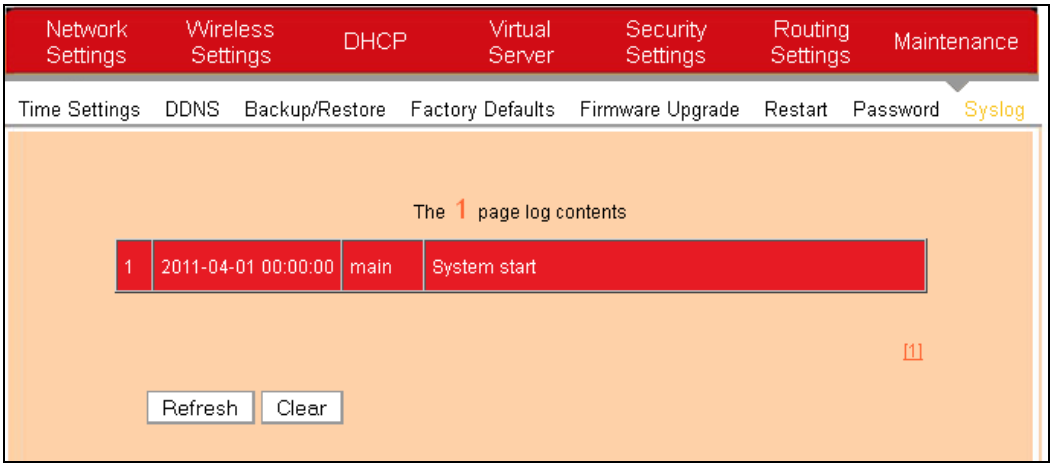


- **Old Password**: Enter the old password.
- **New Password**: Enter a new password.
- **Confirm new Password**: Re-enter the new password for confirmation.
- **OK**: Click it to save your new password.

⚠ **Note:** It is highly recommended that you change default login password.

10.8 SysLog

The Syslog option allows you to view all events that occur upon system startup and check whether there is attack present in your network.



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

Appendix 1: Glossary

Channel

A communication channel, also known as channel, refers either to a physical transmission medium such as a wire or to a logical connection over a multiplexed medium such as a radio channel. It is used to transfer an information signal, such as a digital bit stream, from one or more transmitters to one or more receivers.

If there are several APs coexisting in the same area, it is recommended that you configure a different channel for each AP to minimize the interference between neighboring APs. For example, if 3 American- standard APs (i.e. adopts 11 channels) coexist in one area, you can setup their channels respectively to 1, 6 and 11 to avoid mutual interference.

SSID

Service set identifier (SSID) is used to identify a particular 802.11 wireless LAN. It is the name of a specific wireless network. To let your wireless network adapter roam among different APs, you must set all Aps' SSID to the same name.

WPA/WPA2

The WPA protocol implements the majority of the IEEE 802.11i standard. It enhances data encryption through the Temporal Key Integrity Protocol (TKIP) which is a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet. WPA also includes a message integrity check feature to prevent data packets from being hampered with. Only authorized network users can access the wireless network.

The later WPA2 protocol features compliance with the full IEEE 802.11i standard and uses Advanced Encryption Standard (AES) in addition to TKIP encryption protocol to guarantee better security than that provided by WEP or WPA.

Appendix 3: Troubleshooting

1. **Q**: I entered the device's LAN IP address in the web browser but cannot access the utility. What should I do?

   A: 1) Verify whether the device functions correctly. Sys LED should blink several seconds after you power on the device. If not, then internal malfunction may have occurred; Please contact our technical support for help.

   2) Verify physical connectivity by checking if corresponding port's link LED lights up. If not, try a different cable.

   3) Click "Start" -- "Run", enter "cmd" and then "ping 192.168.1.1"on appearing CLI to diagnose whether your PC has connected to the device or not. If ping succeeds, then check whether the Proxy Server feature is enabled on your browser. If enabled, disable it immediately. In case that ping fails, press and hold the "RESET" button on your device for over 7 seconds to restore factory default settings, and then run "ping192.168.1.1" again.

   4) Contact our technical support for help if the problem still exists after you tried all the above.

2. **Q**: I forget the login password to my device, what should I do?

   A: In this case, you need to restore your device to factory default settings. To do so, Press the hardware button RESET on your device for about 7 seconds and then release.

3. **Q**: My computer shows an IP address conflict error after having connected to the device. What should I do?

   A: 1) Check if there are other DHCP servers present in your LAN. If there are other DHCP servers except your router, disable them immediately.

   2) The default IP address of the device is 192.168.1.1; make sure this address is not used by another pc or device. In case that two computers or devices share the same IP addresses, change either to a different address.

4. **Q**: I cannot access Internet and send/receive emails; what should I do?

   A: This problem mainly happens to users using ADSL dialup or dynamic IP internet connection types. In this case, go to “WAN Settings” to change the MTU value from default 1492 to 1450 or 1400, etc.

5. **Q**: How do I share resources on my computer with users on Internet through the device?

   A: To let Internet users access internal servers on your LAN such as e-mail server, Web, FTP, via the device, use the “Virtual Server” feature. To do so, follow steps below:

Step 1: Create your internal server, make sure the LAN users can access these servers and you need to know related service ports, for example, Web server’s port is 80; FTP is 21; SMTP is 25 and POP3 is 110.

Step 2: Click “Virtual Server” and select “Port Forwarding” on the Router’s web interface.

Step 3: Input the external service port ID, for example, 80.

Step 4: Input the internal Web service port ID, for example, 80.

Step 5: Input the internal server’s IP address. For example, if your Web server’s IP address is 192.168. 1.10 please input it.

Step 6: Select a communication protocol used by your internal host: TCP, UDP or ICMP.

Step 7: Click “OK” to activate the settings.

Server	Protocol	Service Port ID
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
Iphone5.0	TCP	22555
SMTP	TCP	25
POP3	TCP	110

COPYRIGHT & TRADEMARKS

Note: For any technical help on iBall Baton products please contact support@iballbaton.com

www.iBallBaton.com