NetMASTER
KABLO MODEM

WDS-150
WIRELESS AP-ROUTER

User's Manual

TEKNOTEL

Teknotel Bilişim Ürünleri Ltd.Şti.

June 2012

Contents

Package Contents

Thank you for purchasing 802.11n Wireless Router. Please check all the contents of this package.

The product package should include the following:

1. One Wireless Router
2. One power adapter
3. CD (containing User's Manual)
4. Quick Installation Guide

Description

The 802.11n Wireless Router is compatible with IEEE802.11n standard, which supports data rate up to 150 Mbps in 2.4 GHz band, which is also compatible with IEEE 802.11g/b wireless devices. The Wireless router allows multiple users to share one broadband connection, as well as secures your private network. With its built-in 4-port switch and wireless AP, LAN users can share files, and playing network games all at a high speed.

To provide a secure wireless network, this Wireless router supports wireless data encryption with 64/128-bit WEP, WPA and WPA2. Network Address Translation (NAT) Firewall is also support to shield your communications and network from hackers and wireless eavesdroppers.

The Wireless Router built-in with 4-port 10/100Mbps Fast Ethernet Switch is the latest generation of Wireless router product for Home/Office and SOHO users. This full-feature and self-contained compact Wireless Router will be fully for broadband access in both of LAN and Wireless environment. This device has been specifically designed to provide LAN and Wireless users the most cost-effective method with multiple accesses to the Internet at the cost of a single public IP address (IP Sharing)and enjoy the true Plug-and-Play installation. Moreover, the built-in 4-port 10/100Mbps switch lets users plug the network cable into the device without buying additional switch.

This device is also an Access Point. It has a built-in wireless LAN. Users can connect to Internet using wireless network interfaces anywhere within the range of its radio transmission. It's ideal for SOHO users who require instant and convenient access to Internet without the restriction of connecting cables

1.3 Key Features

The switch provides the following key features:

- Complies with 2.4GHz IEEE802.11n Draft v2.0 and backward compatible with IEEE 802.11b/g standards
- Supports NAT/NAPT IP sharing
- WAN Protocols: PPPoE/Static IP/PPTP/DHCP
- Supports advanced 1T1R MIMO technology to enhance the throughput and coverage range significantly
- High speed data rate - up to 150Mbps
- Supports Virtual Server and DMZ
- Supports Wi-Fi Protected Setup (WPS) with reset button
- Supports 64/128-bit WEP encryption and WPA-PSK, WPA2-PSK security

- Supports WMM function to meet the multimedia transmission requirement
- Supports WDS mode
- Supports Special Applications (Port Triggers)
- Supports DDNS (DynDNS, TZO), and QoS
- Supports MAC/IP filtering and URL blocking
- Supports DHCP server and Anti-Dos firewall
- Web user interface (remote configuration)
- System status and security log
- Firmware upgradeable

1.4 Specification

Standards	IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u, CSMA/CA, CSMA/CD, TCP/IP, DHCP, ICMP, NAT, PPPoE
Interface Type	4 x 10/100M RJ45 Port（Auto MDI/MDIX）
	1 x 10/100M RJ45Port（Auto MDI/MDIX）
Frequency range	2.4~2.4835GHz
Radio Data Rate	11n: 270/243/216/162/108/81/54/27Mbps 135/121.5/108/81/54/40.5/27/13.5Mbps 130/117/104/78/52/39/26/13Mbps; 65/58.5/52/39/26/19.5/13/6.5Mbps
	11g: 54/48/36/24/18/12/9/6M
	11b: 11/5.5/2/1M
Channel	13
Sensitivity @PER	270M: -68dBm@10% PER; 130M: -68dBm@10% PER; 108M: -68dBm@10% PER; 54M: -68dBm@10% PER 11M: -85dBm@8% PER; 6M: -88dBm@10% PER 1M: -90dBm@8% PER
RF Power	20dBm（Max）
Antenna Type	5DBI antennas
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m) 100BASE-TX: UTP category 5, 5e cable (maximum 100m)
LEDs	Power, M1, WAN，WLAN, 1,2,3,4
Dimensions	186.2mm x 119.7mm x 26.5mm
Power Supply	DC 9V 800mA
Environmental and Physical	
Operating Temp	0℃~40℃ (32℉~104℉)
Operating Humidity	10% - 95% RH, Non-condensing

Hardware installation

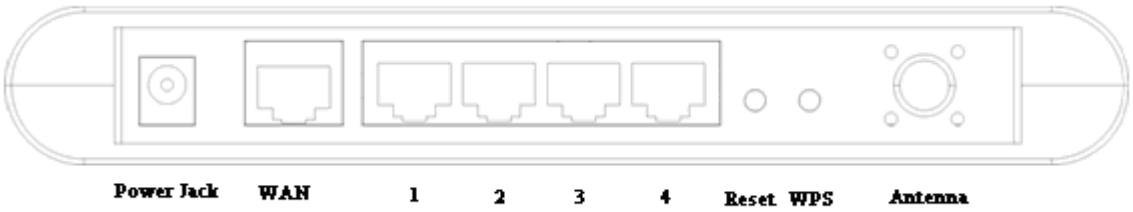
The Front Panel

The front panel of the 802.11n Wireless Router consists of several LED indicators, which is designed to indicate connections. Viewed from left to right. The table describes the LEDs on the front panel of the router.

Name	Action	Description
Power	OFF	No Power
	ON	Power on
SYS	ON	The router is initializing
	Flashing	The router is working properly
	OFF	The router has a hardware error
WLAN	On	The Wireless Radio function is enabled
	Flashing	The Wireless Radio function is transmitting data.
SEC	ON	Security Protect On
WAN	OFF	There is no WAN linked to the corresponding port
	ON	There is a device linked to the corresponding port but no activity
	Flashing	There is an active device linked to the corresponding port
1/2/3/4	OFF	There is no device linked to the corresponding port
	ON	There is a device linked to the corresponding port but no activity
	Flashing	There is an active device linked to the corresponding port

2.2 The Rear Panel

The rear panel contains the following features. (Viewed from left to right:)



Rear Panel 1

1. Wireless antenna

2. WAN RJ45 port for connecting the router to a cable, DSL modem or Ethernet
3. Four LAN 10/100Mbps RJ45 ports for connecting the router to the local PCs or switches.
4. DC power jack: For the power adapter
5. Factory Default Reset button

Factory defaults:

1. turn on the router's power.
2. press and hold the default reset button until the system LED lights up(about 5 seconds).
3. release the reset button and wait for the router to reboot.

System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable modem that has an RJ45 connector (you do not need it if you connect the router to Ethernet)
- Each PC on the LAN needs a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- TCP/IP protocol must be installed on each PC
- Web browser, such as Microsoft Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later

3.4 Hardware installation

This Chapter provides a step-by-step guide to the installation and configuration of the Wireless Router. It is strongly suggested to go over the whole chapter before installation.

3.1 Network configuration

- Connect the ADSL or Cable modem to the Ethernet WAN port on the back of the Wireless Router by using the UTP cable.

- Connect the phone line from the wall socket to the line-in port on the ADSL modem, or the coaxial cable to the line-in port on the Cable modem.

- Plug-in the power adapter to the modem and turn on the power. Install the Ethernet card into the computer by referring to the User Guide that came with the card.

- Connect the computer to the Wireless Router by using standard twisted-pair Ethernet cable from the computer’s Ethernet card to an 10/100Mbps Ethernet

port on the back of the Wireless Router.

 Plug-in the power adapter to the Router and the other side to the wall outlet.

Computer configuration

In order to communicate with this Wireless Router, you have to configure the IP addresses of your computer to be compatible with the device. The router supports DHCP server and it is enabled as default. Users that configure your IP address as **"Obtain an IP address automatically"** may skip the following IP configuration instruction.

Note:

1. The default network setting of the device:

   IP address: 192.168.1.1

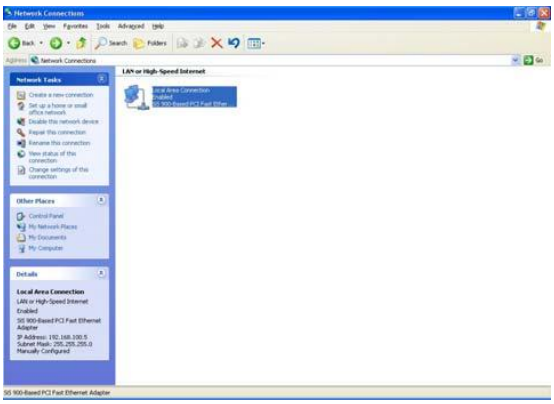
   Subnet Mask: 255.255.255.0

   DHCP Server: enabled

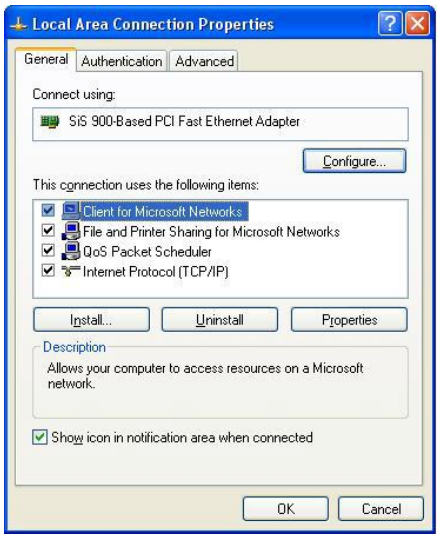
2. In the following TCP/IP configuration guide, the IP address "192.168.1.2" is assumed to be your IP address if you want to specify IP addresses manually. Please **DO NOT** choose "192.168.1.1" for the IP address (192.168.1.1) has been set as the default IP for this device.
3. The following TCP/IP configuration guide uses windows XP as the presumed operation system.

3.3 Procedures to configure IP addresses for your computer

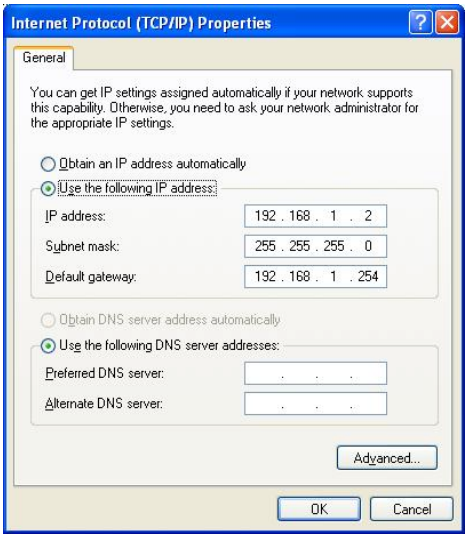
1. If you are in Classic Start menu view, click **Start > Settings > Control Panel > Network Connections**. If you are in Start menu view, click **Start > Control Panel > Network Connections.**
2. Double click **Local Area Connection**.



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



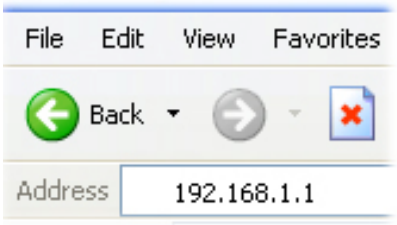
4. You may choose “Obtain an IP address automatically”(recommend) to get IP address automatically or choose “Use the following IP address” to specify IP addresses manually. Please click the **OK** button after your configuration.

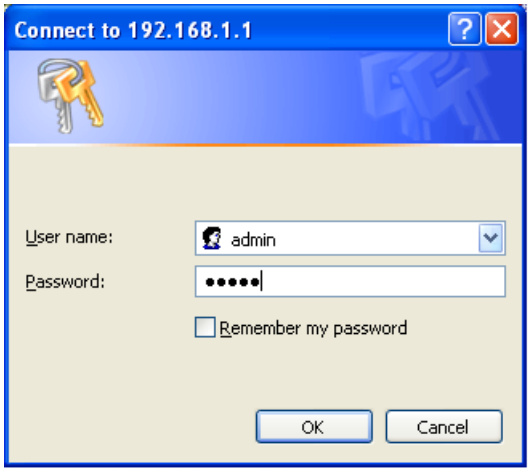


Wireless Router configuration

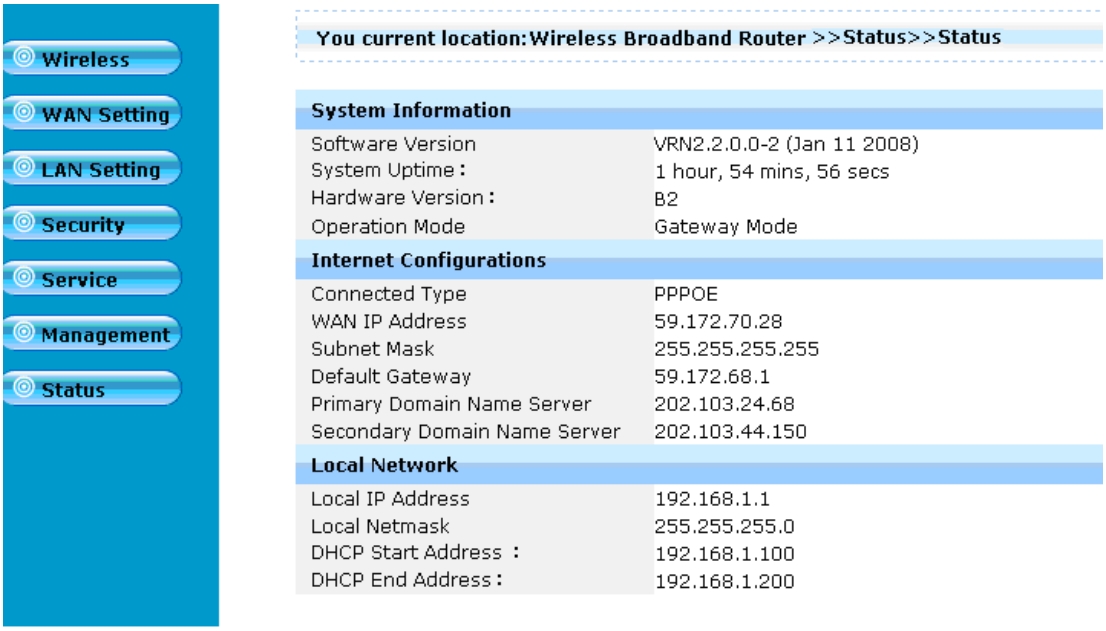
This product provides Web based configuration scheme, which is, configuring by Netscape Communicator or Internet Explorer. Take example for Microsoft Internet Explorer.

1. Activate your browser, select Tools, point to Internet option, click connect, select dial-up network never, affirm inspect setting automatically, configure scrip automatically and use agency server on LAN setting notto be selected.
2. Type http://192.168.1.1 in Address field and press Enter. Key in the user name and password (if you use it first, you can type the factory default setting .User name is admin and password is admin), click on the OK button.





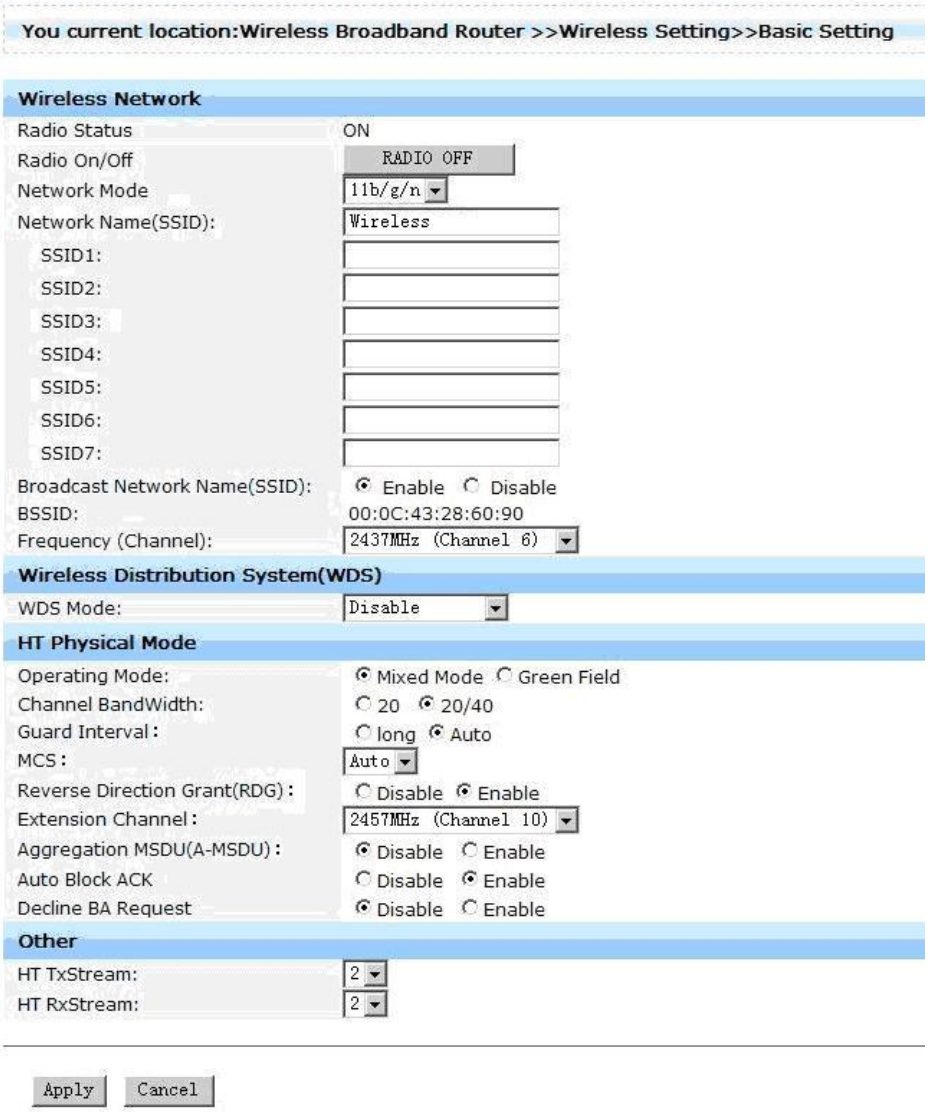
After login successfully, web-configuration will be displayed.



4.2 Wireless Settings

4.2.1 Basic Settings

You can set up the configuration of your Wireless and monitor the Wireless Clients associate with your AP.



1 **Radio Status:** The Status of Wireless.

2 **Radio On/Off:** Click the button to enable the wireless function. If you want to use wireless, click the button 'Radio On', and if you don't want to use wireless, click the button 'Radio off'.

3 **Network mode:** Select one of the following: **11g** - Select if all of your wireless clients are 802.11g. **11b/g** - Select if you are using both 802.11b and 802.11g wireless clients. **11b** - Select if all of your wireless clients are 802.11b. **11b/g/n** - Select if you are using a mix of 802.11n, 11g, and 11b wireless clients.

4 **Network Name(SSID)**: Service Set Identifier (SSID) is the name of your wireless network.. You can use more than one SSID , but less than eight. Create a name using up to 32 characters. The SSID is case-sensitive.

5 **Broadcast Network Name(SSID): Enable** is the default setting. Choose **Enable** to broadcast the SSID across the network. All devices on a network must share the same SSID (Service Set Identifier) to establish communication. Choose **Disable** if you do not wish to broadcast the SSID over the network.

6 **BSSID**: The value of BSSID.

7 **Frequency(Channel)**: Indicates the channel setting for the Wireless Router. By default the channel is set to 1. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable **Auto Channel Scan**, this **Extension Channel** will be greyed out.

8 WDS Mode: WDS is commonly used in areas requiring multiple **AP**s, where wiring is not possible or costly and for providing back-up paths between **AP**s. The number of ports on an AP available for the WDS is dependent on the **AP** model.

Disable – select if there is only one Lan and the range of wireless cover is enough.

Lazy Mode - select if you don't known the **AP MAC Address** on other **AP**s, but you must select the **Phy Mode** and **EncrypType** which is the same as other **AP**s.

Bridge Mode – select if you two different Lan in network, and want to link together. Of course, you need to select the **Phy Mode** and **Encryp Type** in the same mode as **Lazy Mode**, and need the **AP MAC Address** too, there you can use fill **AP MAC Address. Repeater Mode** – select if you want to extend the lan range. Of course, you need to select the **Phy Mode** and **EncrypType** in the same mode as **Lazy Mode**, and need the **AP MAC Address** too, there you can use fill **AP MAC Address.**

9 **Operating Mode:** This is the default setting Mixed Mode，or setting Green Field;

10 **Channel BandWidth:** Select the Channel Width: **20/40 -** This is the default setting. Select if you are using both 802.11n and non-802.11n wireless devices.

11 **Guard Interval: Auto** – check if reduce the guard interval time therefore increasing the data capacity. However, it's less reliable and may create higher data loss. Reverse if check the **long.**

12 **MCS**: This is the default setting Auto Mode

13 **Reverse Direction Grant(RDG)**: **Enable** - facilitate increased communication channel bandwidth efficiency in association with scheduled time periods that allocate channel access to particular stations. According to various aspects, systems and methods are described that facilitate providing and/or utilizing reverse direction grants in connection with scheduled channel access. It can mitigate an amount of unused channel access time after a station completes data transmission prior to an end of the allocated period. **Disable** – select if you don't need this function.

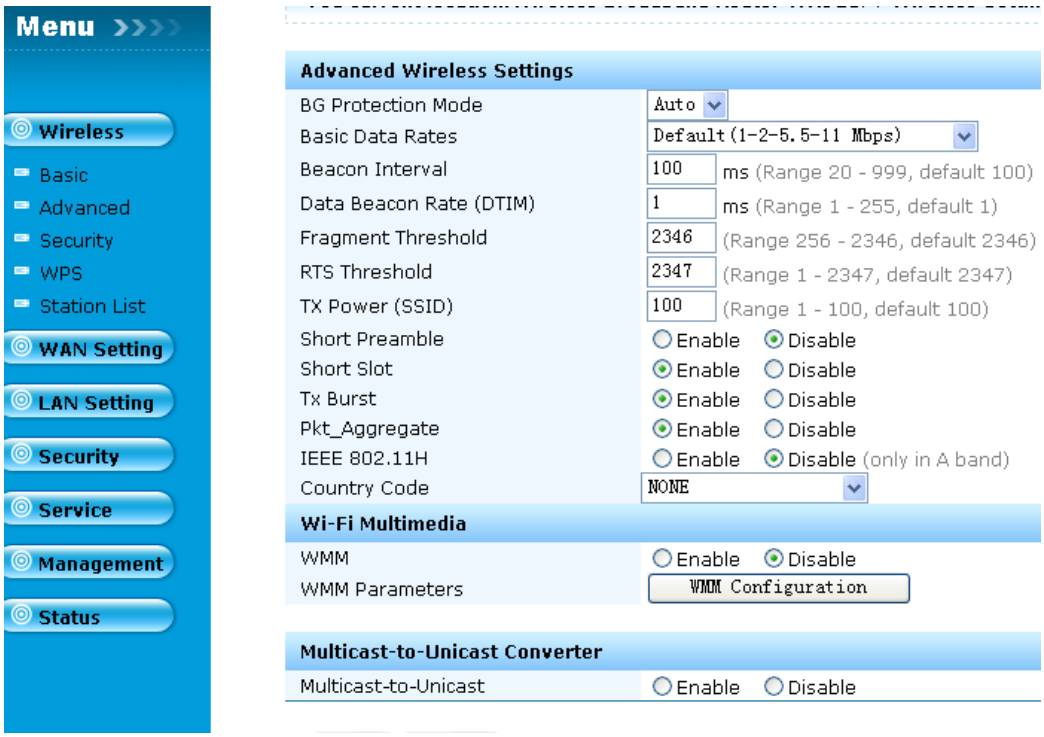
14 **Extension Channel:** If the **Frequency(Channel)** select is not **autoselect** , the **Extension Channel** is enable. You can select the **Extension Channel** you want to. It can help speed recovery.

15 **Aggregation MSDU(A-MSDU):**

16 **Auto Block ACK: Enable** – select if you want to block ACK automally. Or else you can select **Disable**.
17 **Decline BA Request: Enable** – select if you want to Decline BA Request. Or else you can select **Disable**.

4.2.2 Advance

You can set advanced wireless LAN parameters of this router. We recommend not changing these parameters unless you know what changes will be there on this router.

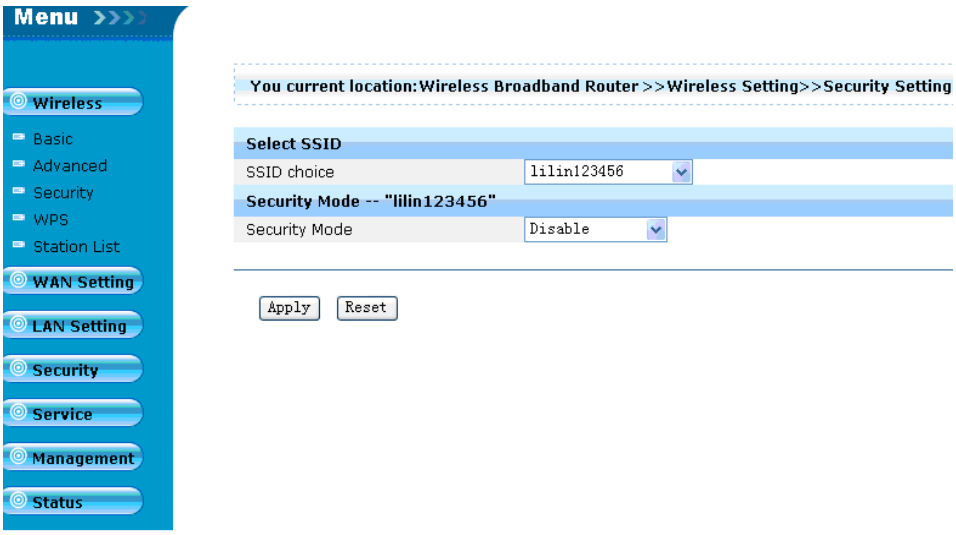


1 **BG Protection Mode:** Select either **Auto On** or **Off**. Default is **Auto**
2 **Basic Data Rates:** Select the data rate. Default is 1-2-5.5-11-22-54Mbps
3 **Beacon Interval:** Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. 100 is the default setting and is recommended.
4 **Data Beacon Rate (DTIM)**: (Delivery Traffic Indication Message) 1 is the default setting. A DTIM is a countdown informing clients of the next page for listening to broadcast and multicast messages.
5 **Fragment Threshold:** The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.
6 **RTS Threshold:** This value should remain at its default setting of 2432. If inconsistent data flow is a problem, only a minor modification should be made.

7 **TX Power (SSID):** Set the transmit power of the antennas.
8 **Short Preamble:** Check this box to reduce the guard interval packet therefore increasing the data capacity. However, it's less reliable and may create higher data loss.
9 **Short Slot:** Check this box to reduce the guard interval time therefore increasing the data capacity. However, it's less reliable and may create higher data loss.
10 **Tx Burst:** Click either **Enable** or **Disable**. Default is **Enable.**
11 **Pkt_Aggregate:** if Click **Enable**, the packets will be Aggregated before they sent. Click either **Enable** or **Disable**. Default is **Enable.**
12 **IEEE 802.11H:** This enables 802.11h opration. 802.11h is a wireless specification developed to allow implementation of wireless networks in countries that cannot use the 802.11 standard. This feature should only be enabled if you are in a country that requires it. Click either **Enable** or **Disable**. Default is **Disable.** only in A band
13 **Country Code**: Here you can select the Country Code.
14 **WMM:** WMM is QoS for your wireless network. Enable this option to improve the quality of video and voice applications for your wireless clients.
15 **WMM Parameters:** Click this button, you will see the configuration of the WMM which in another page. In the page, you can configure the parameters of WMM.
16 **Multicast-to-Unicast**: **Enable** – select if allow multicast traffic to pass through the router from the Internet. **Disable** – select if not allow.

4.2.3 Security

It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

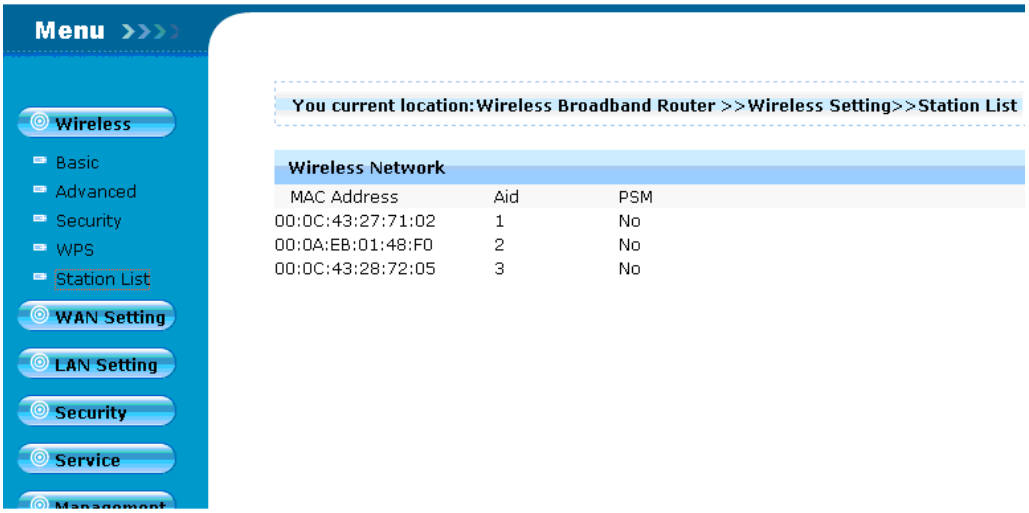


1 **SSID choice:** select the SSID which you want to set its **Security Mode**.
2 **Security Mode:** set the security mode at the SSID which you select. There are nine modes for you select. Whatever you select, the page will show you what parameters you configuration**,** Refer to page 60 for more information regarding wireless security.

4.2.4 WPS

1 **WPS: Enable** – select if you want to make the WPS enable. If you don't need, select disable and click **Apply** button. The follow display the setting and status of WPS.
2 **WPS mode:** the mode of WPS, if you select **PIN** button, you need a PIN, or else, you select the **PBC** button. And then click **Apply** button.
3 **WPS Status**: the status log of WPS.

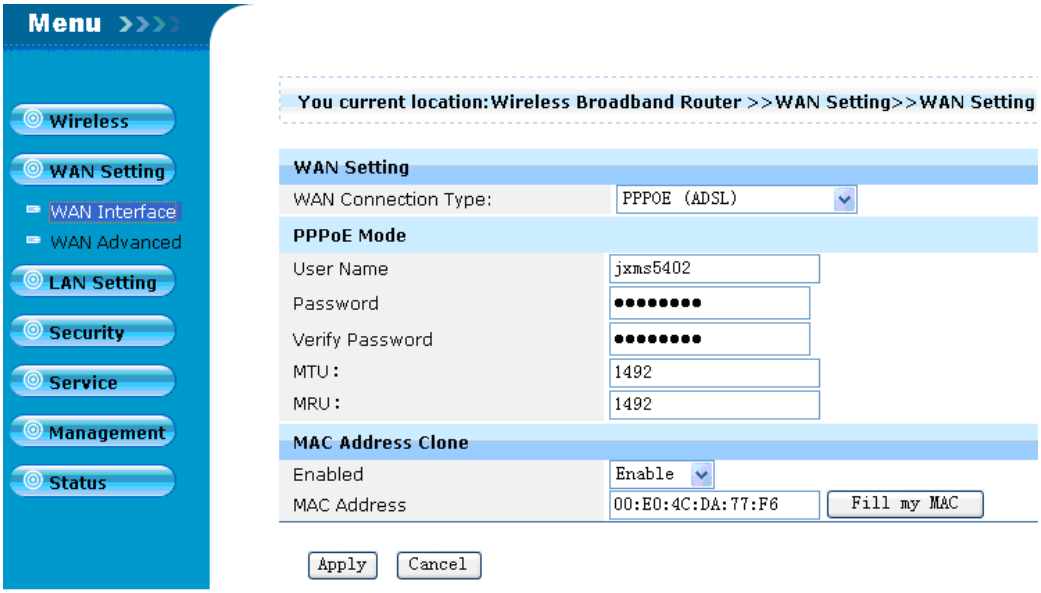
4.2.5 Station List



In this page, you can see the staus station list of the wireless network, which display MAC Address, Aid , PSM.

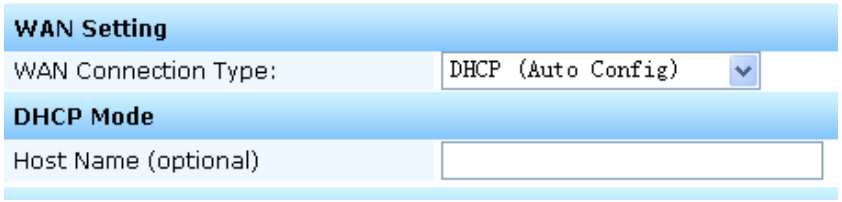
4.3 WAN Setting

4.3.1 WAN Interface

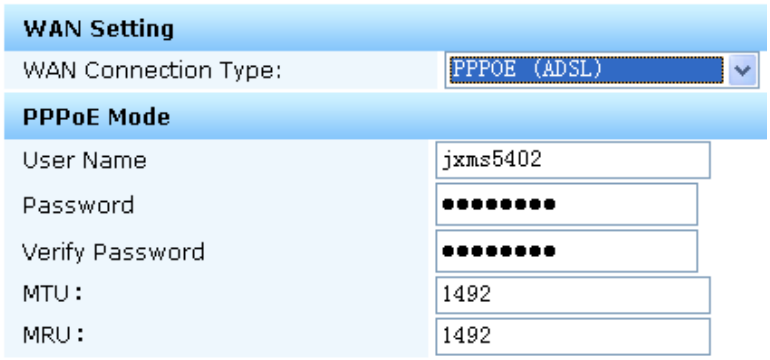


1 **WAN Connection Type:** the connection mode of WAN port. There are five choice you can selest.

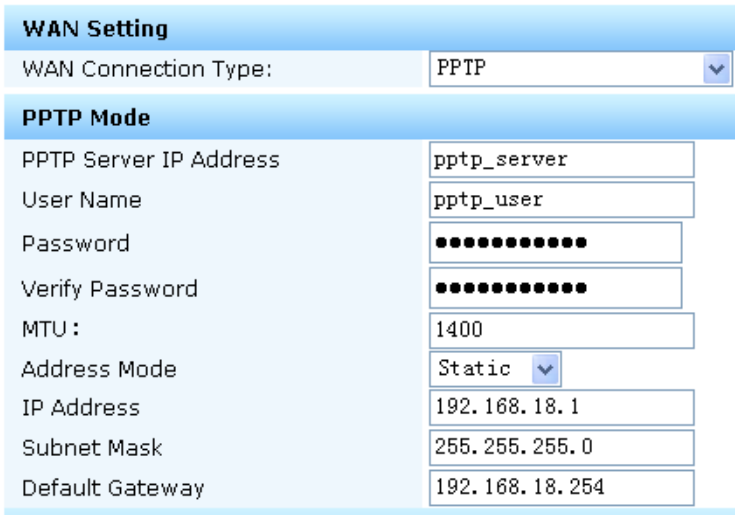
If you select **DHCP (Auto Config)**, information automatically from your ISP. Select this option if your ISP does not give you any IP numbers to use. This option is commonly used for Cable modem services. **Host Name (optional)**: The Host Name is optional but may be required by some ISPs.



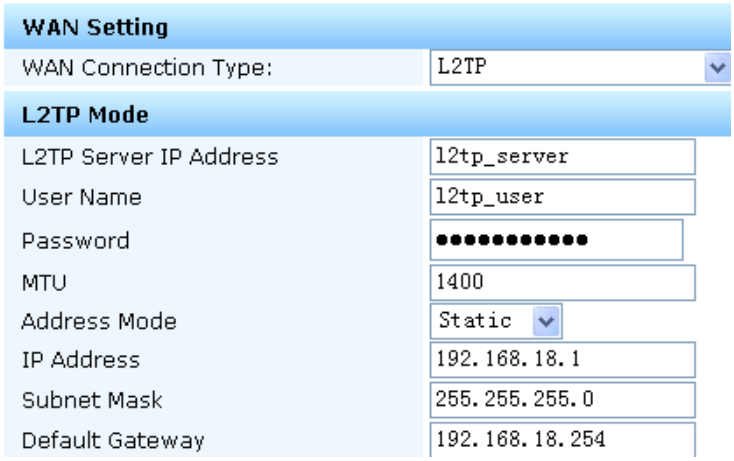
Choose **PPPoE** (Point to Point Protocol over Ethernet) if your ISP uses a PPPoE connection. Your ISP will provide you with a username and password. This option is typically used for DSL services. Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router. **User Name**: Enter your PPPoE user name. **Password:** Enter your PPPoE password and then retype the password in the next box. **MTU**: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1492 is the default MTU. **MRU**: Maximum Receive Unit - you may need to change the MRU for optimal performance with your specific ISP. 1492 is the default MTU.



Choose **PPTP** (Point-to-Point-Tunneling Protocol) if your ISP uses a PPTP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services. **PPTP Server IP Address**: Enter the Server IP provided by your ISP (optional).. **User Name**: Enter your PPTP username. **Password**: Enter your PPTP password and then retype the password in the next box. **MTU**: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1492 is the default MTU. **Address Mode**: Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic**. **IP Address**: Enter the IP address (Static PPTP only). **Subnet Mask**: Enter the Primary and Secondary DNS Server Addresses (Static PPTP only). **Default Gateway:** Enter the Gateway IP Address provided by your ISP.

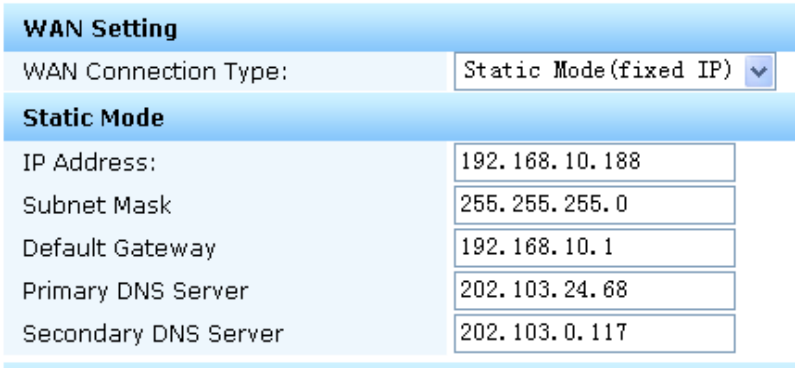


Choose L2TP (Layer 2 Tunneling Protocol) if your ISP uses a L2TP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services. **L2TP Server IP Address**: Enter the Server IP provided by your ISP (optional). **User Name**: Enter your L2TP username. **Password**: Enter your L2TP password and then retype the password in the next box. **MTU**: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1492 is the default MTU. **Address Mode**: Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic**. **IP Address**: Enter the L2TP IP address supplied by your ISP (Static only). **Subnet Mask**: Enter the Subnet Mask supplied by your ISP (Static only). **Default Gateway**: Enter the Gateway IP Address provided by your ISP.



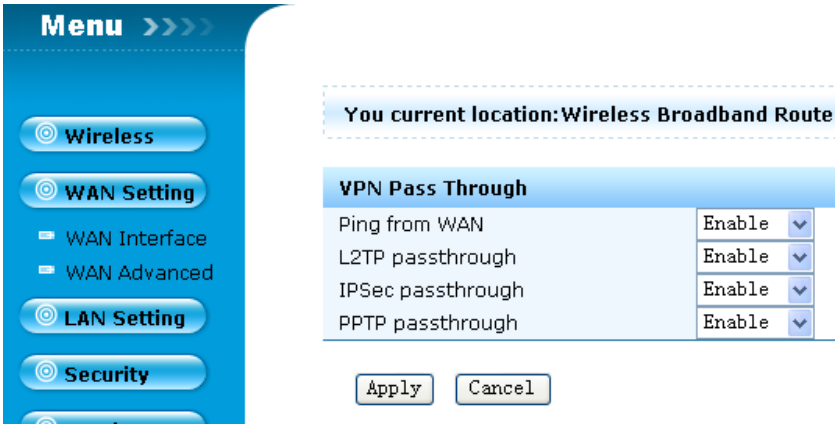
Select Static IP Address if all the Internet port's IP information is provided to you by your ISP. You will need to enter in the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format. **IP Address:** Enter the IP address assigned by your ISP. **Subnet Mask:** Enter the Subnet Mask assigned by your ISP. **Default Gateway:** Enter the Gateway assigned by your ISP. **Primary DNS Server**: The DNS

server information will be supplied by your ISP (Internet Service Provider.). **Secondary DNS Server:** The DNS server information will be supplied by your ISP (Internet Service Provider.).



2 **Enabled: Enable** – select if you want to clone the wan port MAC Address.
3 **MAC Address**: fill the MAC Address you want to clone. Also you can click **Fill my MAC** button to fill you PC's MAC Address automally.

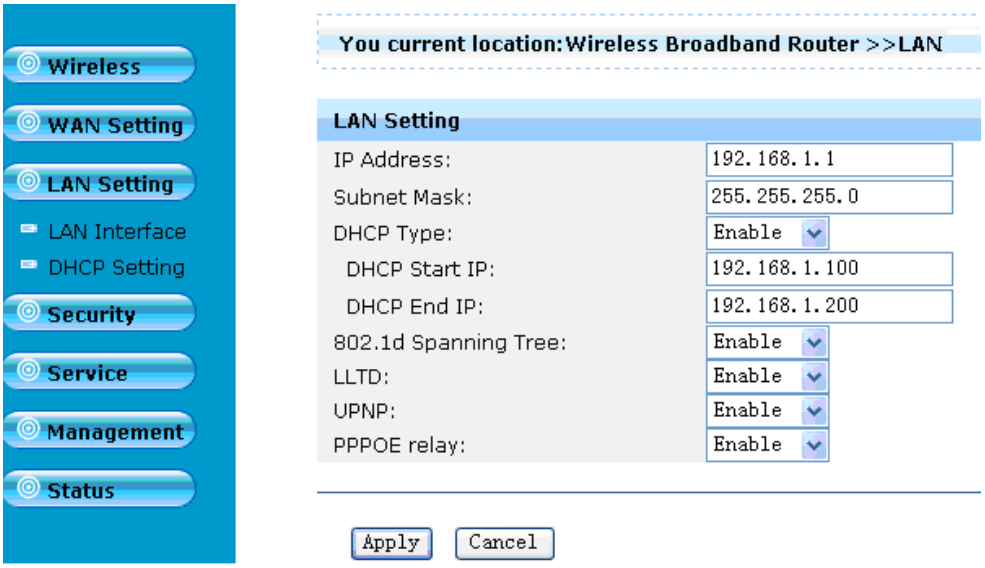
4.3.2 WAN Advanced



1 **Ping from WAN: Enable** – select if you want to ping wan ip from external network.
2 **L2TP passthrough: Enable** – select if you want to let the L2TP packet pass through the Wireless Router from wan port.
3 **IPSec passthrough: Enable** – select if you want to let the IPSEC packet pass through the Wireless Router from wan port.
4 **PPTP passthrough: Enable** – select if you want to let the PPTP packet pass through the Wireless Router from wan port.

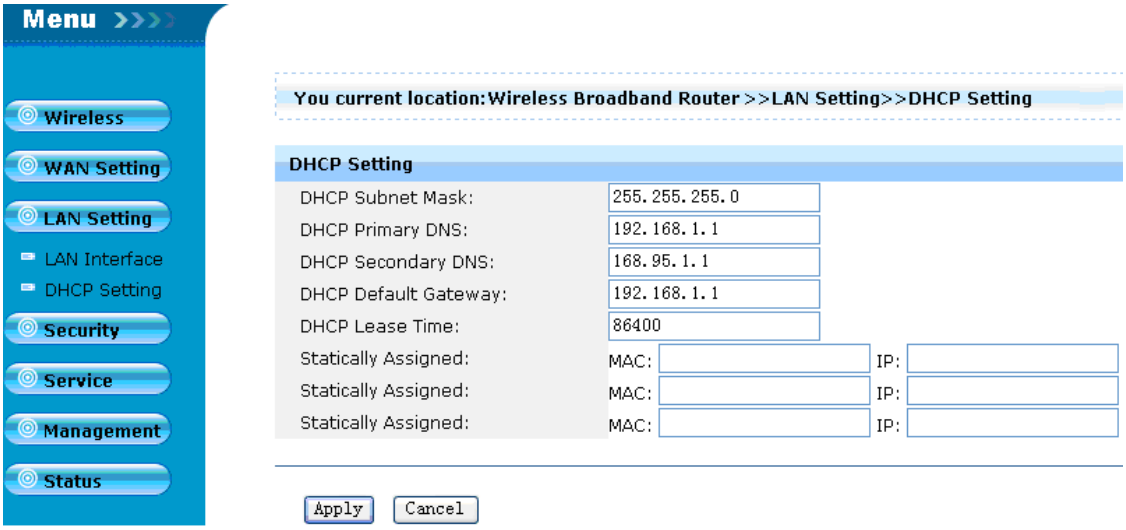
4.4 LAN Setting

4.4.1 LAN Interface



1 **IP Address:** the IP of Lan.
2 **Subnet Mask:** the subnet mask of Lan.
3 **DHCP Type**: **Enable** – select if you want to use the Wireless Router as a DHCP server. And then Enter the starting and ending IP addresses for the DHCP server's IP assignment.
Note: If you statically (manually) assign IP addresses to your computers or devices, make sure the IP addresses are outside of this range or you may have an IP conflict.
4 **802.1d Spanning Tree**: The 802.1D Spanning Tree was designed at a time when the recovery of connectivity after an outage within a minute or so was considered adequate performance. **Enable** – select if you want this function.
5 **LLTD:** allows Wireless Router to query the other devices on the network so it can determine how the network is organized. **Enable** – select if you want this function.
6 **UPNP:** To use the Universal Plug and Play (UPnP™) feature click on **Enabled**. UPNP provides compatibility with networking equipment, software and peripherals.
7 **PPPOE relay**: Uncheck the box to transfer the pppoe server information from your ISP to your computers. If checked, your computers will use the router for a pppoe server.

4.4.2 DHCP Setting



1 **DHCP Subnet Mask**: Enter the Subnet Mask which the DHCP server assignment. The default subnet mask is 255.255.255.0.

2 **DHCP Primary DNS:** the DNS of DHCP server.

3 **DHCP Secondary DNS**: the another DNS of DHCP server.

4 **DHCP Default Gateway:** the gateway where DHCP server assignment IP to DHCP client.

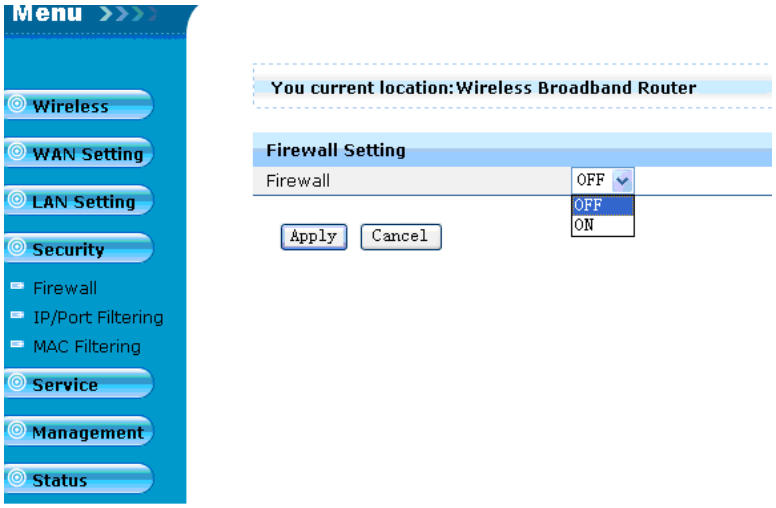
5 **DHCP Lease Time:** The length of time for the IP address lease. Enter the Lease time in minutes

6 **Statically Assigned**: If you want a computer or device to always have the same IP address assigned, you can create a DHCP reservation. The router will assign the IP address only to that computer or device.

Note: This IP address must be within the DHCP IP Address Range.

4.5 Security

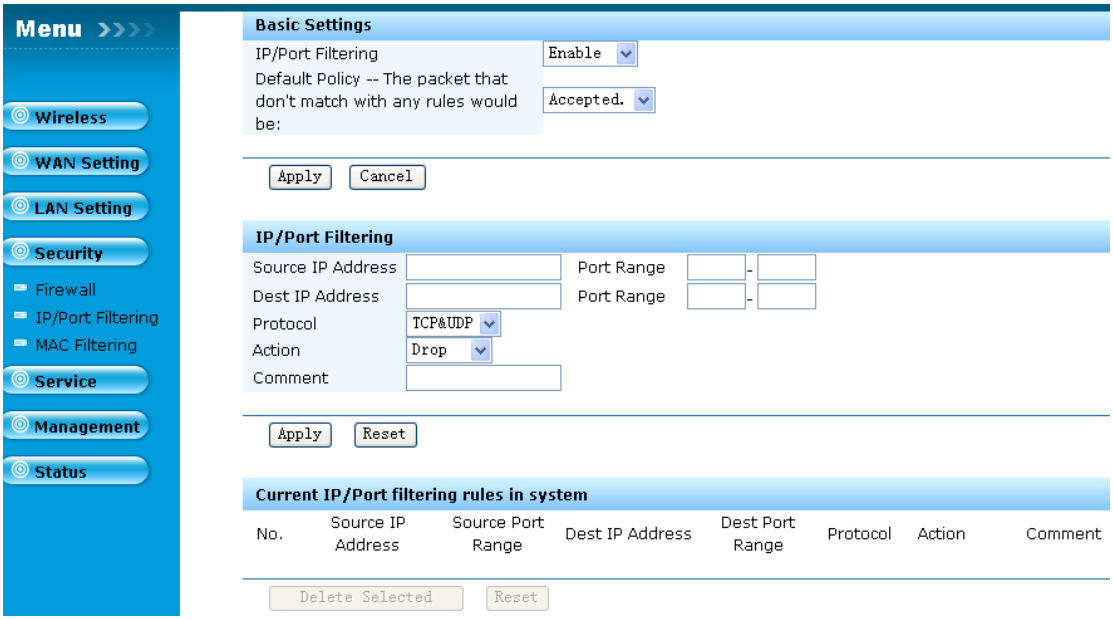
4.5.1 Firewall



1 **Firewall:** firewall feature filters out unrecognized packets to protect your LAN network and prevent cyber attacks. so all computers networked with the Wireless

Router are invisible to the outside world. The Wireless Router offers a firewall type functionality. **Enable** – firewall function is enable. And then click **Apply** button.

4.5.2 IP/Port Filtering



1 **IP/Port Filtering:** Click **Enabled** to apply the filter policy or click **Disabled** to enter an inactive filter policy.(You can reactivate the policy later.)

2 **Default Policy:** default if accept.

3 **Source IP Address**: Enter in the source IP address of the computers that you want the policy to apply to. If it is only a single computer that you want the policy applied to, then enter the IP address of that computer in the Start Source IP and leave the End Source IP blank.

4 **Port Range**: Enter in the source port range of the TCP/UDP ports that you want the policy to apply to. If it is only a single port that you want the policy applied to, then enter the port number in the Start Port field and leave the End Port field blank. If you want to use all the ports, you can leave the port range empty.

5 **Dest IP Address**: Enter in the dest IP address of the computers that you want the policy to apply to. If it is only a single computer that you want the policy applied to, then enter the IP address of that computer in the Start Source IP and leave the End Source IP blank.

6 **Port Range**: Enter in the dest port range of the TCP/UDP ports that you want the policy to apply to. If it is only a single port that you want the policy applied to, then enter the port number in the Start Port field and leave the End Port field blank. If you want to use all the ports, you can leave the port range empty.

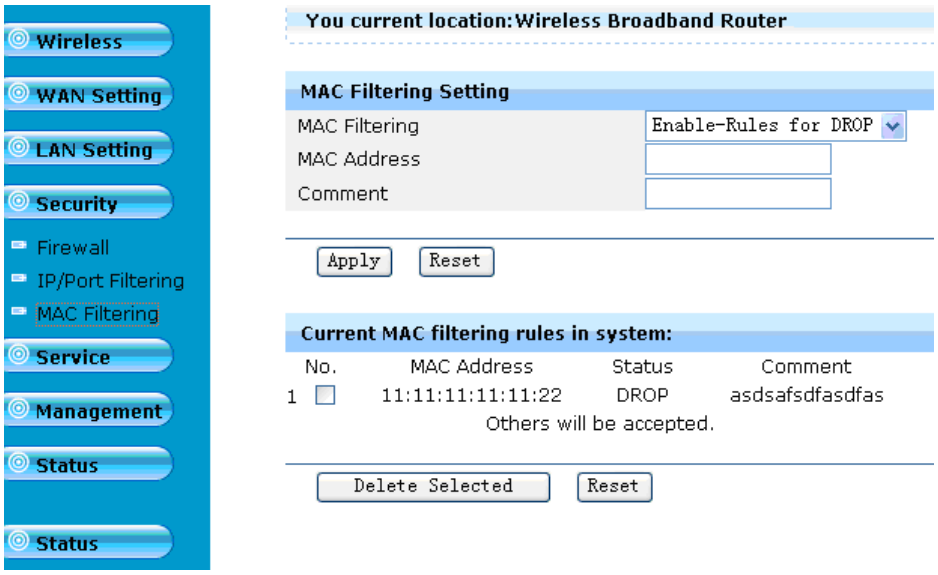
7 **Protocol**: Select the protocol type to allow or deny certain types of IP addresses.

8 **Action**: you can select drop or accept the IP and port you set above access to

internet.

9 **Comment**: you can write some word for comment.

4.5.3 MAC Filtering



1 **MAC Filtering**: Select **Disable** if you do not want to use MAC filters. Or else select another if you want to use MAC filter.

2 **MAC Address**: fill the MAC address you want to drop. Only if you don't select **MAC Filtering** disable.

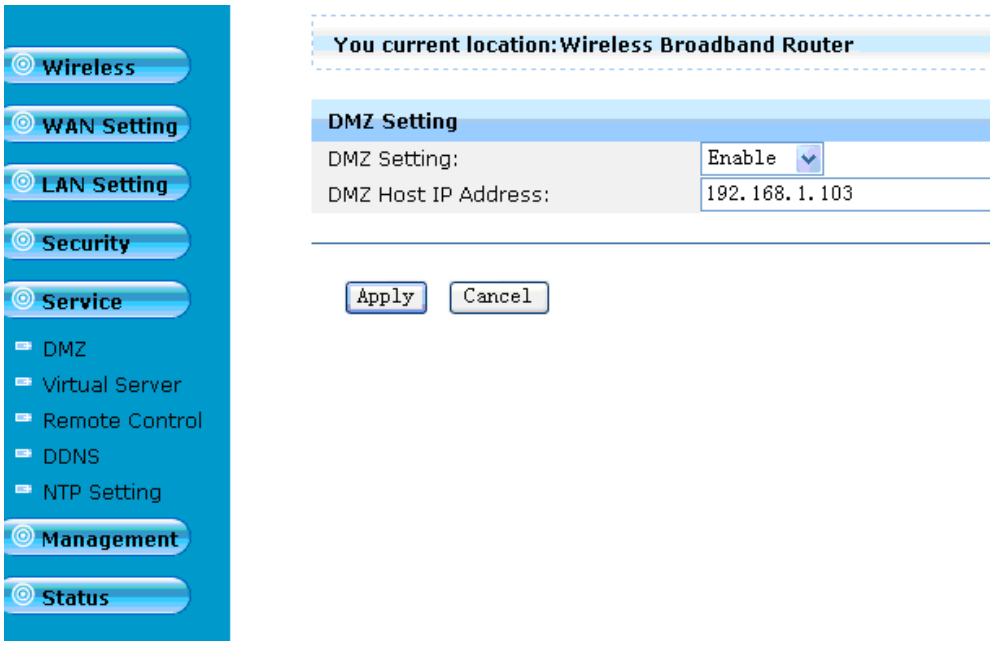
3 **Comment:** fill some word you want to comment.

In the below of the page, you will see the current MAC filtering rules in system you just set. You can delete some rules if you want on clicking **Delete selected** button when you have selected.

4.6 Service

4.6.1 DMZ

Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you cam enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.



1 **DMZ Setting**: If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer.

Note: Placing a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

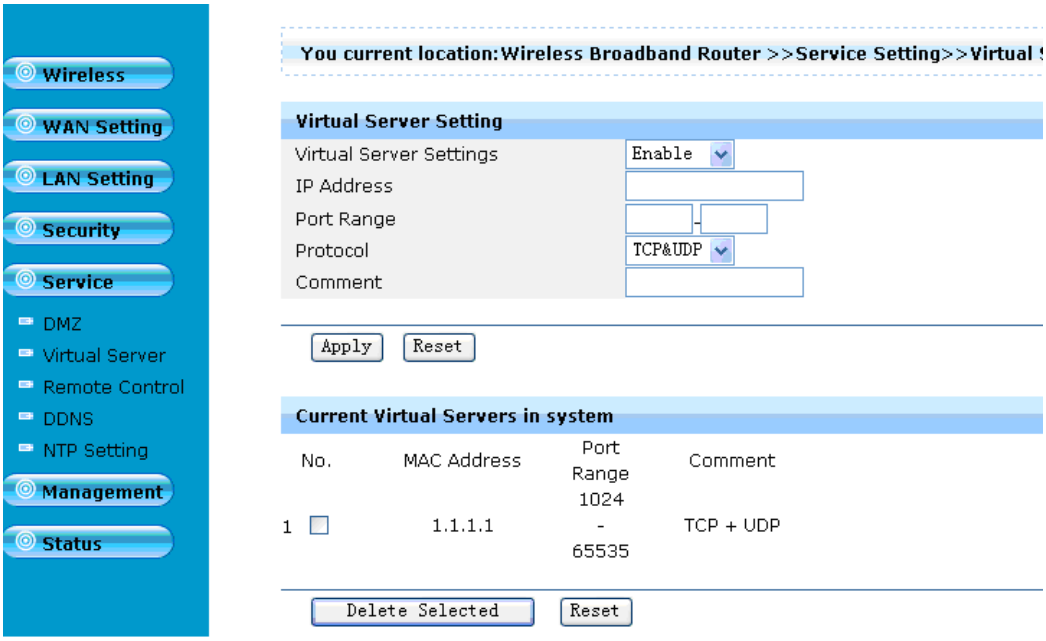
2 **DMZ Host IP Address**: Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains it's IP address automatically using DHCP, be sure to make a static reservation on the Basic > DHCP page so that the IP address of the DMZ machine does not change.

4.6.2 Virtual Server

The Wireless Router can be configured as a virtual server so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN (Local Area Network).

The Wireless Router is also capable of port-redirection meaning incoming traffic to a particular port may be redirected to a different port on the server computer.

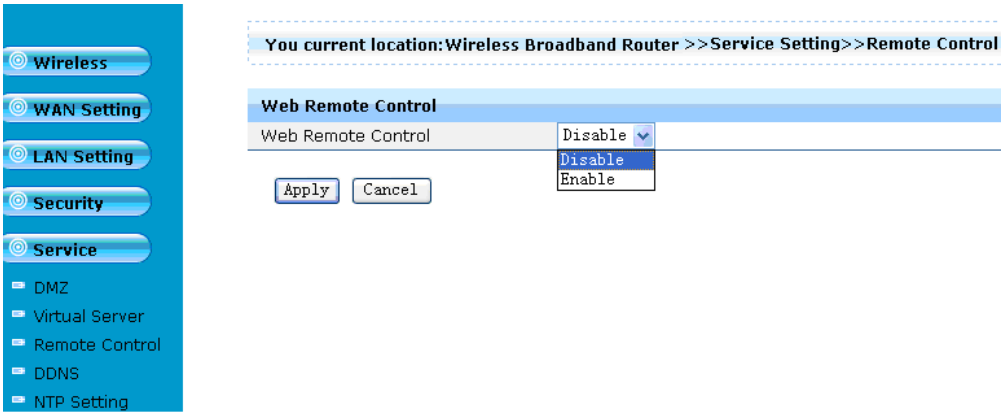
Each virtual service that is created will be listed at the bottom of the screen in the Virtual Servers List.



1 **Virtual Server Settings**: Check **Enabled** to activate entry.
2 **IP Address:** enter the IP Address of the computer on your local network that you want to allow the incoming service to.
3 Port Range: enter the port range of the computer on your local network that you want to allow the incoming service to.
4 Protocol: either TCP, UDP, or both. If you are not sure, select both.
5 Comment: Enter a name for your virtual server entry.
In the below of the page, you will see the current current virtual servers in system you just set. You can delete some rules if you want on clicking **Delete selected** button when you have selected.

4.6.3 Remote Control

Remote Control allows the device to be configured through the WAN (Wide Area Network) port from the Internet using a web browser. A username and password is still required to access the browser-based management interface.

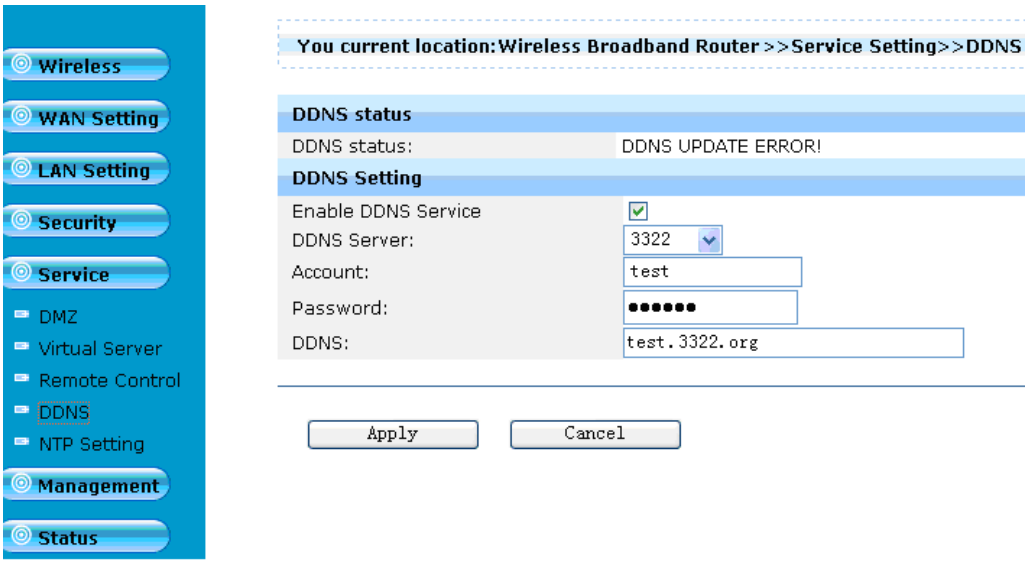


1 **Web Remote Control**: **Enable** – the Remote Control fuction is become effective.

4.6.4 DDNS

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc…) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter in your domain name to connect to your server no matter what your IP address is.

DDNS (Dynamic Domain Name System) keeps dynamic IP addresses (*e.g.*, IP addresses assigned by a DHCP capable router or server) linked to a domain name. Users who have a Dynamic DNS account may use this feature on the Wireless Router.



1 **DDNS status**: the status of DDNS you set.

2 **Enable DDNS Service**: When an IP address is automatically assigned by a DHCP server, DDNS automatically updates the DNS server. Check the box to enable DDNS.

3 **DDNS Server**: Choose your DDNS provider from the drop down menu.

4 **Account:** Enter the Username for your DDNS account.

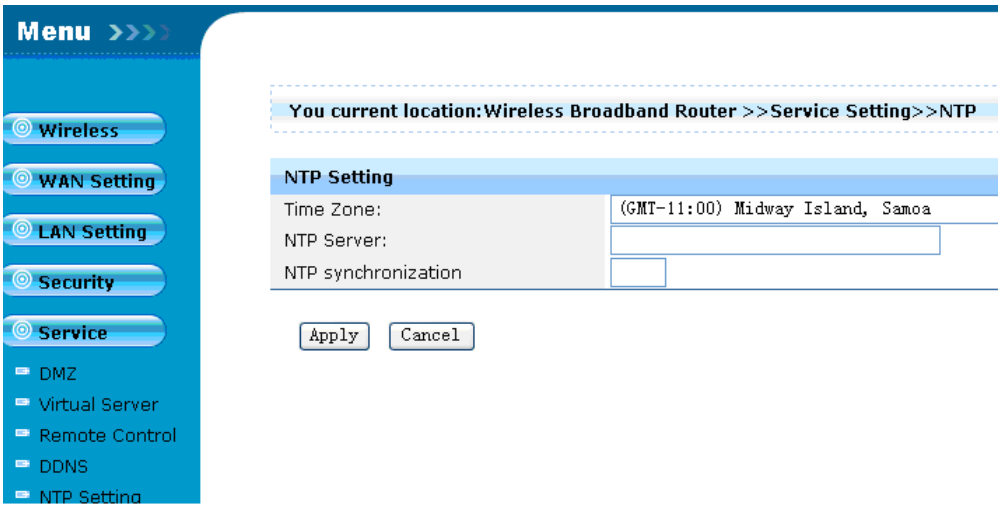
5 **Password:** Enter the Password for your DDNS account.

6 **DDNS**: Enter the Host Name that you registered with your DDNS service provider.

4.6.5 NTP Setting

The NTP Setting allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you

are in and set the Time Server. Daylight Saving can also be configured to automatically adjust the time when needed.



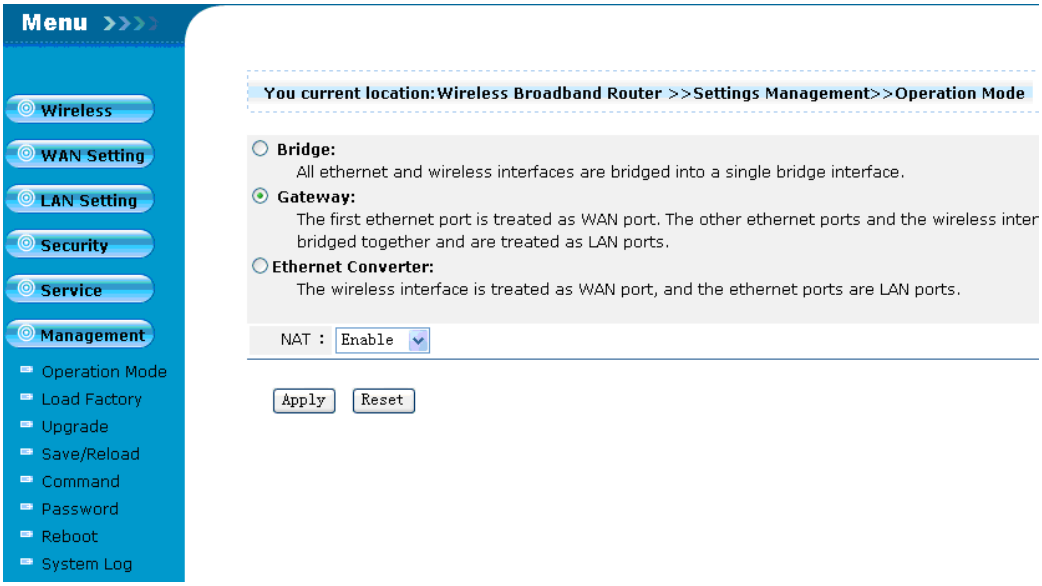
1 **Time Zone**: Select the Time Zone from the drop-down menu.

2 **NTP Server**: NTP is short for Network Time Protocol. NTP synchronizes computer clock times in a network of computers. Check this box to use a NTP server. This will only connect to a server on the Internet, not a local server.

3 **NTP synchronization**: synchronise NTP

4.7 Management

4.7.1 Operation Mode



1 Bridge: if you select Bridge**,** All ethernet and wireless interfaces are bridged into a single bridge interface.

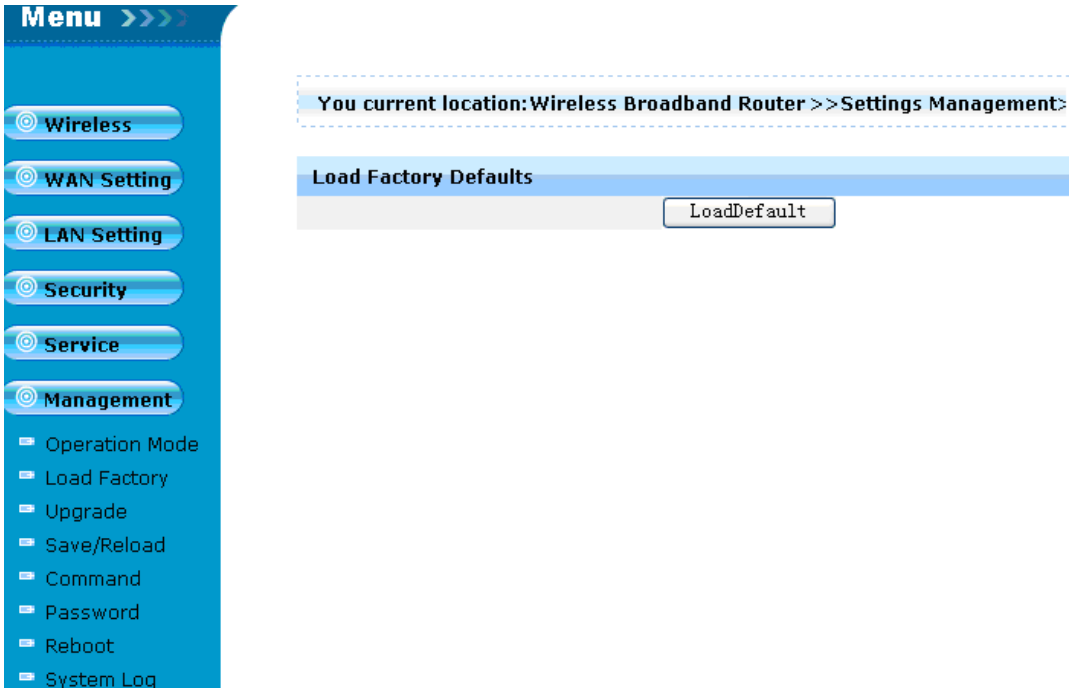
2 Gateway: if you select **Gateway,** The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports.

3 Ethernet Converter: if you select **Ethernet Converter,** The wireless interface is treated as WAN port, and the ethernet ports are LAN ports.

4 NAT: Enable – select if you want to NAT function. Only you select **Gateway,** it can configure.

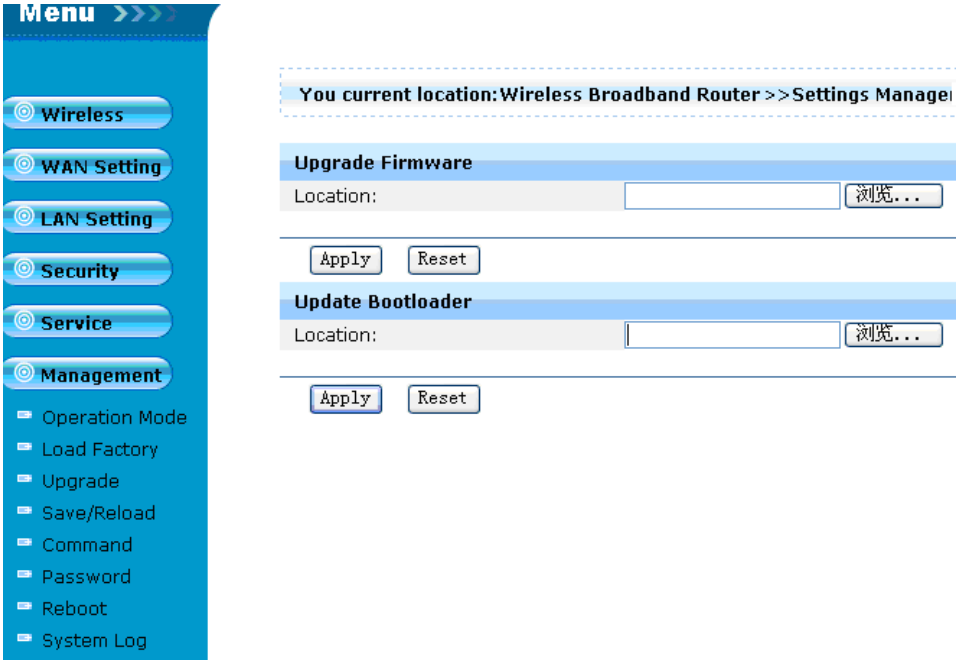
4.7.2 Load Factory Defaults

The device can also be reset back to factory default settings by clicking on "Load Default" button. Use the restore feature only if necessary. This will erase previously saved settings for the unit. Make sure to save your system settings before doing a factory restore.



4.7.3 Upgrade

You can upgrade the firmware or bootloader of the device using this tool. Make sure that the firmware or bootloader you want to use is saved on the local hard drive of the computer. Click on "Browse" to search the local hard drive for the firmware or bootloader to be used for the update. Upgrading the firmware or bootloader will not change any of your system settings but it is recommended that you save your system settings before doing a firmware upgrade. Please contact your distributor or dealer for details.



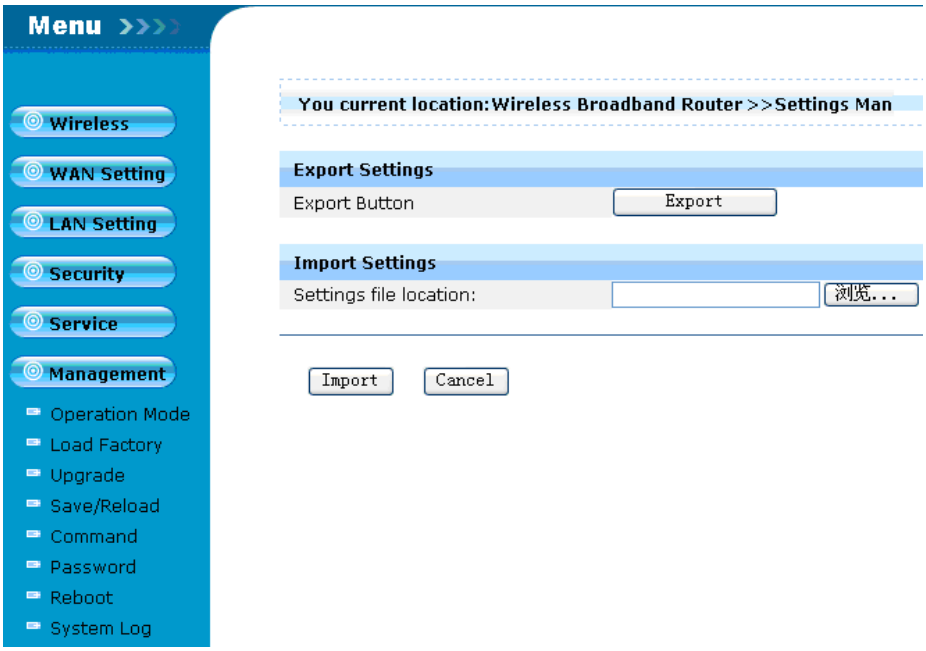
1 Browse: After you have downloaded the new firmware, click Browse in this window to locate the firmware update on your hard drive. Click Apply to complete the firmware upgrade.

2 Browse: After you have downloaded the new bootloader, click Browse in this window to locate the bootloader update on your hard drive. Click Apply to complete the bootloader upgrade.

Note: Do not power off the unit when it is being upgraded. When theupgrade is complete, the unit will be restarted automatically.

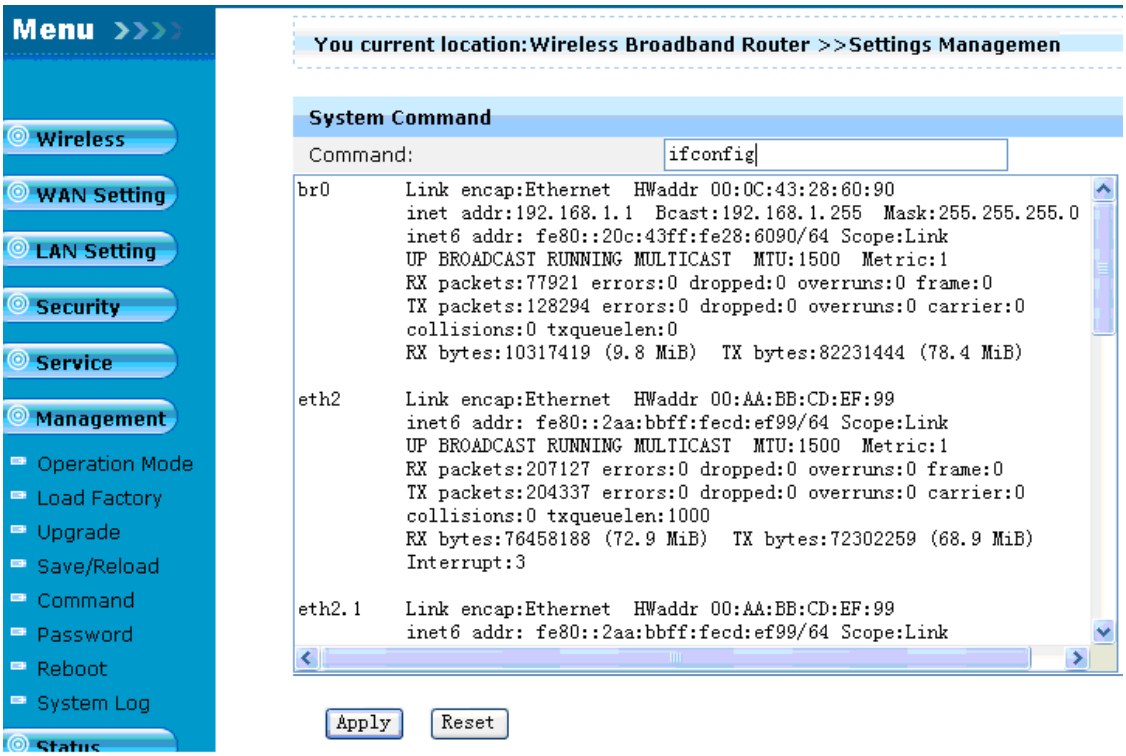
4.7.4 Save/Reload

The current system settings can be saved as a file onto the local hard drive only clicking **Export** button. The saved file or any other saved setting file created by the Wireless Router can be uploaded into the unit. To reload a system settings file, click on "Browse" to search the local hard drive for the file to be used, then click **Import** button when finished.



4.7.5 Command

In this page, you can use the Commands in the system to see the message about Wireless Router.

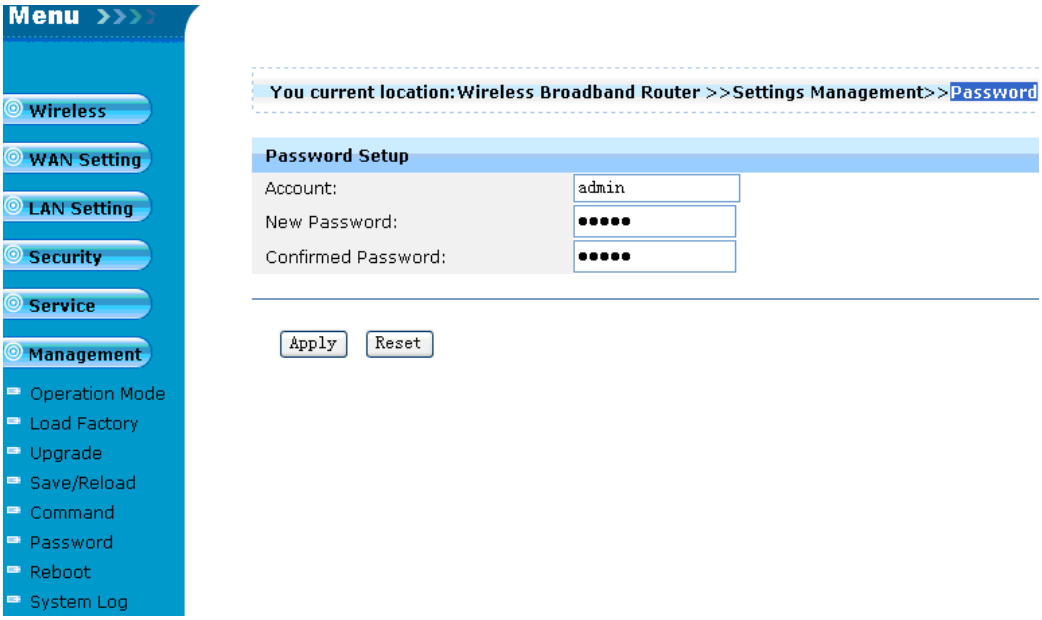


4.7.6 Password

This page allows you to change the factory default user name and password of the router.

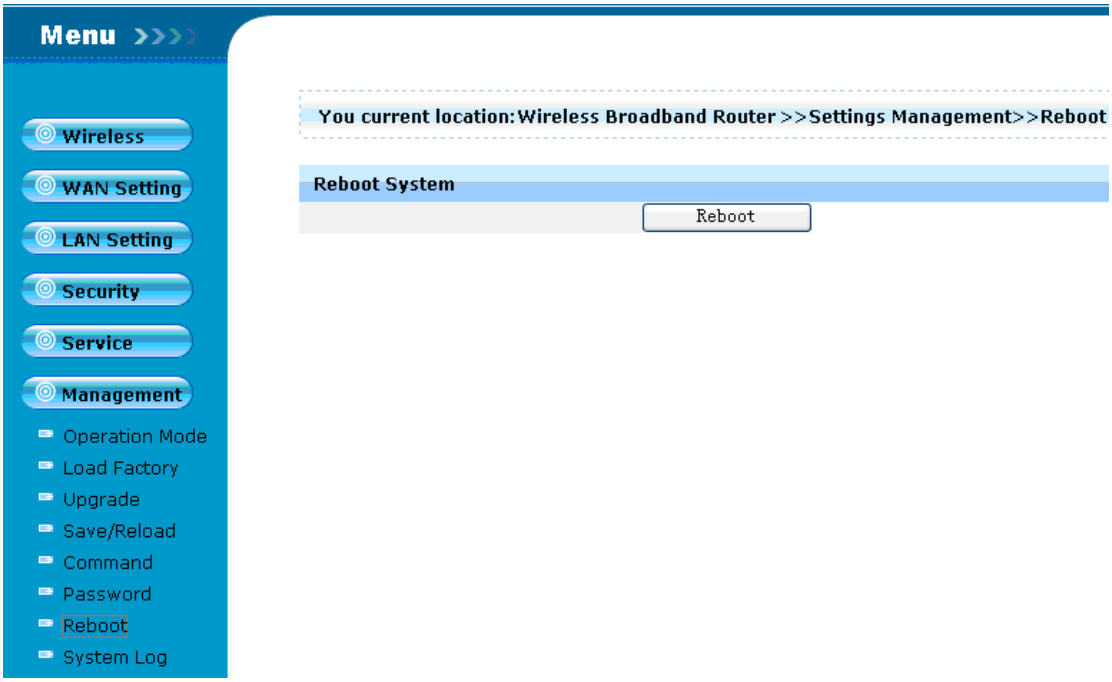
It is strongly recommended that you change the factory default username and password of the router. All users who try to access the router's web-based utility will be prompted for the router's user name and password.

Note: The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new password twice to confirm it. And click **Apply** button when finished.



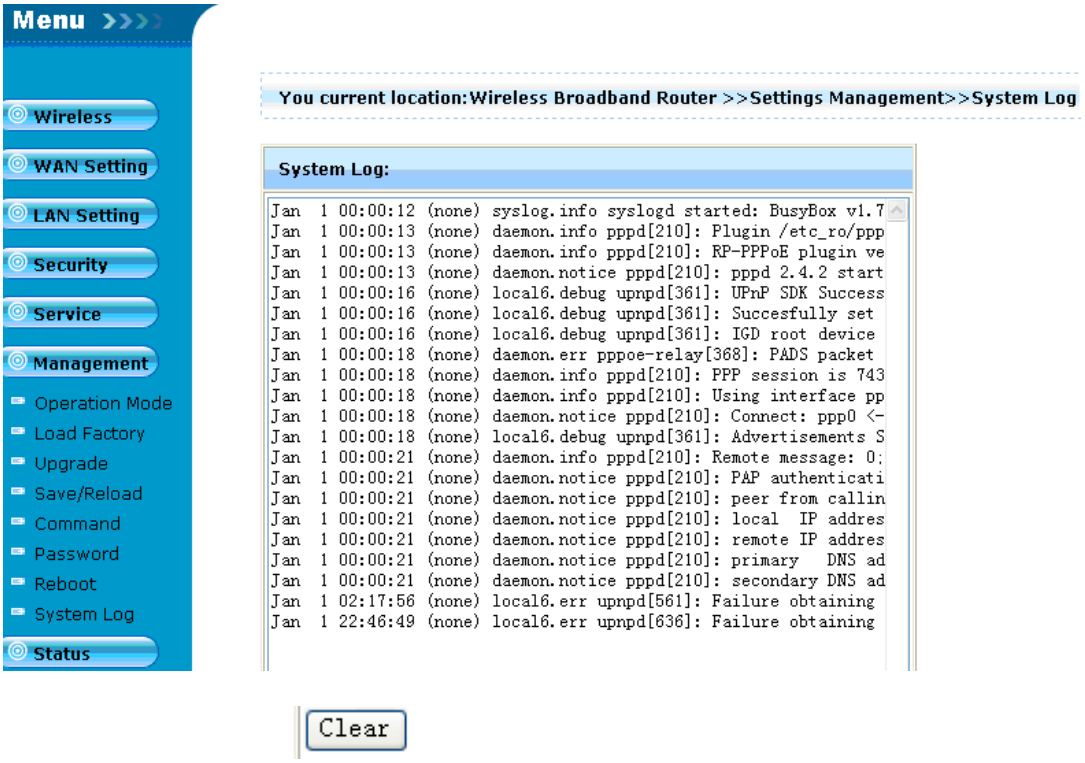
4.7.7 Reboot

Click **Reboot** button to restart the unit.



4.7.8 System Log

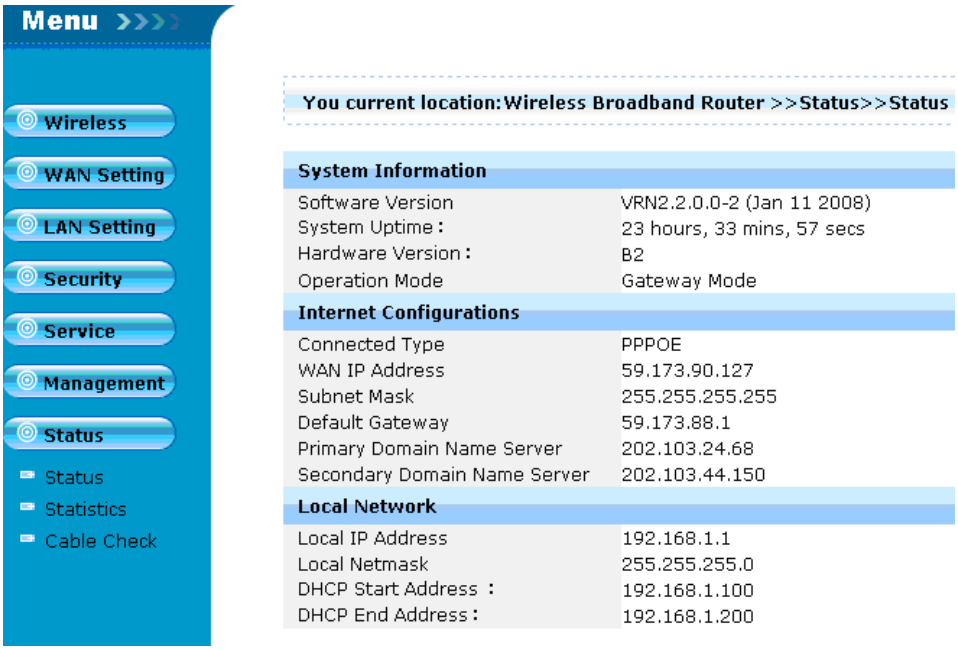
The router automatically logs (records) events of possible interest in it's internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. The **System Log** allows you to view the router logs. You can also click **Clear** button to the current log.



4.8 Status

4.8.1 Status

The Status page displays the router's current status and configuration. All information is read-only



1 **System Information**

This field displays the current system information for the **Software Version, System Uptime, Hardware Version, Operation Mode**.

2 **Internet Configurations**

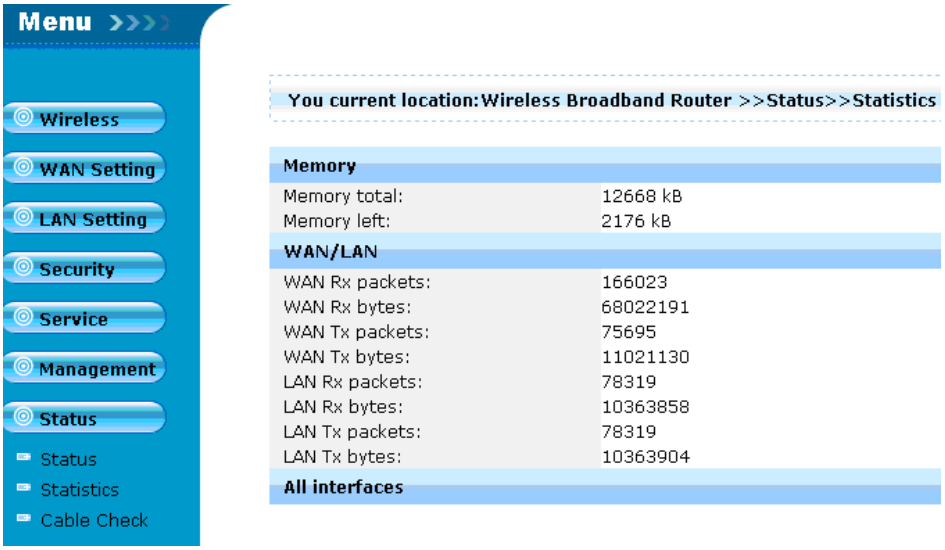
This field display the Internet Configuration for the **connected types, WAN IP address, Subnet Mask, Default Gateway, Primary Domain Name Server, Secondary Domain Name Server.**

3 **Local Network**

This field display the Local Network for the **Local IP Address, Local Netmask, DHCP Start Address, DHCP End Address.**

4.8.2 Statistics

The Status page displays the router's current status and message. All information is read-only



1 Memory

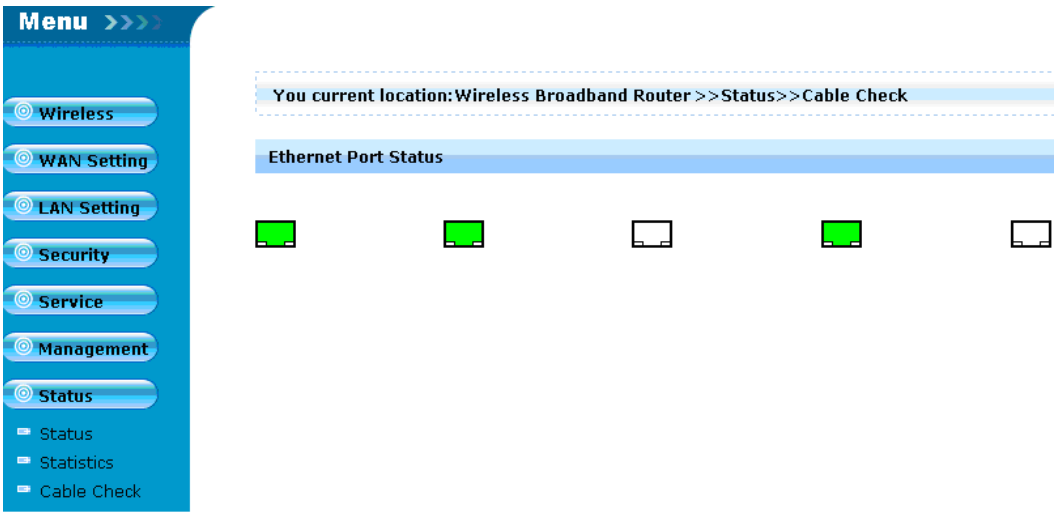
This field displays the current system Memory for the **total memory, left memory.**

2 WAN/LAN

This field displays the current WAN port and LAN port packet message for the **WAN Rx packets, WAN Rx bytes, WAN Tx packets, WAN Tx bytes, LAN Rx packets, LAN Rx bytes, LAN Tx packets, LAN Tx bytes,**

4.8.3 Cable Check

The Status page displays the router's current status of Cable.



Appendix 1: Wireless Basics

Wireless product are based on industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home, business or public access wireless networks. Strictly adhering to the IEEE standard, the wireless family of products will allow you to securely access the data you want, when and where you want it. You will be able to enjoy the freedom that wireless networking delivers.

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards. Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A Wireless Router is a device used to provide this link.

What is Wireless?

Wireless or Wi-Fi technology is another way of connecting your computer to the network without using wires. Wi-Fi uses radio frequency to connect wirelessly, so you have the freedom to connect computers anywhere in your home or office network.

How does wireless work?

Wireless works similar to how cordless phone work, through radio signals to transmit data from one point A to point B. But wireless technology has restrictions as to how you can access the network. You must be within the wireless network range area to be able to connect your computer. There are two different types of wireless networks Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

Wireless Local Area Network (WLAN)

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth over radio signals. With an indoor access point as seen in the picture, the signal can travel up to 300 feet. With an outdoor access point the signal can reach out up to 30 miles to serve places like manufacturing plants, industrial locations, college and high school campuses, airports, golf courses, and many other outdoor venues.

Wireless Personal Area Network (WPAN)

Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPAN operate in a range up to 30 feet away.

Compared to WLAN the speed and wireless operation range are both less than WLAN, but in return it doesn't use nearly as much power which makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

Who uses wireless?

Wireless technology as become so popular in recent years that almost everyone is using it, whether it's for home, office, business, D-Link has a wireless solution for it.

Home

• Gives everyone at home broadband access
• Surf the web, check email, instant message, and etc
• Gets rid of the cables around the house
• Simple and easy to use

Small Office and Home Office

• Stay on top of everything at home as you would at office
• Remotely access your office network from home
• Share Internet connection and printer with multiple computers
• No need to dedicate office space

Where is wireless used?

Wireless technology is expanding everywhere not just at home or office. People like the freedom of mobility and it's becoming so popular that more and more public facilities now provide wireless access to attract people. The wireless connection in public places is usually called "hotspots".

Using a Cardbus Adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like: Airports, Hotels, Coffee Shops, Libraries, Restaurants, and Convention Centers.

Wireless network is easy to setup, but if you're installing it for the first time it could be quite a task not knowing where to start. That's why we've put together a few setup steps and tips to help you through the process of setting up a wireless network.

Tips

Here are a few things to keep in mind, when you install a wireless network.

Centralize your router or Access Point

Make sure you place the router/access point in a centralized location within your network for the best performance. Try to place the router/access point as high as possible in the room, so the signal gets dispersed throughout your home. If you have a two-story home, you may need a repeater to boost the signal to extend the range.

Eliminate Interference

Place home appliances such as cordless telephones, microwaves, and televisions as far away as possible from the router/access point. This would significantly reduce any interference that the appliances might cause since they operate on

same frequency.

Security

Don’t let you next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA security feature on the router. Refer to product manual for detail information on how to set it up.

Wireless Security This section will show you the different levels of security you can use to protect your data from intruders. The DIR-635 offers the following types of security: • WPA2 (Wi-Fi Protected Access 2) • WPA2-PSK (Pre-Shared Key) • WPA (Wi-Fi Protected Access) • WPA-PSK (Pre-Shared Key)

Appendix 2: Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer.

An Infrastructure network contains an Access Point or wireless router. All the wireless devices, or clients, will connect to the wireless router or access point.

An Ad-Hoc network contains only clients, such as laptops with wireless cardbus adapters. All the adapters must be in Ad-Hoc mode to communicate.

Appendix 3: FAQ

This chapter provides solutions to problems that can occur during the installation and operation of the Wireless Router. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

1. Why can’t I access the web-based configuration utility?

When entering the IP address of the router (192.168.1.1 for example), you are not connecting to a website on the Internet or have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

• Make sure you have an updated Java-enabled web browser. We recommend the following:

• Internet Explorer 6.0 or higher
• Netscape 8 or higher
• Mozilla 1.7.12 (5.0) or higher
• Opera 8.5 or higher
• Safari 1.2 or higher (with Java 1.3.1 or higher)
• Camino 0.8.4 or higher

• Firefox 1.5 or higher
• Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
• Disable any internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.
• Configure your Internet settings:
• Go to **Start** > **Settings** > **Control Panel**. Double-click the **Internet Options** Icon. From the **Security** tab, click the button to restore the settings to their defaults.
• Click the **Connection** tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click **OK**.
• Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.
• Close your web browser (if open) and open it.
• Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your the web management.
• If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

2. What can I do if I forgot my password?

If you forgot your password, you must reset your router. Unfortunately this process will change all your settings back to the factory defaults.

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The default IP address is 192.168.1.1. When logging in, the username is **admin** and the password is admin.

3. Why can't I connect to certain sites or send and receive emails when connecting through my router?

If you are having a problem sending or receiving email, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

Note: AOL DSL+ users must use MTU of 1400.

To find the proper MTU Size, you'll have to do a special ping of the destination you're trying to go to. A destination could be another computer, or a URL.

• Click on **Start** and then click **Run**.
• Windows® 95, 98, and Me users type in **command** (Windows® NT, 2000, and XP users type in **cmd**) and press **Enter** (or click **OK**).
• Once the window opens, you'll need to do a special ping. Use the following syntax:
ping [url] [-f] [-l] [MTU value]
example: ping www.baidu.com –f –l 1424
and ping www.baidu.com –f –l 1425

```
C:\Documents and Settings\test>ping www.baidu.com -f -l 1424

Pinging www.a.shifen.com [220.181.37.55] with 1424 bytes of data:

Reply from 220.181.37.55: bytes=1424 time=91ms TTL=51
Reply from 220.181.37.55: bytes=1424 time=91ms TTL=51
Reply from 220.181.37.55: bytes=1424 time=323ms TTL=51
Reply from 220.181.37.55: bytes=1424 time=90ms TTL=51

Ping statistics for 220.181.37.55:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 90ms, Maximum = 323ms, Average = 148ms

C:\Documents and Settings\test>

C:\Documents and Settings\test>ping www.baidu.com -f -l 1425

Pinging www.a.shifen.com [220.181.37.55] with 1425 bytes of data:

Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
```

You should start at 1424 and work your way down by 10 each time. Once you get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to the value to account for the various TCP/IP headers. For example, lets say that 1402 was the proper value, the actual MTU size would be 1480, which is the optimum for the network we're working with (1402+28=1430).
Once you find your MTU, you can now configure your router with the proper MTU size.

To change the MTU rate on your router follow the steps below:
• Open your browser, enter the IP address of your router (192.168.1.1) and click **OK**.
• Enter your username (admin) and password (admin). Click **OK** to enter the web configuration page for the device.
• Click on **WAN Setting** and then click **WAN Interface**.
• To change the MTU enter the number in the MTU field and click **Apply** to save your settings.
• Test your email. If changing the MTU does not resolve the problem, continue

changing the MTU in increments of ten.

3. What is WPA?

WPA, or Wi-Fi Protected Access, is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.

4. What is NAT?

NAT stands for **Network Address Translator**. It is proposed and described in RFC- 1631 and is used for solving the IP Address depletion problem. Each NAT box has a table consisting of pairs of local IP Addresses and globally unique addresses, by which the box can "translate" the local IP Addresses to global address and vice versa. Simply put, it is a method of connecting multiple computers to the Internet (or any other IP network) using one IP Address. The broadband routers (ie: Wireless Router) support NAT. With proper configuration, multiple users can access the Internet using a single account via the NAT device.