User's Manual

Wireless 11n AP/Router
(1T2R & 2T2R)

Brand: ACEEX
Model No: NR22

Index

Chapter 1 Introduction 5
1.1 Overview 5
1.2 Features 5
1.3 System Requirements 6
Chapter 2 Installation 7
2.1 Checklist 7
2.2 The Front LEDs 8
2.3 The Rear Ports 9
2.4 The Bottom Port 9
Chapter 3 Configuration 10
3.1 Determine your connection settings 10
3.2 Connecting the Wireless 11n Router to your network 10
3.3 Configuring with Web Browser 10
3.3.1 Wireless 11n Router Setting 11
3.3.2 Operation Mode Setting 12
3.3.2 Operation Mode Setting 12
3.4.1 WAN Setting 13
3.4.2 LAN Setting 19
3.4.3 DHCP Clients Setting 21
3.4.4 Advanced Routing Setting 22
3.4.5 QoS Setting 23
3.5.1 Wireless-Basic Setting 24
3.5.2 Advanced Setting 26
3.5.3 Security Setting 30
3.5.4 WPS Setting 35
3.5.5 Station List 36
3.6.1 MAC/IP/Port Filtering Setting 37
3.6.2 Port Forwarding Setting 39
3.6.3 DMZ Setting 40
3.6.4 System Security Settings 41
3.6.5 Content Filtering Settings 42
3.7.1 Management Settings 43
3.7.2 System Log 44
3.7.3 Settings Management 45
3.7.4 System Status 46
3.7.5 Statistic 47

3.7.6 System Log 48
3.8.1 TCP/IP Settings for Windows Operating System 49
Certification: FCC, CE 56
Appendix A Glossary 56
Appendix B Cabling / Connection 64

FCC and Other Compliance Statements

Federal Communication Commission

Interference Statement

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

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

FCC Caution

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

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, and (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 authority to operate equipment.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

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

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However,

special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not intended for use

None.

Chapter 1 Introduction

Congratulations on your purchase of an Instant Wireless 11n Router for cable/xDSL application. The Wireless 11n Router is the perfect option to connect a small group of PCs to a high-speed Broadband Internet connection or to an Ethernet backbone. Configurable as a DHCP server, the Broadband Router acts as the only externally recognized Internet device on your local area network (LAN). The Router serves as an Internet firewall, protecting your network from being accessed by outside users. The data rates up to 300Mbps for wireless connection, user can easy to share HD video or data transfer.

1.1 Overview

Wireless 11n will replace the 11b/g as the new generation solution. Via MIMO technology, the wireless through put and coverage can be better than 11b/g.The new WPS technology, will be very easy to set the wireless security just push the button only, all the wireless encryption will auto finish.

1.2 Features

- Router Mode
  - PPP over Ethernet (RFC-2516)
  - DHCP Server and Client
  - NAPT (Network Address and Port Translation)
  - NAT (Network Address Translation
- Internet Access
  - TCP/IP, UDP, ICMP, ARP, RARP, PPPoE, NAT, DHCP (client/server), Static IP assignment
- Security Features
  - Password protected configuration access
  - User authentication (PAP/CHAP) for PPP connection
- Wireless Features
  - Support 802.11b/g, 802.11n draft 3.0 Wireless Access Point
  - Support 128-Bit and 64-Bit WEP encryption , 802.1x, WPA, WPA2, WPS
  - Support wireless operation mode as AP, WDS and AP Client
- Security
  - Support packet inspection and filtering
  - Intrusion detection and protection
  - Password protected system management

- Ethernet Interface
  - Compliant with IEEE 802.3 and 802.3u 10/100 Mbps
- HTTP Web-Based Management
  - Firmware upgrade by UI
  - WAN and LAN side connection statistics
  - Advanced QoS
  - Password protected access
  - Wireless LAN
  - System log

1.3 System Requirements

1) Personal computer (PC)

2) Pentium II 233 MHz processor minimum

3) 32 MB RAM minimum

4) 20 MB of free disk space minimum

5) Ethernet Network Interface Controller (NIC) RJ45 Port

6) Internet Browser

Chapter 2 Installation

This chapter offers information about installing your router. If you are not familiar with the hardware or software parameters presented here, please consult your service provider for the values needed.

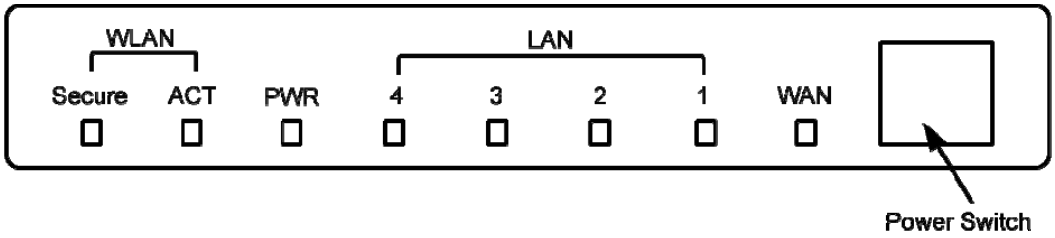
2.1 Checklist

Check the shipping box carefully to ensure that the contents include the items you ordered. If any of the items are missing or damaged, contact your local distributor. The contents of your carton may vary depending on your service provider.

Contents description

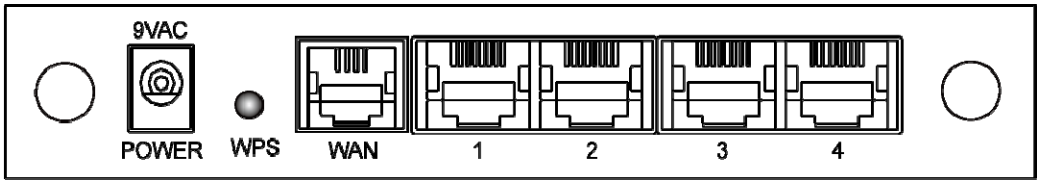
1) Wireless 11n Router for home/office use
2) Wireless 11n Router Installation and Operation Guide (this publication)
3) Power supply with 9VAC / 1Ampere power adapter
4) Ethernet cable Ethernet category 5 twisted pair cable (6 ft)
5) CD for user manual

2.2 The Front LEDs



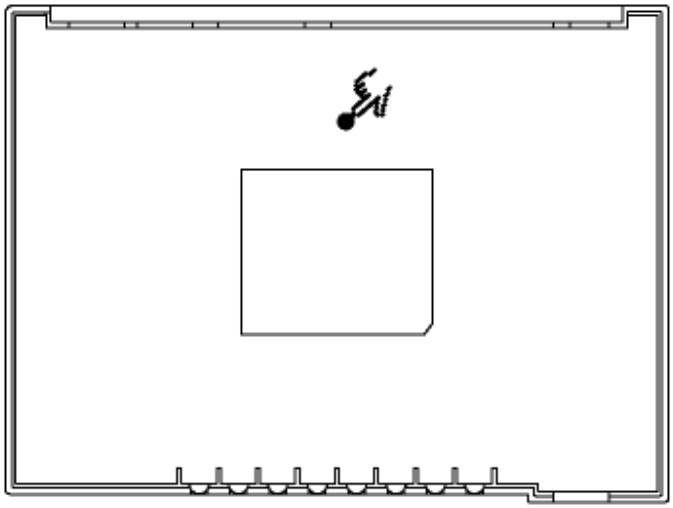
LED	State	Description
POWER	ON	Press the button to power one the router.
WAN	ON	"Showtime"-successful connection between ADSL modem and telephone company's network.
	Flashing	"Handshaking"-modem is trying to establish a connection to telco's network Modem is powered OFF ADSL Carrier Detect if LED is flash.
	OFF	No link.
PWR	ON	The router power on and running well.
WLAN-Secure	ON	When wireless security encryption enable.
WLAN-ACT	Flashing	Wireless LAN enable and link status.
LAN 1-4	ON	Ethernet cable link and enable.
	Flashing	TX or RX activity
	OFF	No Link These four LAN (Local Area Network) ports are where you will connect networked devices, such as PCs, print servers remote hard drives, and anything else you want to put on your network.

2.3 The Rear Ports



Connector	Description
POWER	Power connector with 9VAC / 1Ampere.
LAN (1-4)	Router is successfully connected to a device through the corresponding port (1, 2, 3 or 4). If the LED is flashing, the Router is actively sending or receiving data over that port.
WAN	The WAN (Wide Area Network) Port is where you will connect your cable, DSL modem or Ethernet backbone.
WPS	Push button for WPS link.
R/SMA Connector	Antenna Connector.

2.4 The Bottom Port



Connector	Description
Reset Switch	The reset button, the router restore default settings when press until reboot.

Chapter 3 Configuration

3.1 Determine your connection settings

Before you configure the router; you need to know the connection information supplied by your service provider.

3.2 Connecting the Wireless 11n Router to your network

Via Ethernet Cable to LAN Port and connect to your PC/NB RJ-45 Port or via wireless link to access the 11n router.

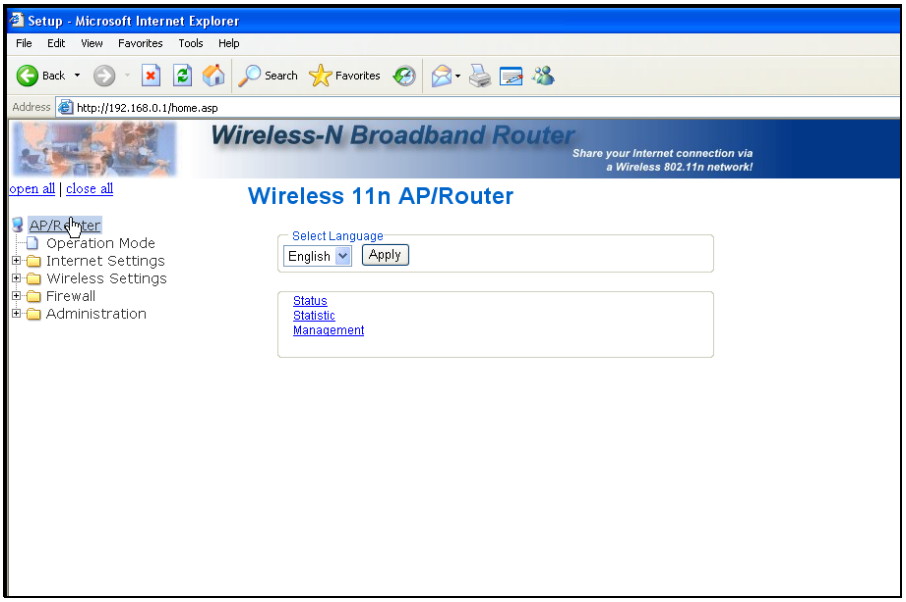
3.3 Configuring with Web Browser

It is advisable to change the administrator password to safeguard the security of your network.

To configure the router, open your browser, type **'http://192.168.0.1'** into the address bar and click 'Go' to get to the login page. Save this address in your Favorites for future reference.

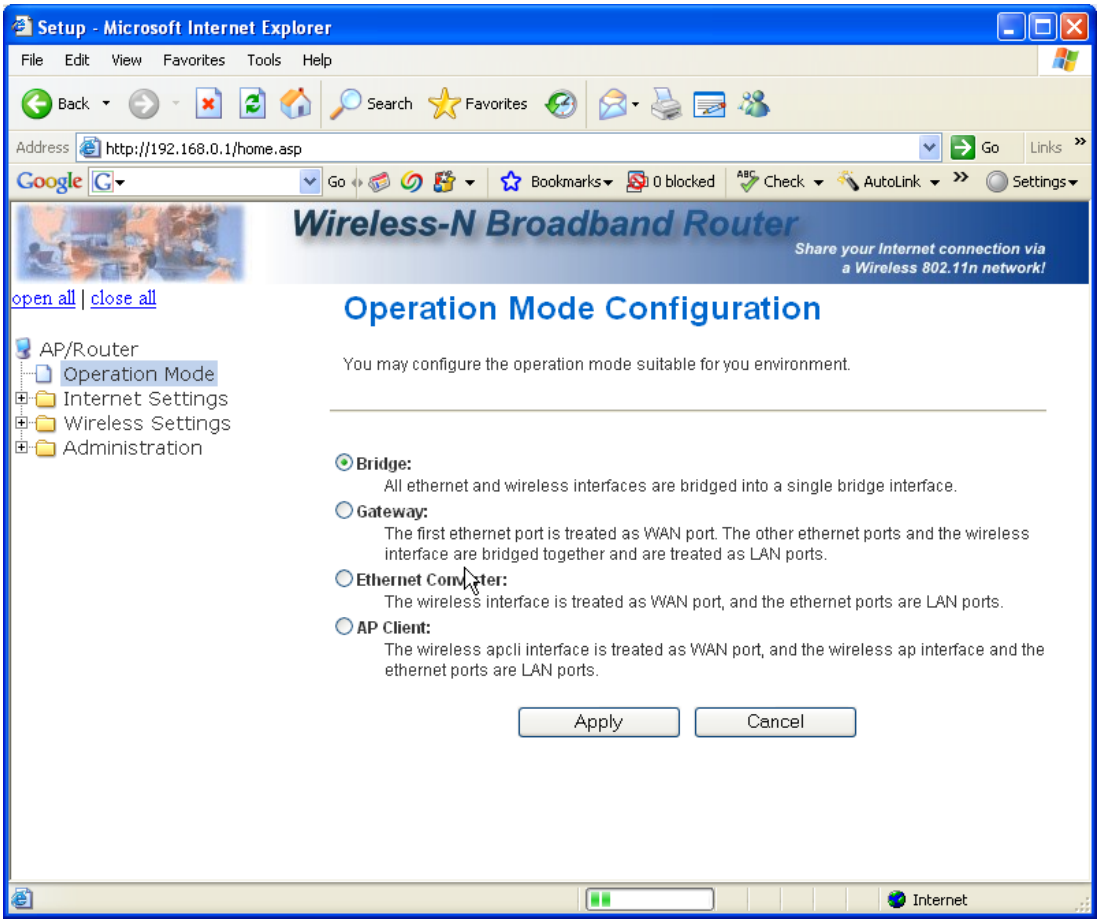
At the Password prompt, the User name is **'admin'** and the password is ’**admin**’. You can change these later if you wish. Click **'OK'** to login.

3.3.1 Wireless 11n Router Setting



In AP/Router root page, user can change the language. Click Status, Statistic or Management can directly jump to the related pages.

3.3.2 Operation Mode Setting



There are four operation modes can choose, Bridge, Gateway, Ethernet Converter or AP Client.

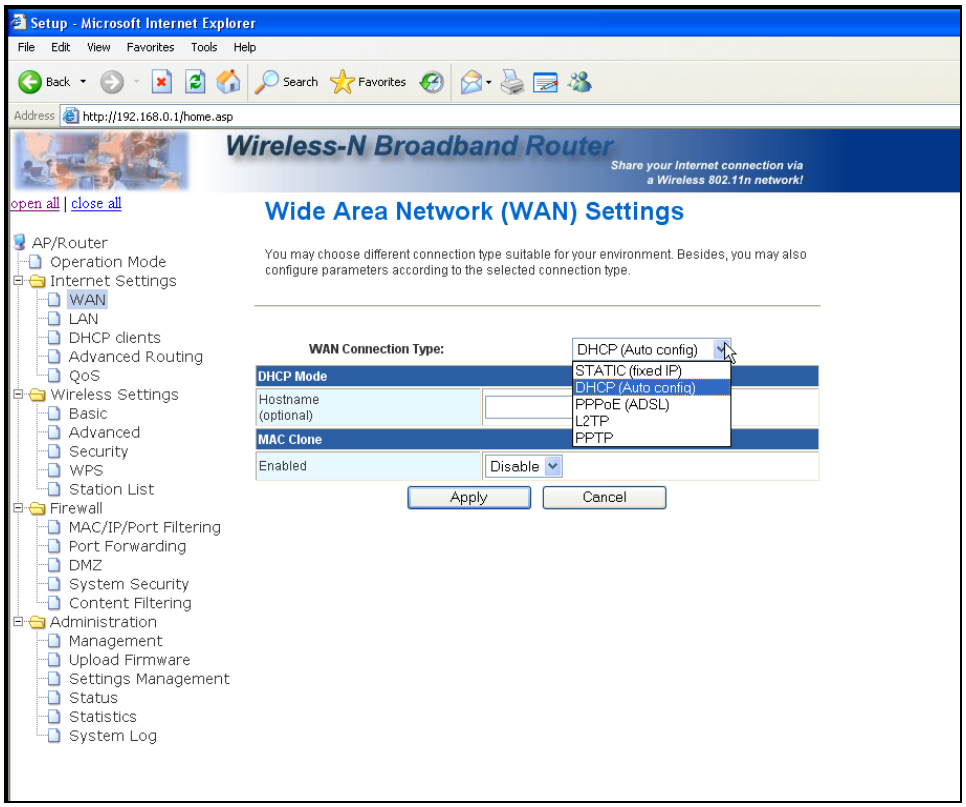
Bridge : All Ethernet ports and wireless interfaces are bridged into a single bridge interface. The router will work as bridge only..

Gateway: The device work as wireless router. The NAT will can set as enable or disable, WAN port need to link to the Internet. User can enable/disable the NAT function.

Ethernet Converter: The wireless interface is treated as WAN port, and the Ethernet ports are LAN ports.

AP Client: The wireless set as wireless client so it is treated as WAN port, all the Ethernet ports are LAN ports. User can enable/disable the NAT function.

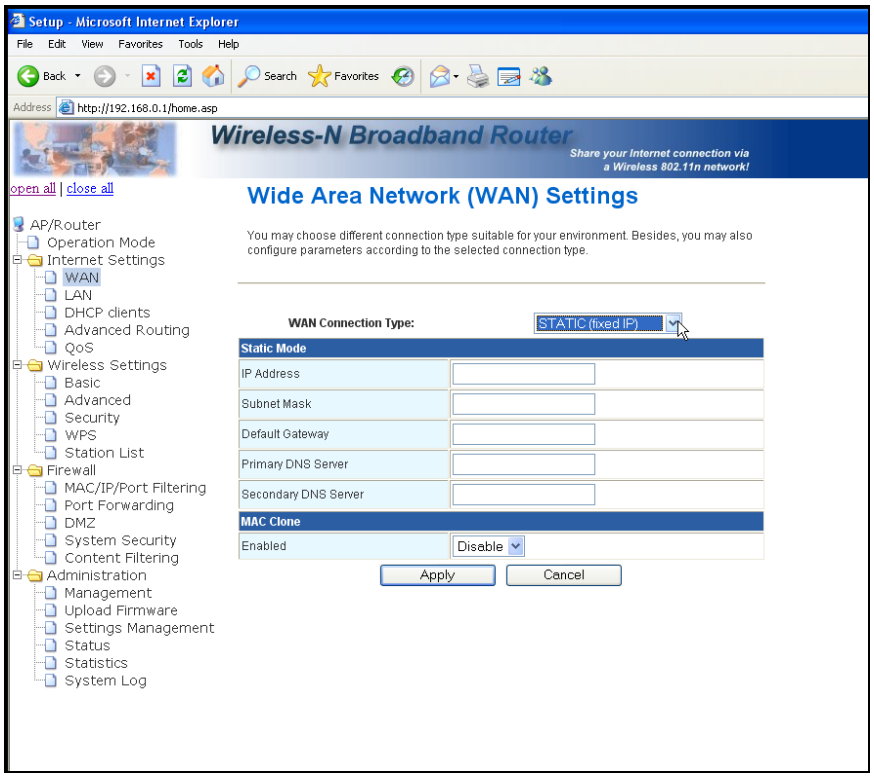
3.4.1 WAN Setting



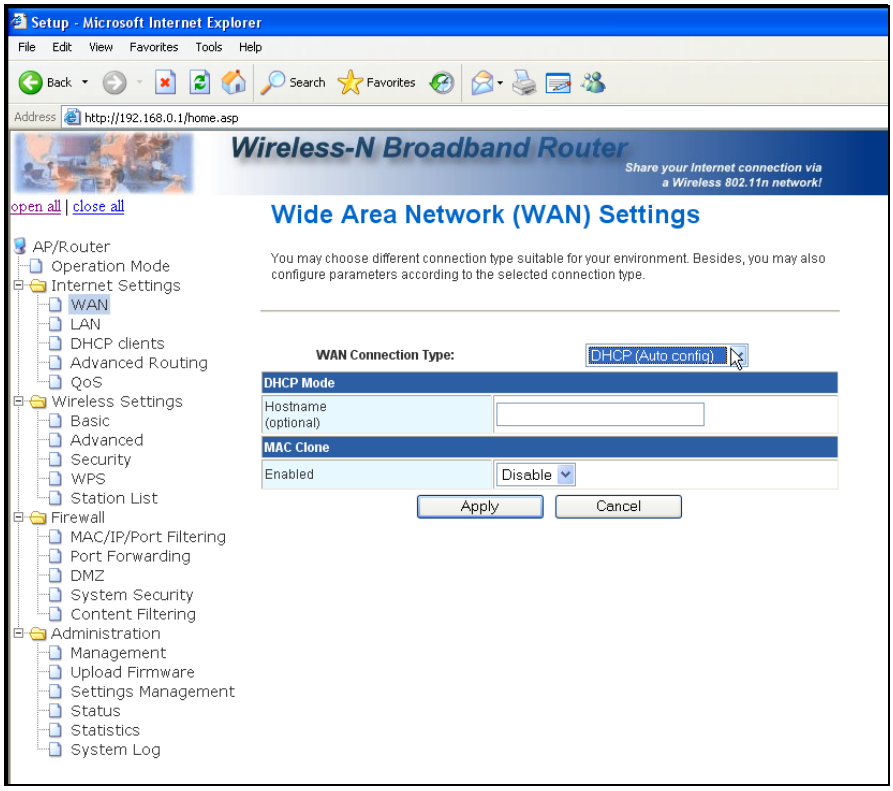
There are 5 selections for WAN connection type, the detail information as follows.

STATIC(Fixed IP): If you need to assign static IP addresses to the devices in your network, please remember that the IP address for each computer or device must be in the same IP address range as all the devices in the network. Each device must also have the same subnet mask. For example: Assign the first computer an IP address of 192.168.1.2 and a subnet mask of 255.255.255.0, the second device an IP address of 192.168.1.3 and a subnet mask of 255.255.255.0, and so on.

Note: Devices that are assigned the same IP address may not be visible on the network. Enter the IP address of the DNS server. The DNS server translates domain names into IP addresses.



DHCP(Auto config): It's will auto get the IP address from the DHCP Server.. Assign the length of time for the IP lease, default setting is 86400 seconds. The Hostname is the name of the device.

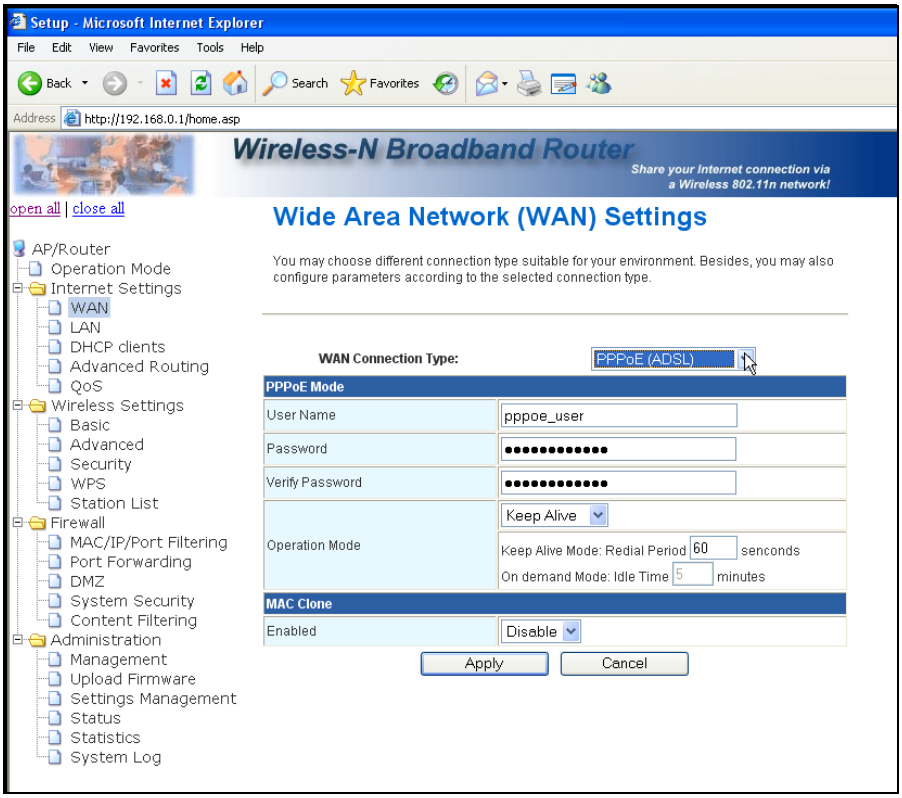


PPPoE(ADSL):

Username and Password: Fill in the User Name and Password that provided by your ISP.

Verify Password: Retype the password to confirm.

Operation Mode: Set the router as Keep Alive or On demand.



L2TP: Layer 2 Tunneling Protocol (L2TP), a tunneling protocol used to support virtual private networks (VPNs).

Server IP Address: Fill in the L2TP Server IP address that provided by your Internet Service Provider (ISP).

Username and Password: Fill in the User Name and Password that provided by your ISP.

Address Mode: Select to use Static or Dynamic IP mode.

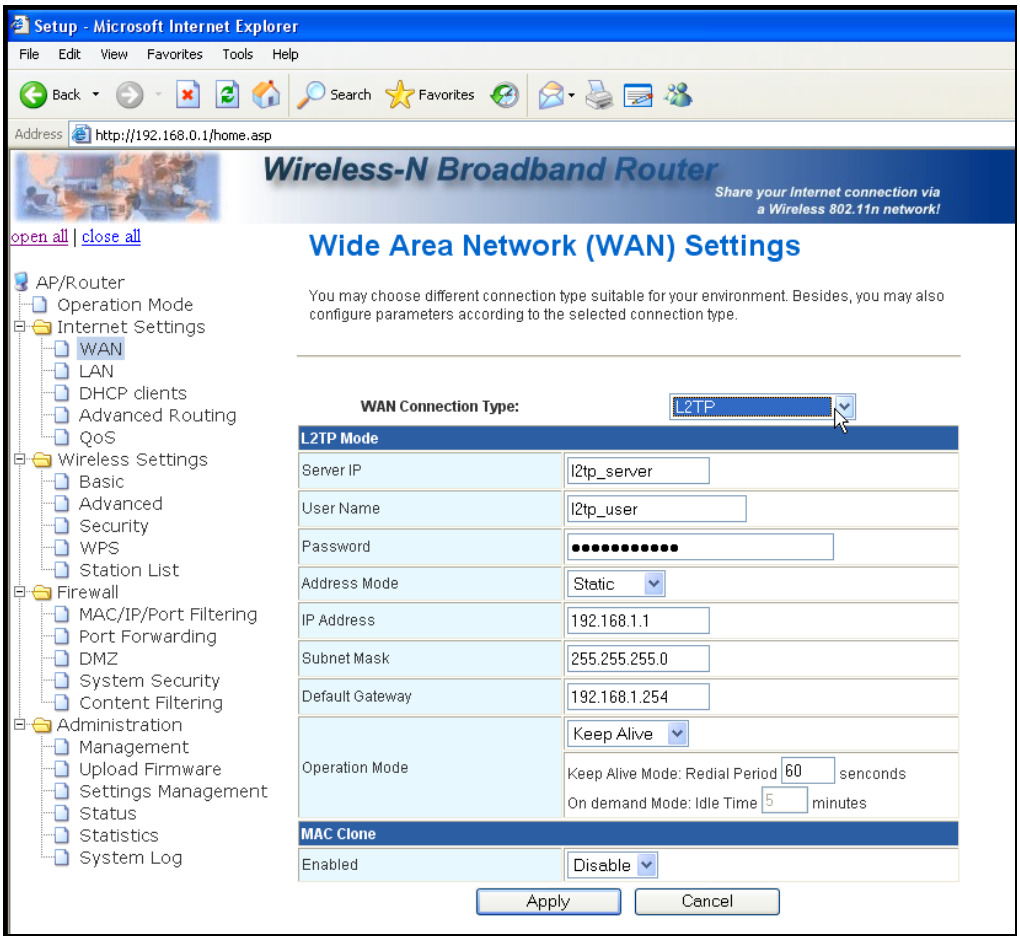
IP Address, Subnet Mask and Default Gateway: Fill in the IP address, Subnet Mask and Default Gateway that provided by your Internet Service Provider (ISP).

Operation Mode: Set the router as Keep Alive or On demand.

MAC Clone: Select to use the following MAC as the MAC address while serving Internet:

Original MAC: the MAC of the device.

Manual Settings: the MAC of your computer. Click on “Clone MAC Address from your Computer” to clone your computer MAC address in the blank. You can also change the MAC address if you need.



PPTP: Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks (VPNs).

Server IP Address: Fill in the PPTP Server IP address that provided by your Internet Service Provider (ISP).

Username and Password: Fill in the User Name and Password that provided by your ISP.

Address Mode: Select to use Static or Dynamic IP mode.

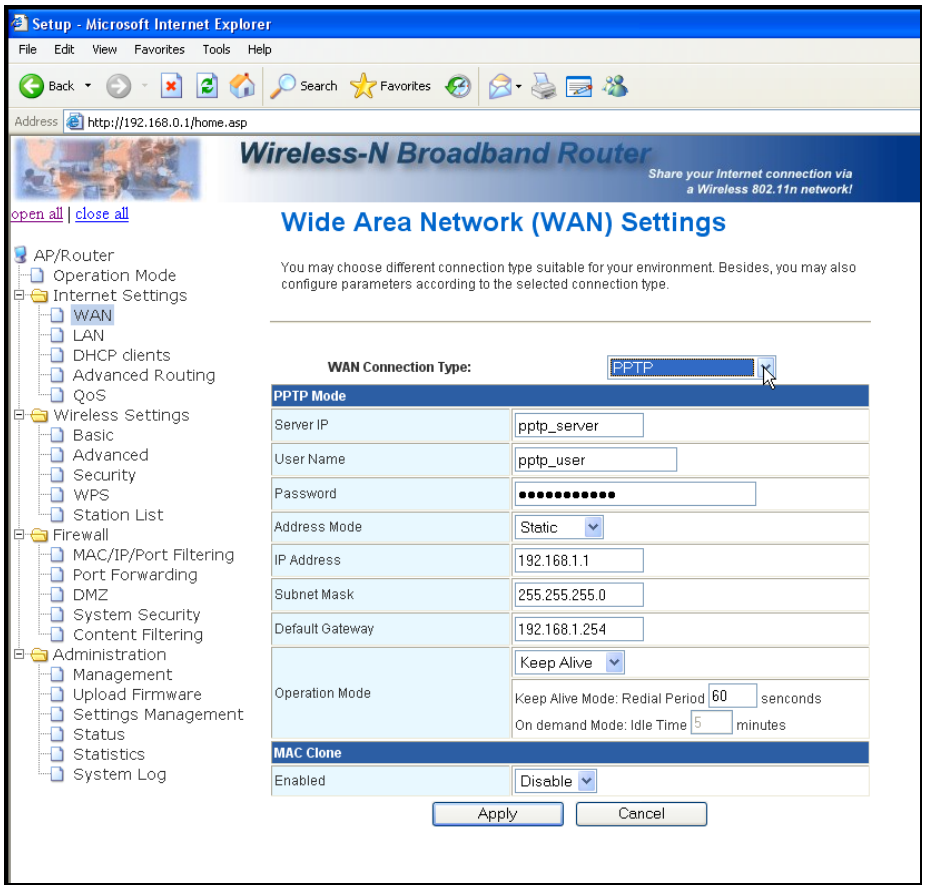
IP Address, Subnet Mask and Default Gateway: Fill in the IP address, Subnet Mask and Default Gateway that provided by your Internet Service Provider (ISP).

Operation Mode: Set the router as Keep Alive or On demand.

MAC Clone: Select to use the following MAC as the MAC address while serving Internet:

Original MAC: the MAC of the device.

Manual Settings: the MAC of your computer. Click on “Clone MAC Address from your Computer” to clone your computer MAC address in the blank. You can also change the MAC address if you need.



3.4.2 LAN Setting

To set up the configuration of LAN interface, private IP of your router LAN port and subnet mask for your LAN segment. Default IP is 192.168.0.1.

IP Address: The IP of your Router LAN port (default 192.168.0.1).

Subnet Mask: Subnet Mask of you LAN (default 255.255.255.0). All devices on the network must have the same subnet mask to communicate on the network.

LAN2: Enable / Disable LAN 2.

LAN2 IP: The IP address of LAN2.

LAN2 Subnet Mask: Subnet Mask of LAN2.

DHCP Type: To give your LAN Client an IP, you have to enable DHCP server. If not, manual setting up your client IP is necessary when you want to use the router as your client's default gateway.

Start IP Address: Specify the DHCP Client start IP address.

End IP Address: Specify the DHCP Client End IP address.

Note: The number of the "End IP" must be greater than "Start IP", and cannot be the same as the router's IP address.

DHCP Lease Time: Choose the length of the time for the device to recycle and give out the IP addresses to the devices in your network (default 86400).

Statically Assigned: Can statically assigned the client MAC and IP address. There are three IP can assign.

802.1d Spanning Tree: Enable/Disable. The Spanning Tree Protocol is an OSI layer-2 protocol that ensures a loop-free topology for any bridged LAN.

LLTD: Enable/Disable. Link Layer Topology Discovery (LLTD) is a proprietary Link Layer protocol for network topology discovery and quality of service diagnostics. It was developed by Microsoft as part of the Windows Rally set of technologies. The LLTD protocol operates over both wired (IEEE 802.3 Ethernet) as well as wireless (IEEE 802.11) networks.

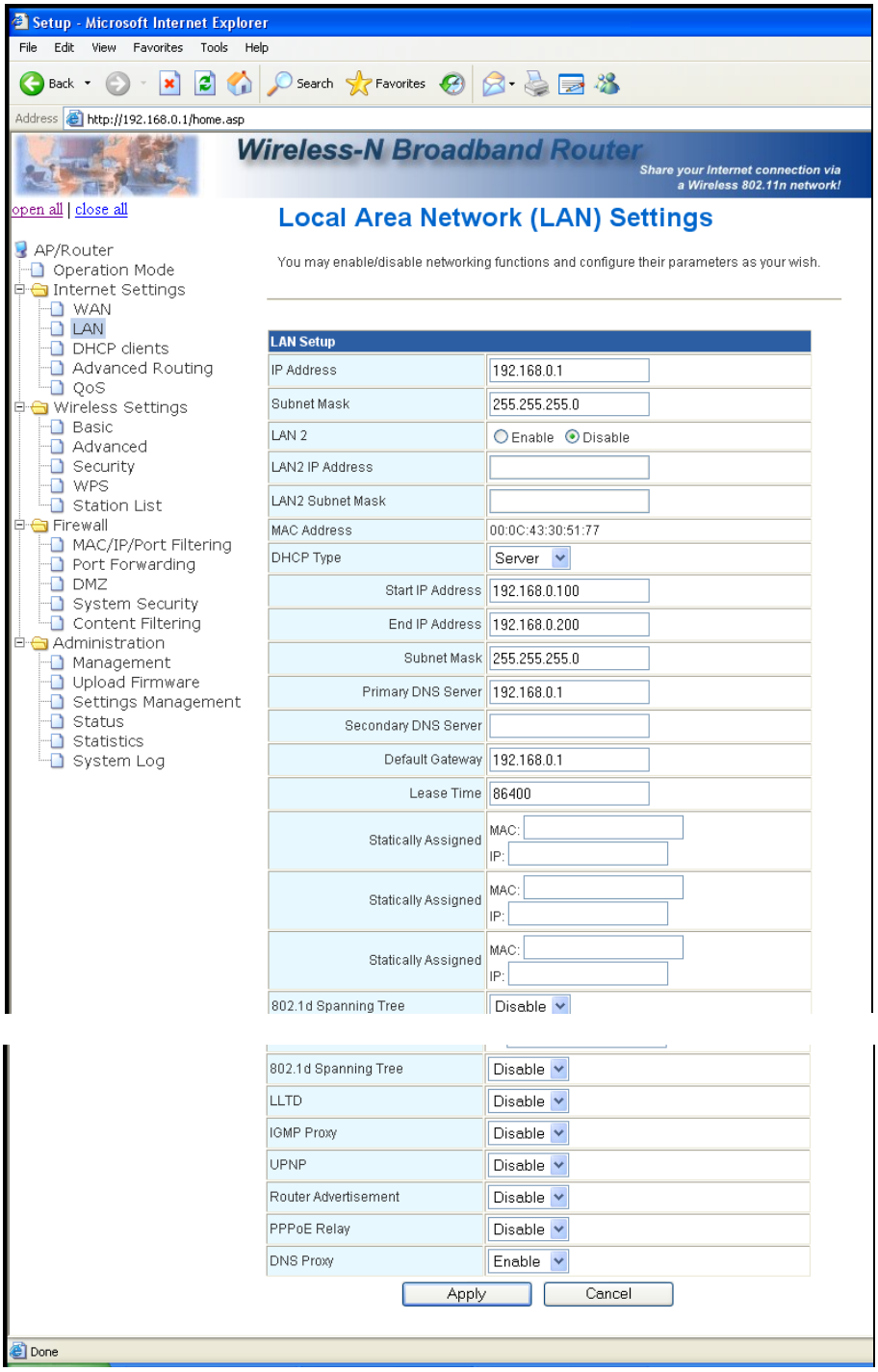
IGMP Proxy: Enable/Disable. IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts.

UPNP: Enable/Disable. (Universal Plug-and-Play). Network architecture based on TCP/IP and intended to allow terminals to be networked without the need for configuration. In the Barricade router, for example, the correct ports are automatically opened for applications like Net meeting, online games, etc. You can choose to enable or disable the UPnP Service.

Router Advertisement: Enable/Disable. The ICMP router discovery messages.

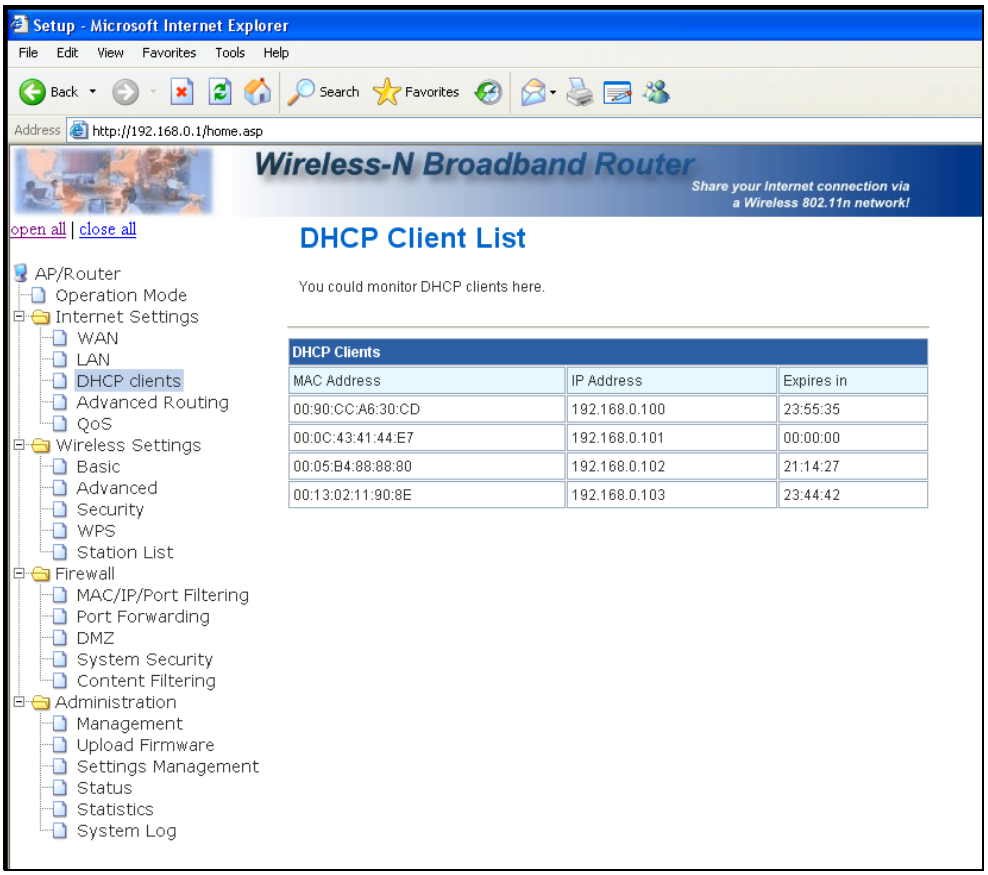
PPPoE Relay: Enable/Disable PPPoe Relay.

DNS Proxy: Enable/Disable DDNS Proxy.

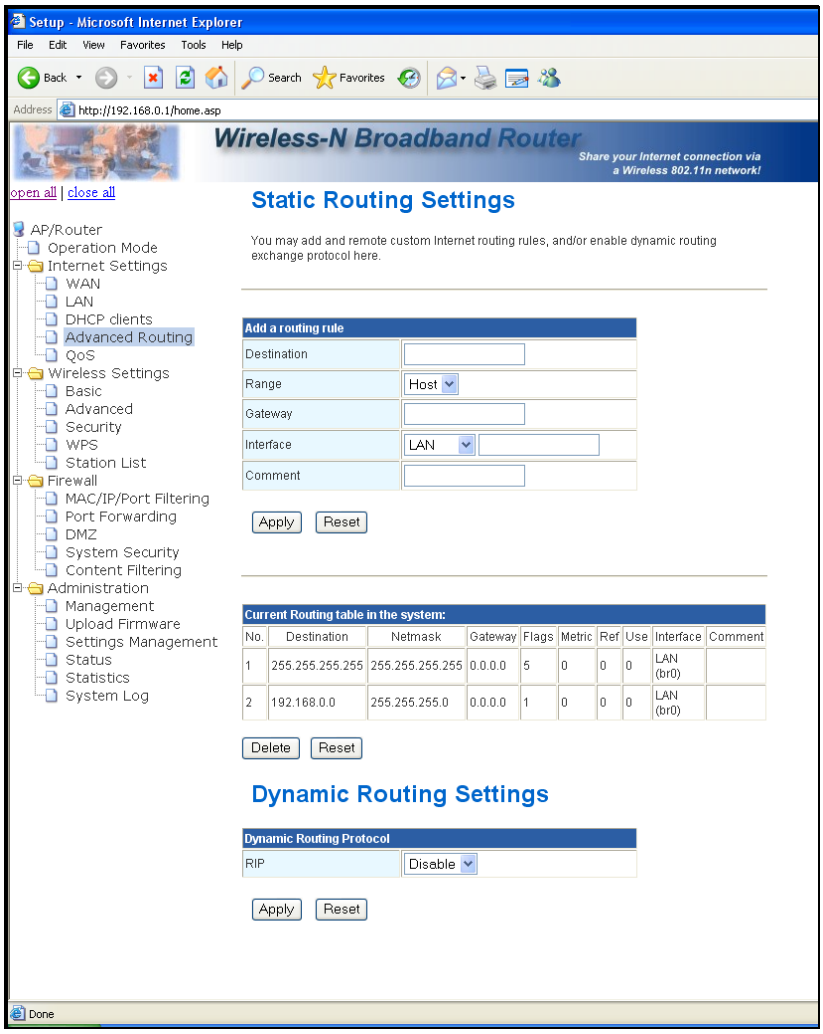

Setup - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.0.1/home.asp
Wireless-N Broadband Router
Share your Internet connection via a Wireless 802.11n network!
open all | close all
AP/Router
Operation Mode
Internet Settings
WAN
LAN
DHCP clients
Advanced Routing
QoS
Wireless Settings
Basic
Advanced
Security
WPS
Station List
Firewall
MAC/IP/Port Filtering
Port Forwarding
DMZ
System Security
Content Filtering
Administration
Management
Upload Firmware
Settings Management
Status
Statistics
System Log
Local Area Network (LAN) Settings
You may enable/disable networking functions and configure their parameters as your wish.
LAN Setup
IP Address 192.168.0.1
Subnet Mask 255.255.255.0
LAN 2 Enable Disable
LAN2 IP Address
LAN2 Subnet Mask
MAC Address 00:0C:43:30:51:77
DHCP Type Server
Start IP Address 192.168.0.100
End IP Address 192.168.0.200
Subnet Mask 255.255.255.0
Primary DNS Server 192.168.0.1
Secondary DNS Server
Default Gateway 192.168.0.1
Lease Time 86400
Statically Assigned MAC: IP:
Statically Assigned MAC: IP:
Statically Assigned MAC: IP:
802.1d Spanning Tree Disable
802.1d Spanning Tree Disable
LLTD Disable
IGMP Proxy Disable
UPNP Disable
Router Advertisement Disable
PPPoE Relay Disable
DNS Proxy Enable
Apply Cancel
Done

3.4.3 DHCP Clients Setting

The information of IP, MAC, address and expire time of the DHCP clients that have connected with this device.



3.4.4 Advanced Routing Setting



Static Routing Settings

User can set a route rule(table) in here..

Destination: The destination IP address.

Range: Host/Net, when select “Net”, there is another “Netmask” column need to fill out.

Gateway: The gateway for the routing.

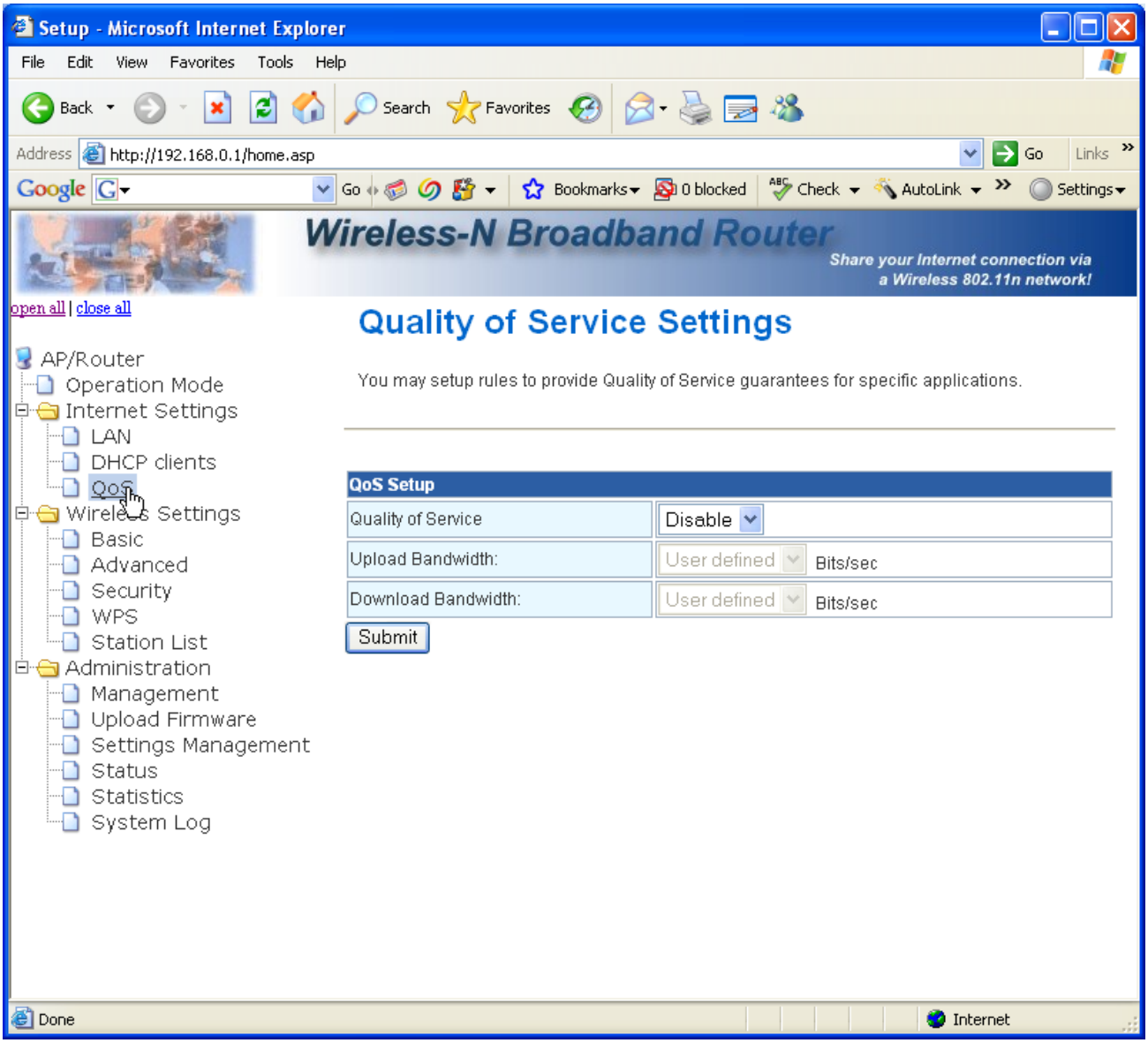
Interface: Via LAN/WAN or User can define by custom.

Comment: Memo for the routing rule.

Dynamic Routing Settings

Use RIP to auto build the routing rule. User can enable the dynamic routing settings in here.

3.4.5 QoS Setting



The QoS (Quality of Service) Settings page provides different priority to different users or data flows.

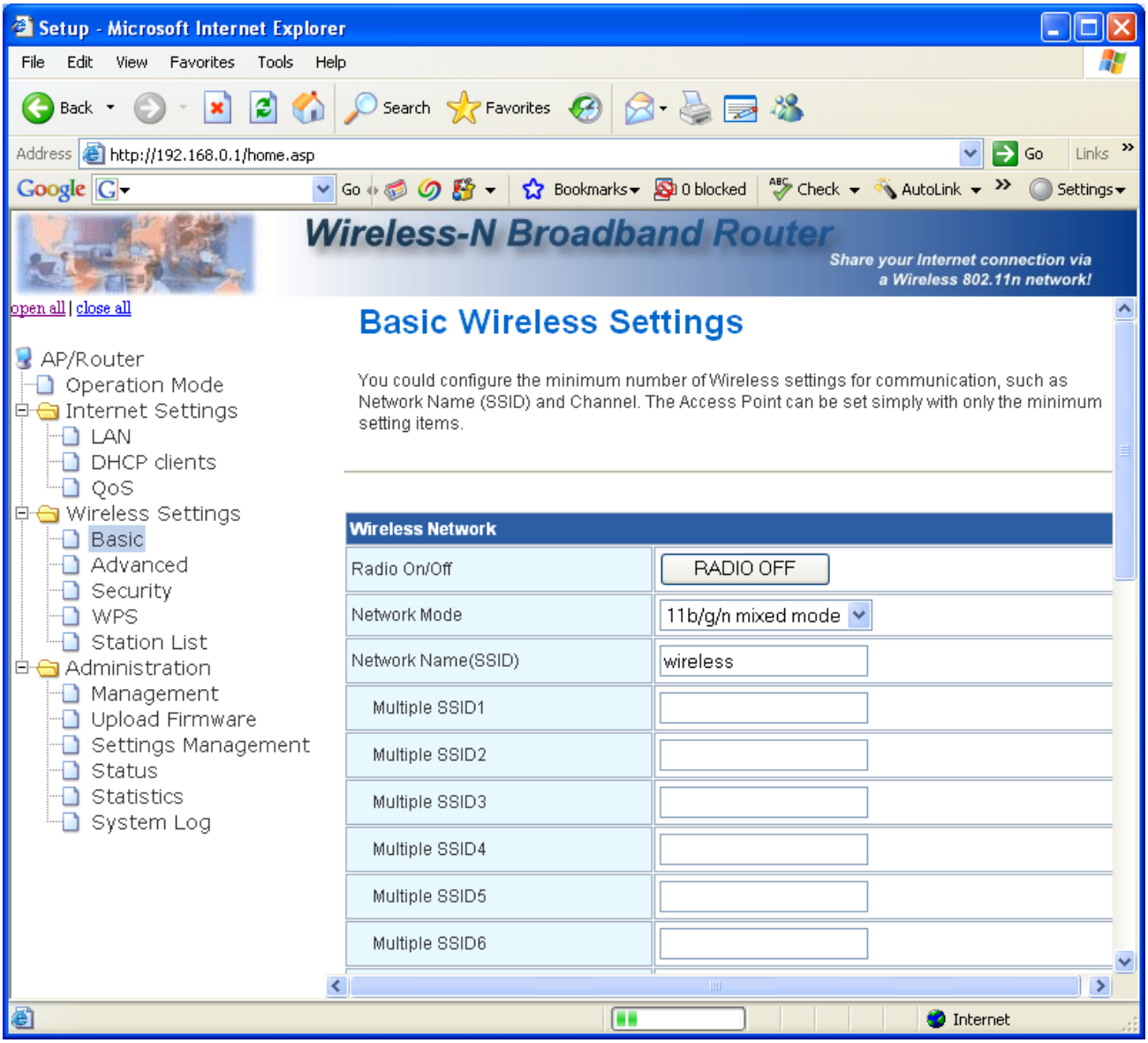
Quality of Service: Enable/Disable the QoS, default setting is Disable.

Upload Bandwidth: The parameter for upload bandwidth.

Download Bandwidth: The parameter for download bandwidth.

Please don't forget to submit when you finish the setting.

3.5.1 Wireless-Basic Setting



Radio Off: Enable/Disable the wireless.

Network Mode: There are 3 mode can choose, 11/b/g/n mixed mode/11b only/11g only.

SSID: set up the wireless ID, default is wireless.

Multiple SSID 1 ~ 7: You can set up to four SSID for this wireless network.

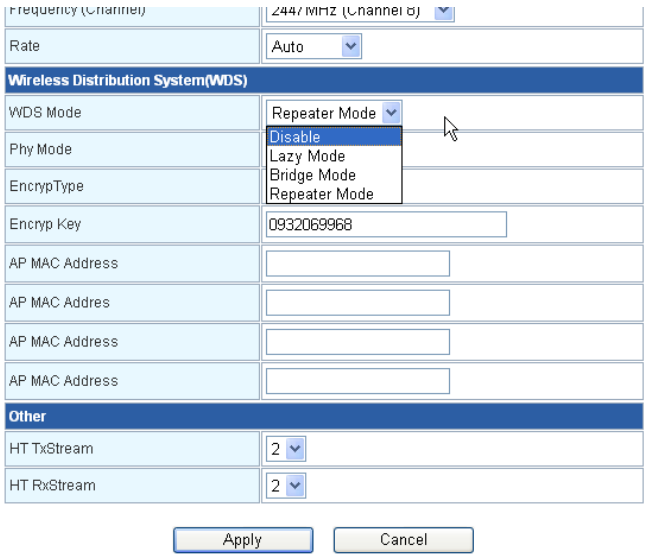
Broadcast Network Name(SSID): Enable/Disable the SSID broadcast.

AP Isolation: Enable/Disable this function. Create a separate virtual network for your wireless network. When this feature is enabled, each of your wireless clients will be in its own virtual network and will not be able to communicate with each other. You may want to utilize this feature if you have many guests that frequent your

wireless network.

MBSSID AP Isolation: Enable/Disable this function.

BSSID: Displays the Basic Service Set Identity (BSSID) of this router. This parameter is the same as the MAC address of LAN port.



WDS (Wireless Distribution System):

WDS Mode: Default is Disable, there are 3 Mode can choose, Lazy Mode(Auto), Bridge Mode(Bridge Only) and Repeater Mode(AP + Bridge).

Phy Mode: Select the option in the drop-down list to enable CCK, OFDM, HTMIX, or GREENFIELD mode for physical layer transceivers.

EncrypType: Select the option in the drop-down list to enable WEP, TKIP, and AES encryption types. If you select None, any data will be transmitted without encryption and any station can access the router.

EncrypKey: For encryption type of TKIP and AES, you have to fill in the WPA encryption key. Please use Pass Phrase (8~32bytes) key format.

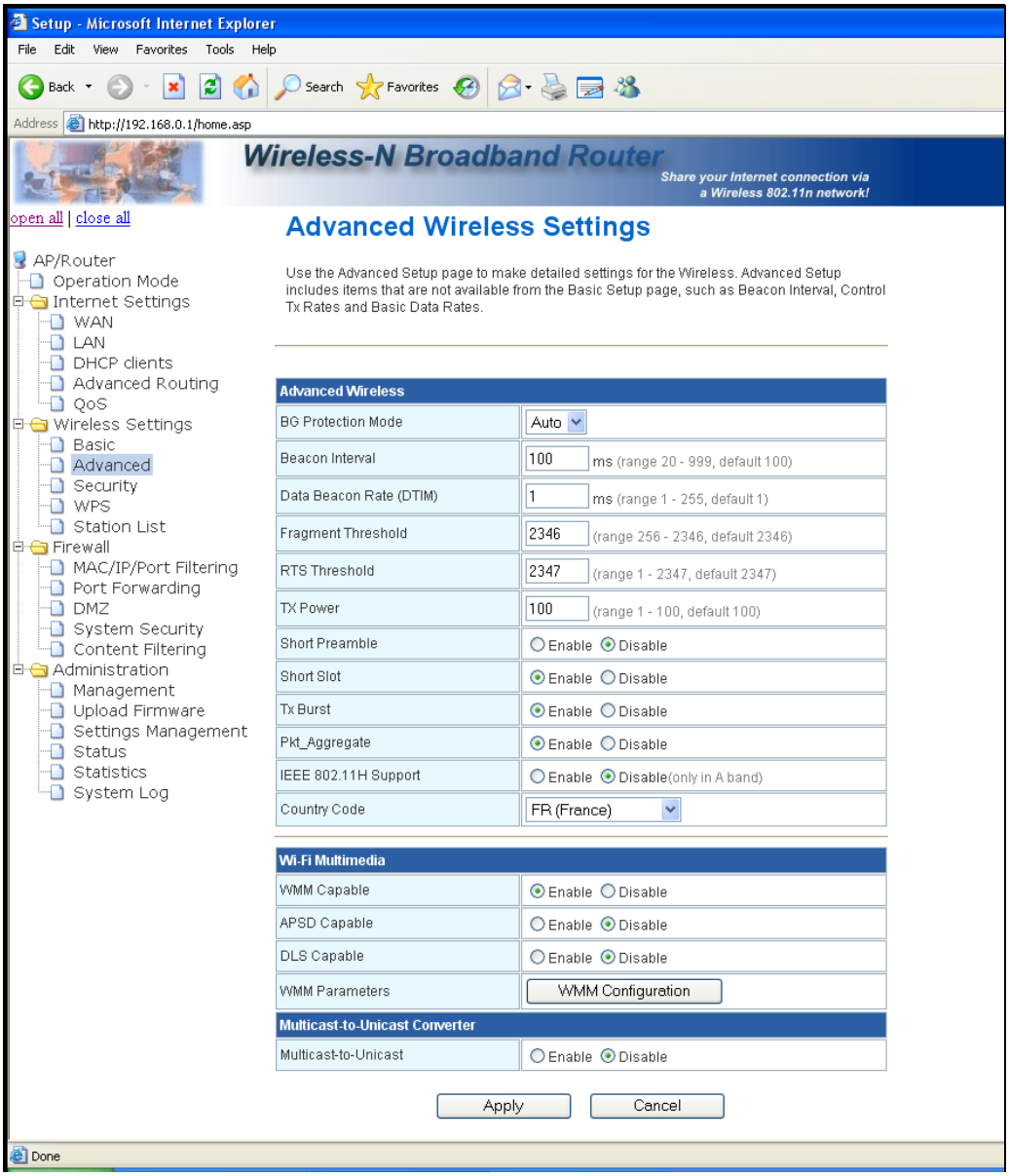
AP MAC Address: For encryption type of TKIP and AES, you have to fill in the WDS AP MAC. You can fill up to 4 sets of WDS AP MAC lists.

Other :

HT TxStream: Set the Tx via 1 or 2 antennas.

HT RxStream: Set the Rx via 1 or 2 antennas.

3.5.2 Advanced Setting



Advanced Wireless:

BG Protection Mode: Some 802.11g wireless adapters support 802.11g protections, which allows the adapter search for 802.11b/g singles only. Select “Auto” to turns it on or off automatically, select “On” to support protection or select “Off” to disable this function.

Beacon Interval: Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. Default (100ms) is recommended.

Data Beacon Rate(DTIM): Enter a value between 1 and 255 (default 1) for the Delivery Traffic Indication Message (DTIM). A DTIM is a countdown informing clients of the next window for listening to broadcast and

multicast messages.

Fragment Threshold: This value should remain at its default setting of 2346. If you experience a high packet error rate, you may slightly increase your fragmentation threshold within the value range of 0 to 2346. Setting the fragmentation threshold too low may result in poor performance.

RTS Threshold: Request To Send threshold. This value should remain at its default setting of 2347. If you encounter inconsistent data flow, only minor modifications to the value range between 1 and 2347 are recommended.

Tx Power: Transmit power. You can set the output power of wireless radio. This value should remain at its default setting of 100. If you

Short Preamble: The length of CRC blocks in the frames during the wireless communication.

Short Slot: Indicates that the 802.11g network is using a short slot time because there are no legacy (802.11b) stations present

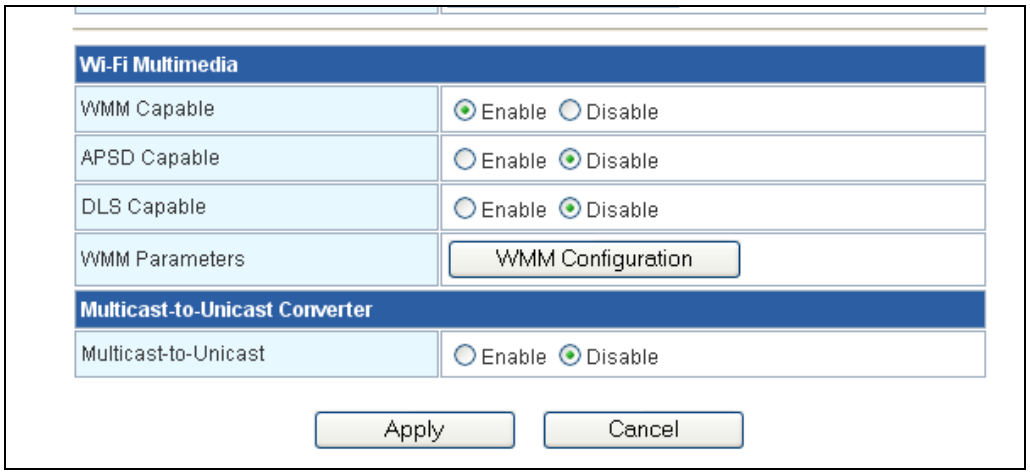
Tx Burst: Select to enable or disable connecting to a Tx Burst supported device.

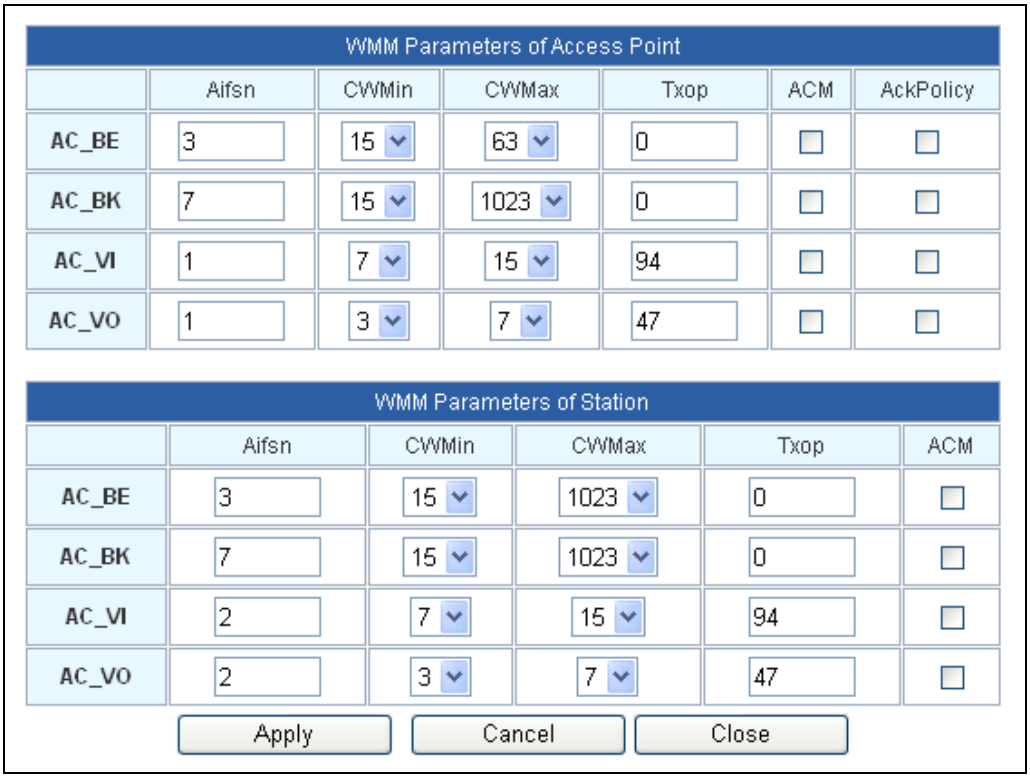
Pkt_Aggregate: To aggregate lots of packets into a big one before transmitting packets. This can reduce control packet overhead.

IEEE 802.11H Support: Enable/Disable.

Country Code: Select wireless country code. Six countries can choose.

Wi-Fi Multimedia:





WMM Capable: This will enhance the data transfer performance of multimedia contents when they're being transferred over wireless network.

APSD Capable: Automatic Power saves Delivery. Select to enable / disable data flow using power saving mode during transmitting.

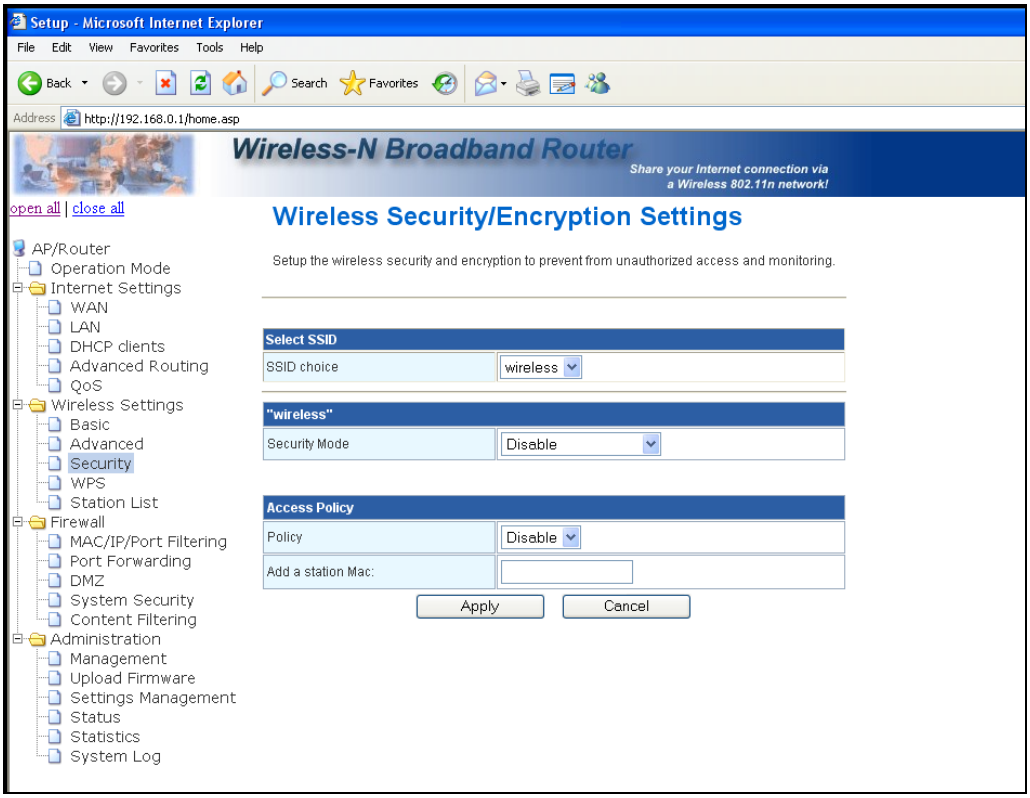
DLS Capable: Enable/Disable this function.

WMM Parameters: You can configure WMM parameters by clicking on the WMM Configuration button. The

configuration window pops up (as shown below). Manually configure the parameters and click on the “Apply” button to execute.

Multicast-to-Unicast: It can receives Multicast streams from the network backbone, converts them to Unicast format, and routes them to the set-top-boxes of end-users over the last mile infrastructure (e.g. DSL, Ethernet, WiFi).

3.5.3 Security Setting



SSID Choice: Please choose a SSID you have set for this router in the Wireless Settings > Basic Settings from the drop-down list. The SSID will be shown on the wireless network for recognizing..

Security Mode: There are 10 modes for you to select: Open, Shared, WEP Auto, WPA, WPA-PSK, WPA2, WPA2-PSK, and WPA-PSKWPA2-PSK, WPA1WPA2, 802.1x. Please refer to the following description.

Security Mode -- Open / WEP Auto

Default Key: Select to use the WEP key value of 1, 2, 3 or 4 as in the following settings.

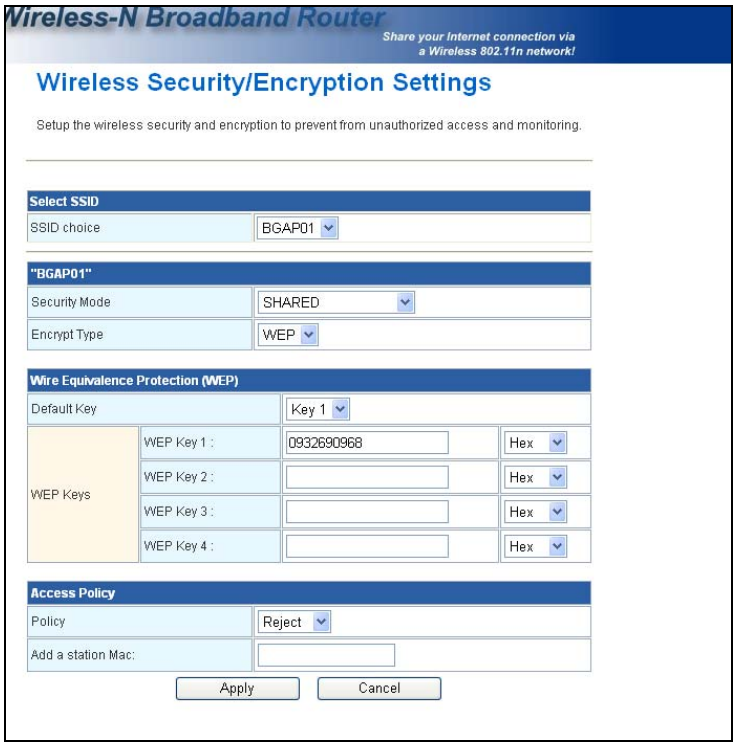
WEP Keys: Select ASCII or Hex to setup the key value. ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers from 0-127. Hexadecimal digits consist of the numbers 0-9 and the letters A-F.

Access Policy:

Policy: Default is Disable, you can allow or Reject the wireless station.

Add a station Mac: Fill out the MAC address of wireless station you want to allow or reject.

Security Mode -- Shared



Default Key: Select to use the WEP key value of 1, 2, 3 or 4 as in the following settings.

WEP Keys: Select ASCII or Hex to setup the key value. ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers from 0-127. Hexadecimal digits consist of the numbers 0-9 and the letters A-F.

Access Policy:

Policy: Default is Disable, you can allow or Reject the wireless station.

Add a station Mac: Fill out the MAC address of wireless station you want to allow or reject.

Security Mode -- WPA-PSK / WPA2-PSK / WPA-PSK + WPA2-PSK

WPA Algorithms: Mark the option to enable modes of TKIP, AES, or TKIPAES (TKIPAES is only available in the security modes of WPA2-PSK and WPAPSK + WPA2-PSK)

Pass Phrase: Enter a pass phrase encryption key format (8~32 bytes).

Key Renewal Interval: Enter a value to setup the WPA key renewal interval. The device regenerates the key in every interval seconds that you have setup without disconnection.

Access Policy:

Policy: Default is Disable, you can allow or Reject the wireless station.

Add a station Mac: Fill out the MAC address of wireless station you want to allow or reject.

Security Mode -- WPA / WPA2 / WPA1 + WPA2 / 802.1x

WPA Algorithms: Mark the option to enable modes of TKIP, AES, or TKIPAES (TKIPAES is only available in the security modes of WPA2-PSK and WPAPSK + WPA2-PSK)

Key Renewal Interval: Enter a value to setup the WPA key renewal interval. The device regenerates the key in every interval seconds that you have setup without disconnection.

Radius Server:

IP Address: Radius Server IP address.

Port: The default port number is 1812.

Shared Secret: The default is “ralink”.

Session Timeout: default is 0.

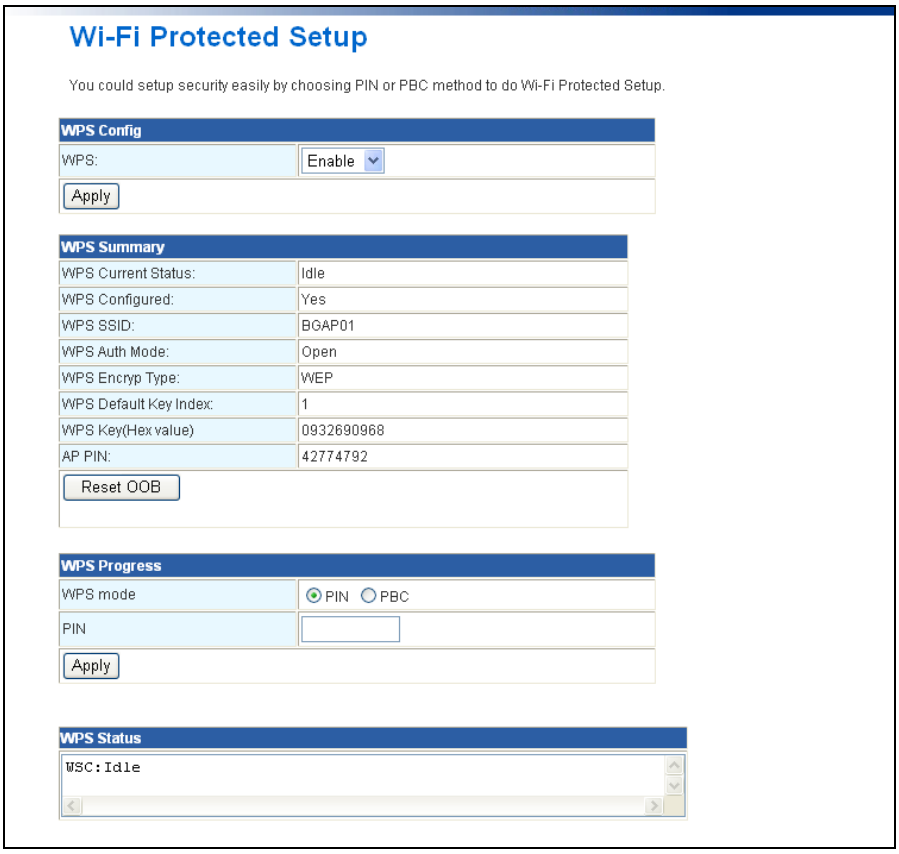
Idle Timeout: The idle timeout setting.

Access Policy:

Policy: Default is Disable, you can allow or Reject the wireless station.

Add a station Mac: Fill out the MAC address of wireless station you want to allow or reject.

3.5.4 WPS Setting



The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. This Router supports the configuration setup using PIN configuration method or PBC configuration method through an internal or external Registrar.

WPS: Enable/Disable the WPS. Default setting is disable.

WPS Summary: Shows the information of WPS current status, configured, SSID, authentication mode, and pre-shared key. Click on Reset OOB button to Reset WPS AP to the OOB (out of box) configuration.

WPS Progress: Show the WPS current status.

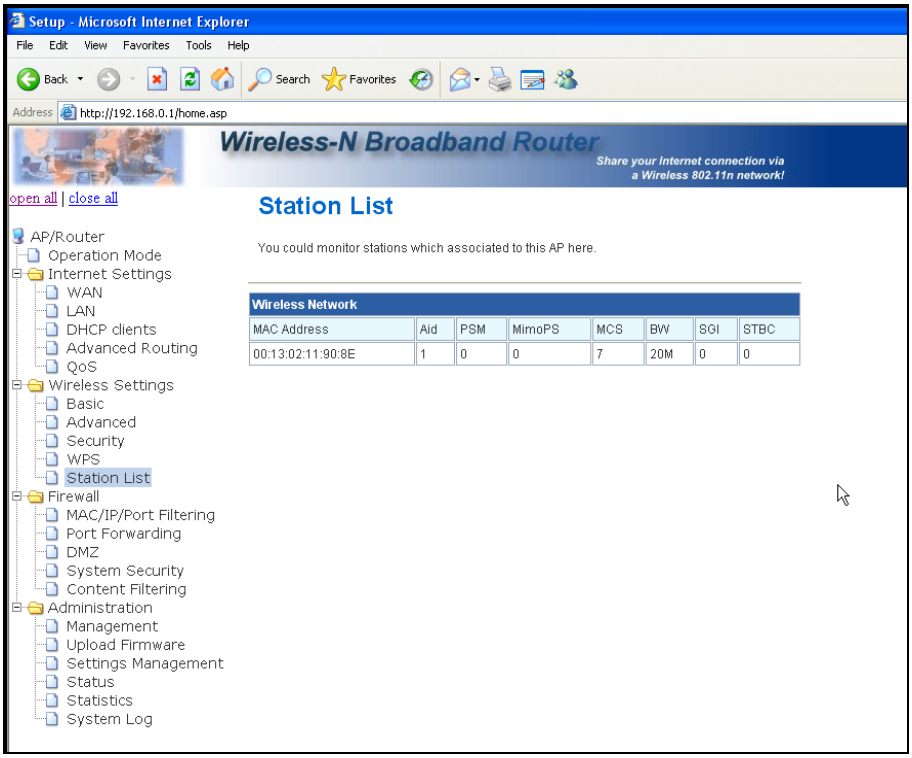
WPS mode:

PIN method (Personal Identification Number): read the PIN from either a sticker on the new STA or a display.

PBC method (Push Button Communication): in which the user simply has to push a button, either an actual or virtual one, on both the AP and the new STA. (Users can simply push the

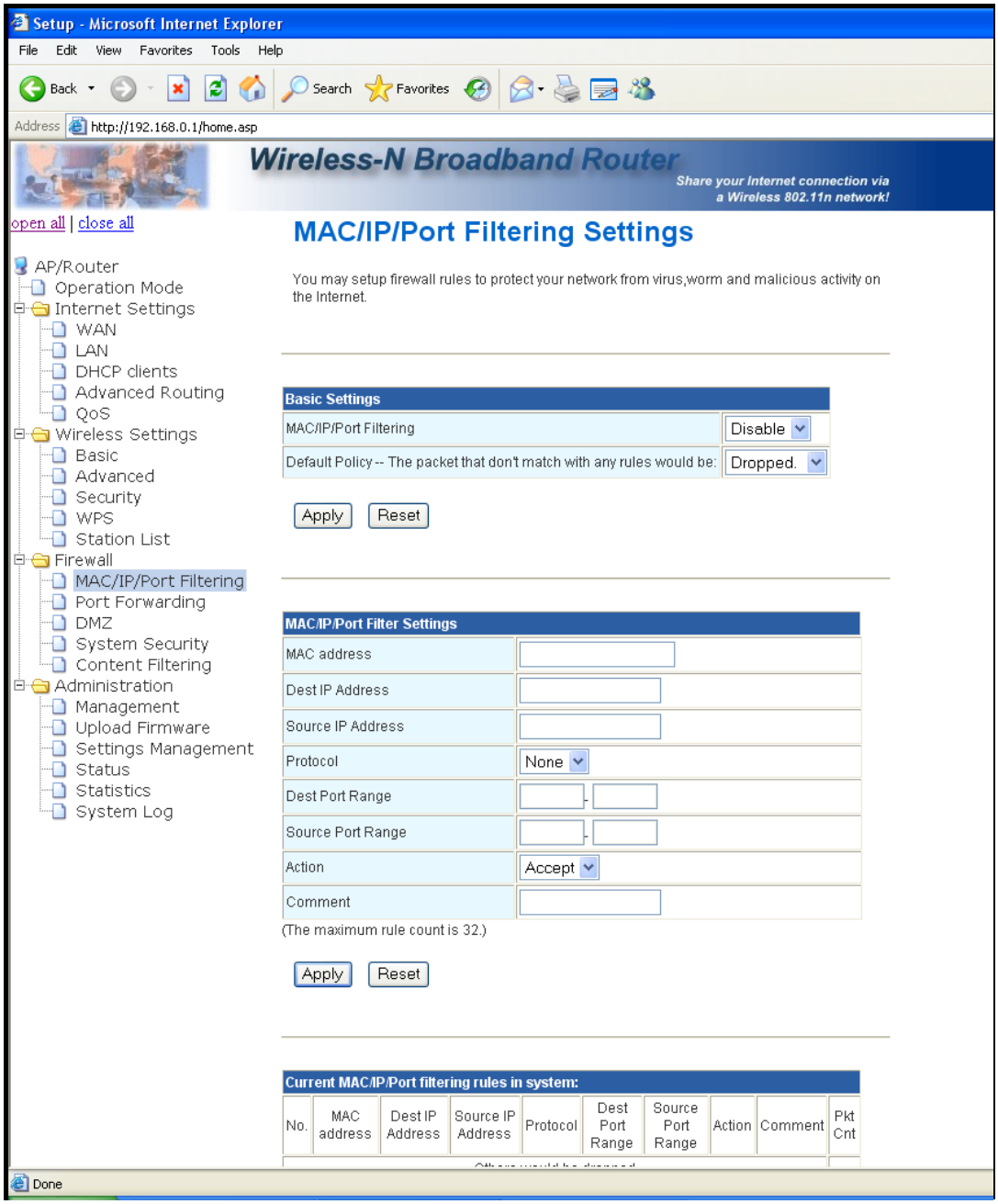
PIN: Users have to fill in the PIN code to enrollee device if selecting PIN mode as the WPS Config method.

3.5.5 Station List



Monitor Stations which associated to this AP/Router here.

3.6.1 MAC/IP/Port Filtering Setting



The Wireless Router could filter the outgoing packets for security or management consideration. You can set up the filter against the IP addresses to block specific internal users from accessing the Internet. The firewall could not only obstruct outside intruders from intruding your system, but also restricting the LAN users. Port filter restricts certain type of data packets from your LAN to Internet through the router.

Basic Settings:

MAC/IP/Port Filtering: Enable/Disable the function.

Default Policy - The packet that don't match with any rules would be: Dropped/Accepted.

MAC/IP/Port Filtering Settings:

MAC address: Fill out the MAC address that you wish to filter.

Dest IP Address: Fill in the destination IP address that you wish to filter.

Source IP Address: Fill in the source IP address that you wish to filter.

Protocol: Select the protocol type of TCP, UDP or ICMP.

Dest Port Range: Fill in the destination port range that you wish to filter.

Source Port Range: Fill in the source port range that you wish to filter.

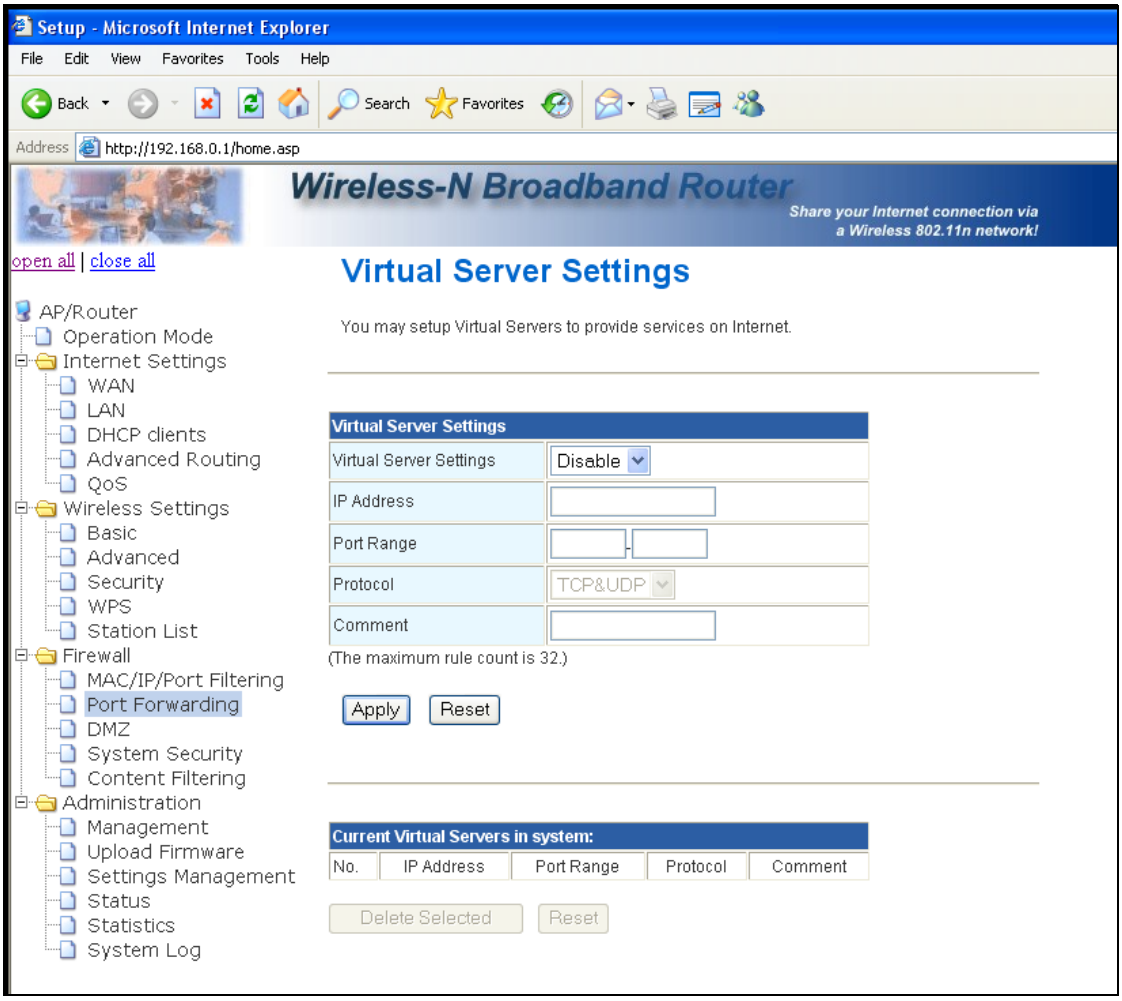
Action: Accept or Drop the action.

Comment: Input any text to describe this mapping, up to 16 alphanumerical characters.

IP / Port Filter Rule List

Lists the IP / Port Filter Settings you have added before. Click on the list to change configuration, or the delete button to delete the list.

3.6.2 Port Forwarding Setting



Virtual Server help redirect requests from computers on the LAN to a server set up on the LAN. You can setup an Internet service on the computer on local network, without exposing it on Internet directly. You can also build many sets of port redirection, to provide many different Internet services on different local computers via a single Internet IP address.

Virtual Server Settings: Enable/Disable.

IP Address: Fill in the IP of your LAN Server.

Port Range: Fill in the port range that you wish to filter.

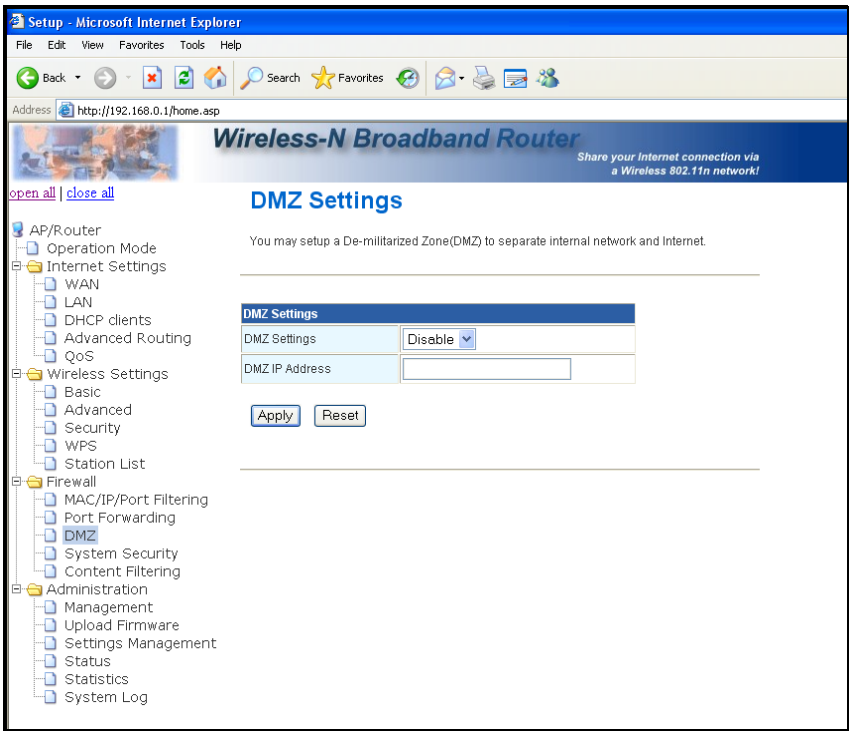
Protocol: Select the protocol type of TCP, UDP or Both.

Comment: Input any text to describe this mapping, up to 16 alphanumerical characters.

Virtual Server Mapping List

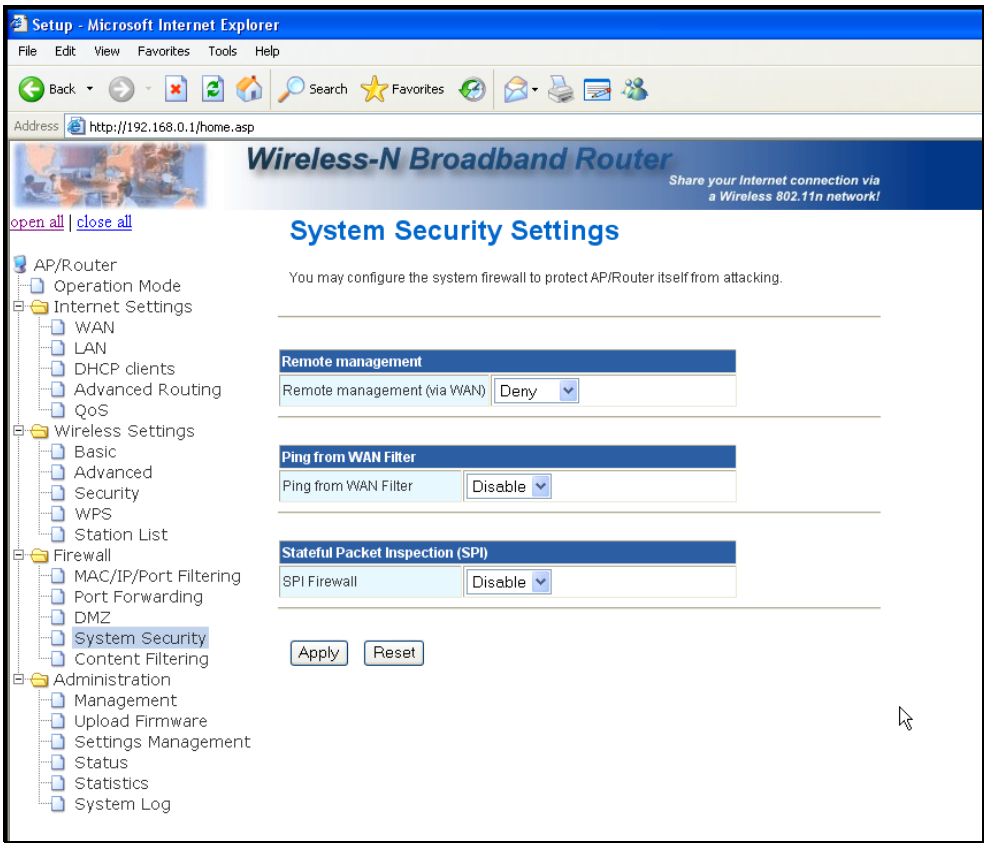
Lists the Virtual Server Settings you have added before. Click on the list to change configuration, or the Delete button to delete the list.

3.6.3 DMZ Setting



The virtual DMZ (Demilitarized Zone) is used to enable protocols, which need to open ports on the router. The router will forward all unspecified incoming traffic to the host specified in this page. To configure it, mark to enable virtual DMZ and then enter the Host IP (private IP address) and click **Apply** to enact the setting.

3.6.4 System Security Settings

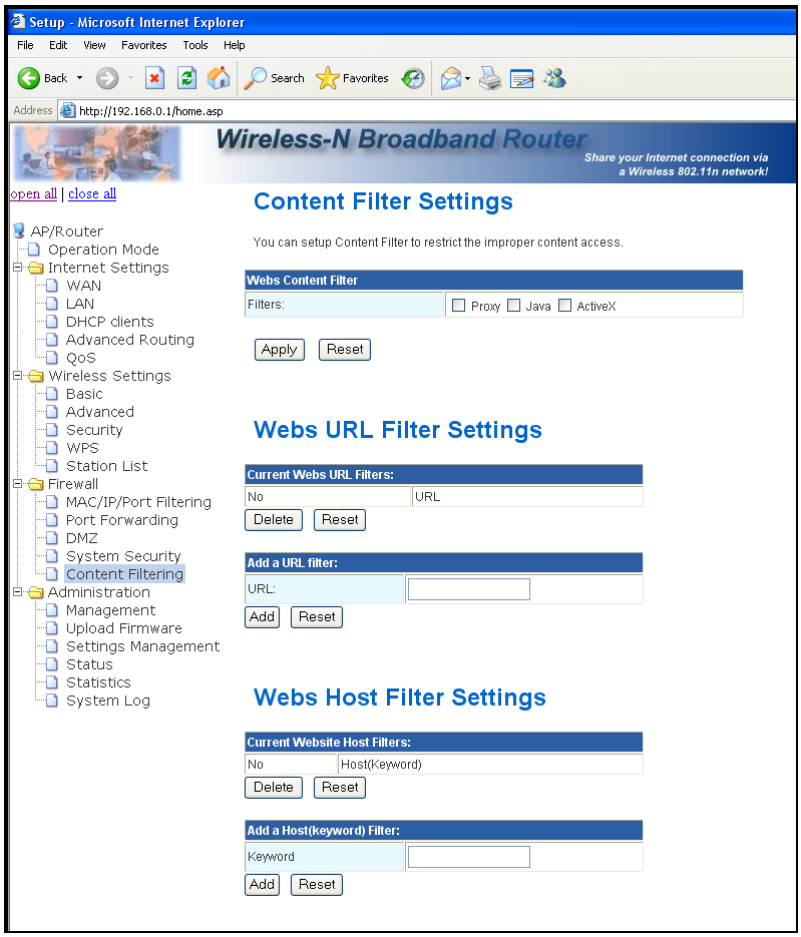


Remote Management via WAN: Allow/Deny.

Ping from WAN filter: Disable/Enable.

Stateful Packet Inspection (SPI): Disable/Enable.

3.6.5 Content Filtering Settings



User can set up content filter to restrict the importer content access.

Webs Content Filter: Can filter Proxy/Java or ActiveX.

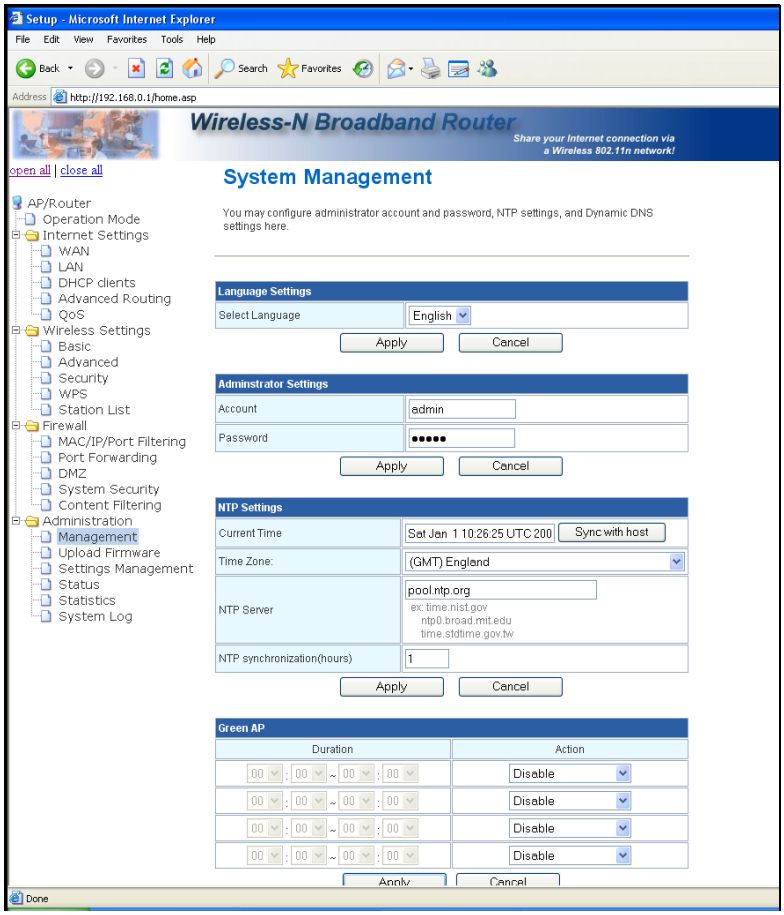
Webs URL Filter Settings:

Add a URL filter: Fill in the URL you want to filter.

Webs Host Filter Settings

Add a Host(Keyword) Filter: Fill in the keyword which you want to filter.

3.7.1 Management Settings



Language Settings: Can select language which you want.

Administrator Settings: Set the account and password to set and manage the Wireless Device.

NTP Settings: Can set the NTP server here.

Green AP: Can set the save mode for the device, set the duration and Wi-Fi Tx power.

DDNS Settings:

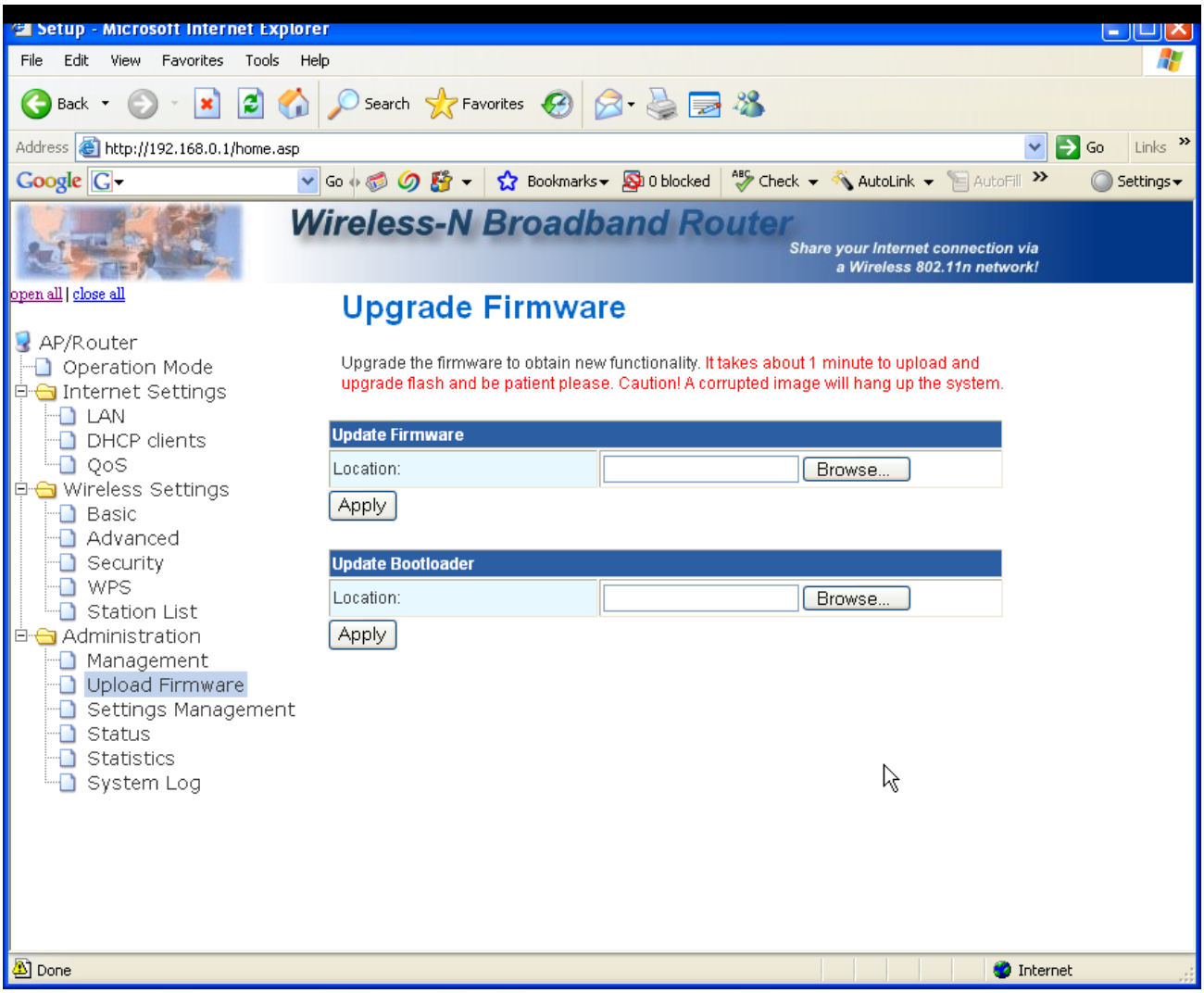
Dynamic DNS Provider: The website that provides DDNS service. Please select from the drop-down list.

Account: DDNS login account. For DynDNS users, please fill in your user name; for No-IP and TZO users, please fill in your email address.

Password: The password of your DDNS service account.

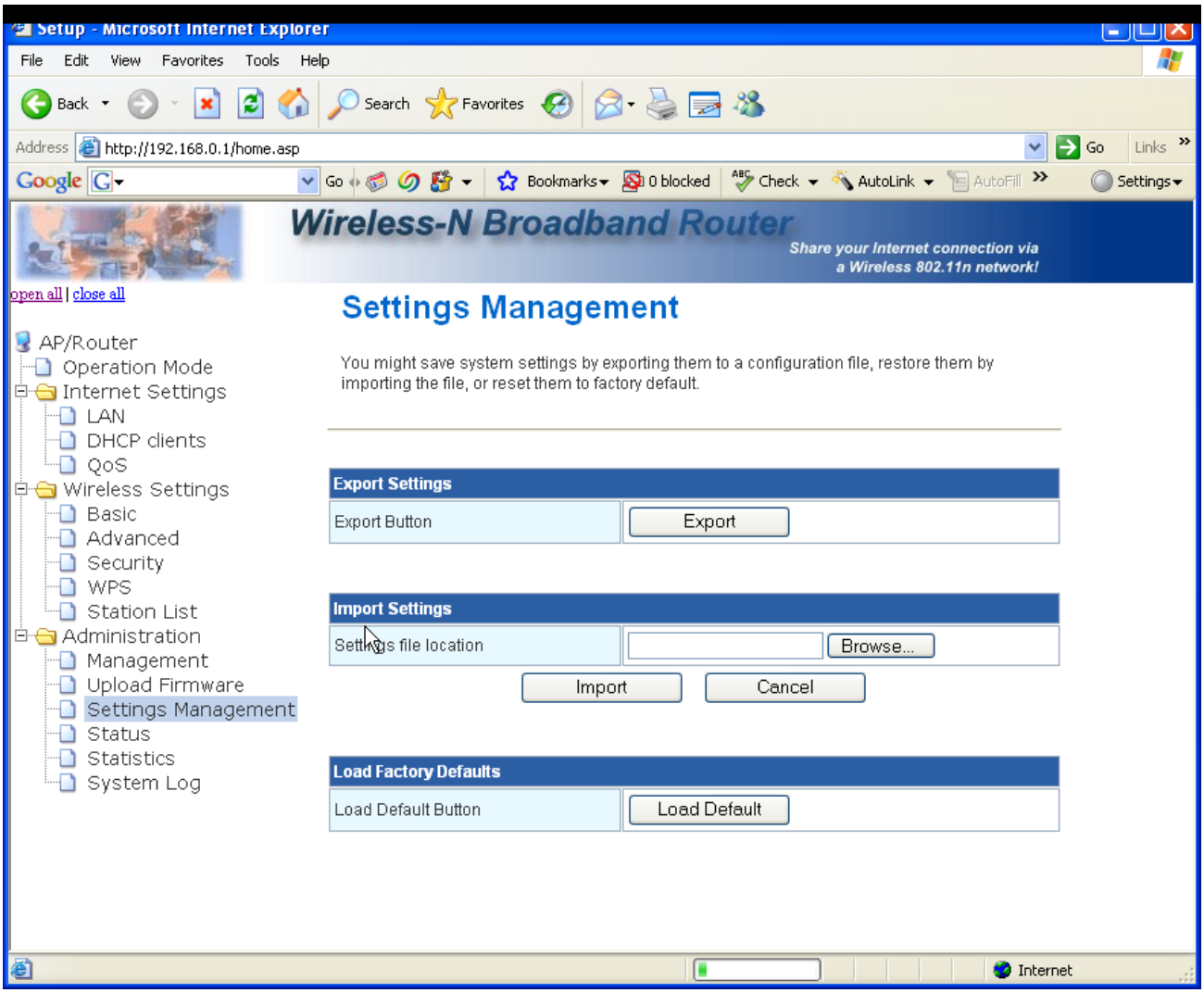
DDNS: The hostname that you have applied for the device.

3.7.2 System Log



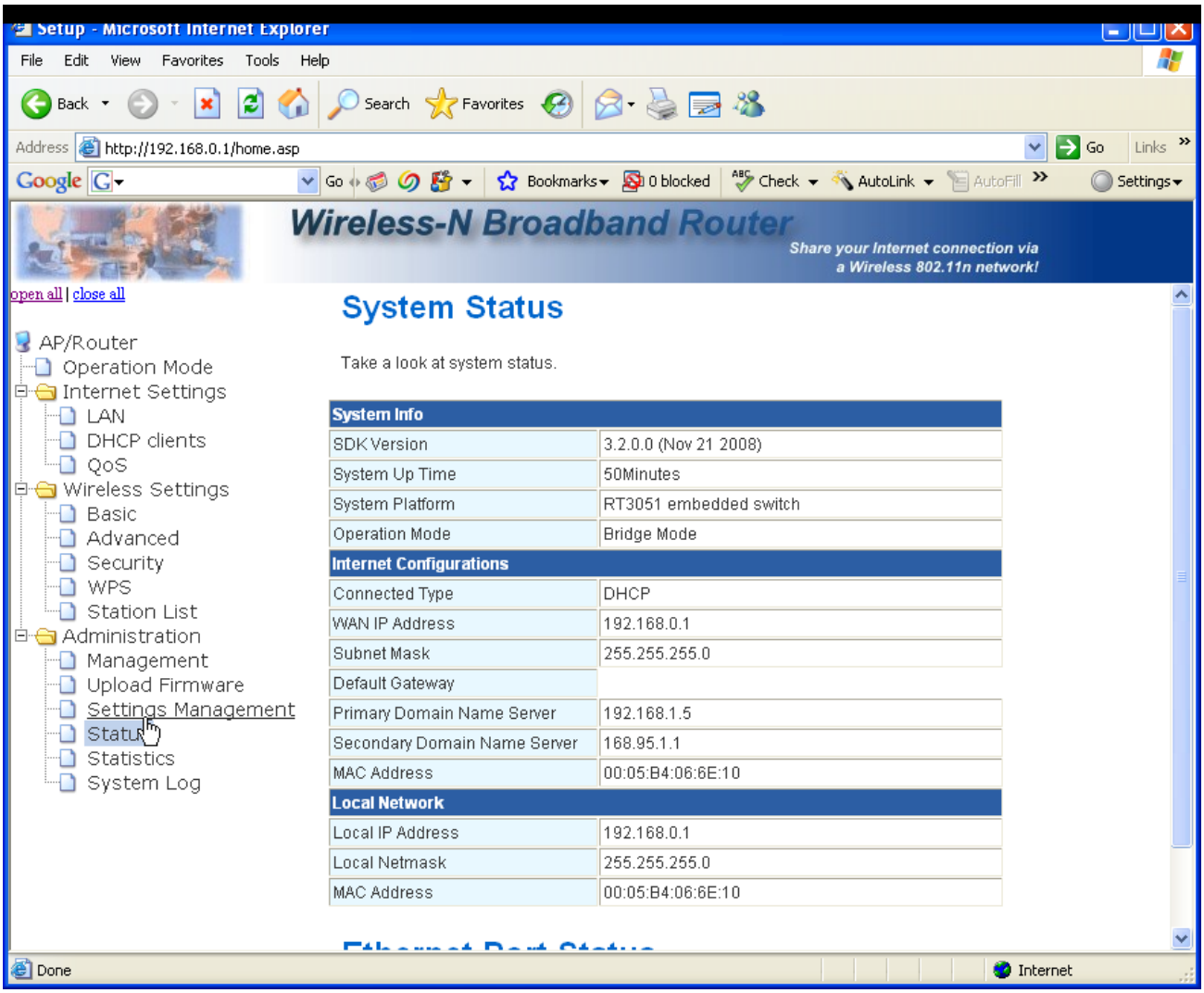
User can upgrade the firmware in this page. Be careful, don't power off when doing the upgrade process.

3.7.3 Settings Management



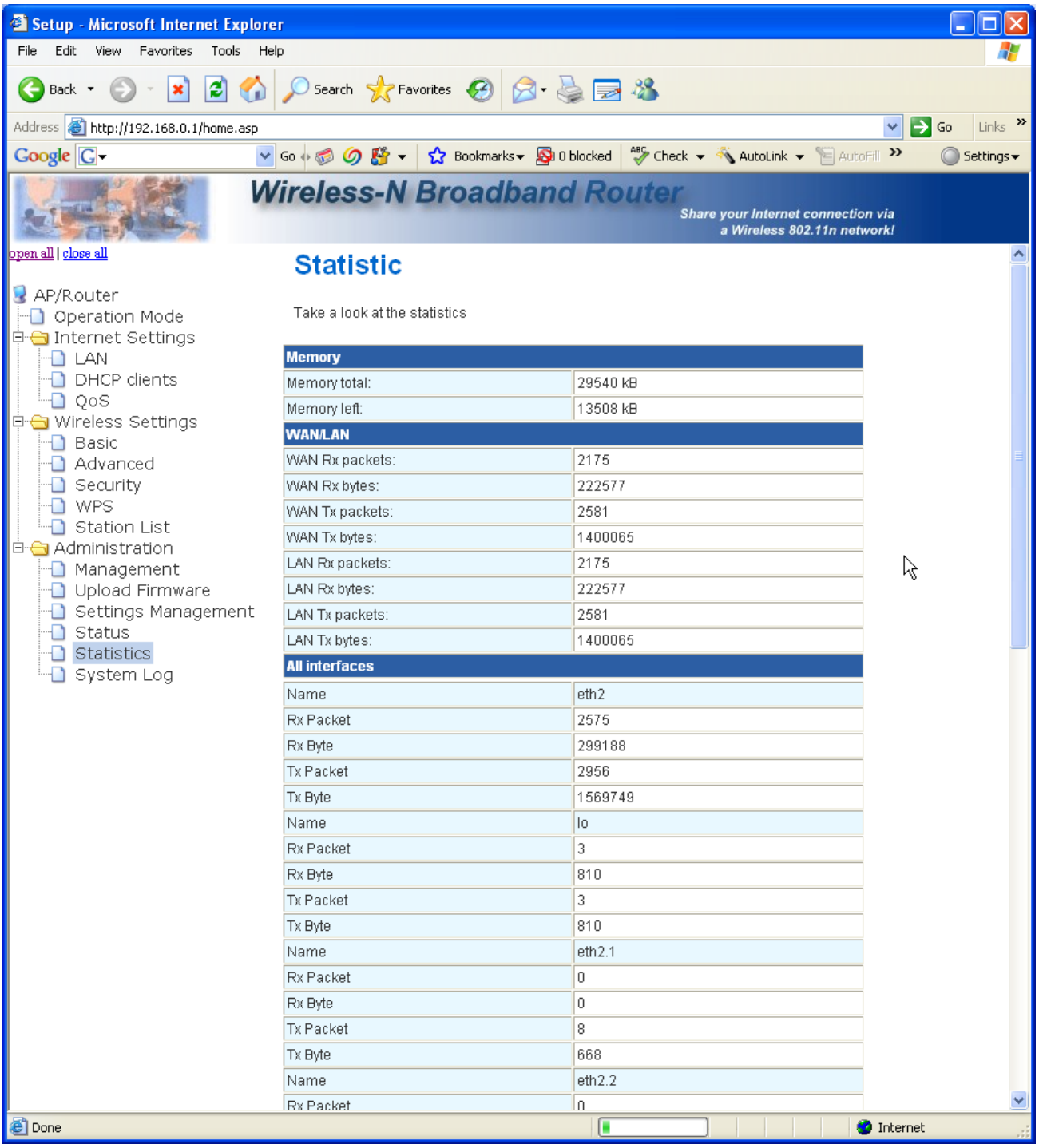
Users can Export Settings or Import Settings here. If want to load the factory defaults, please click the Load default button.

3.7.4 System Status



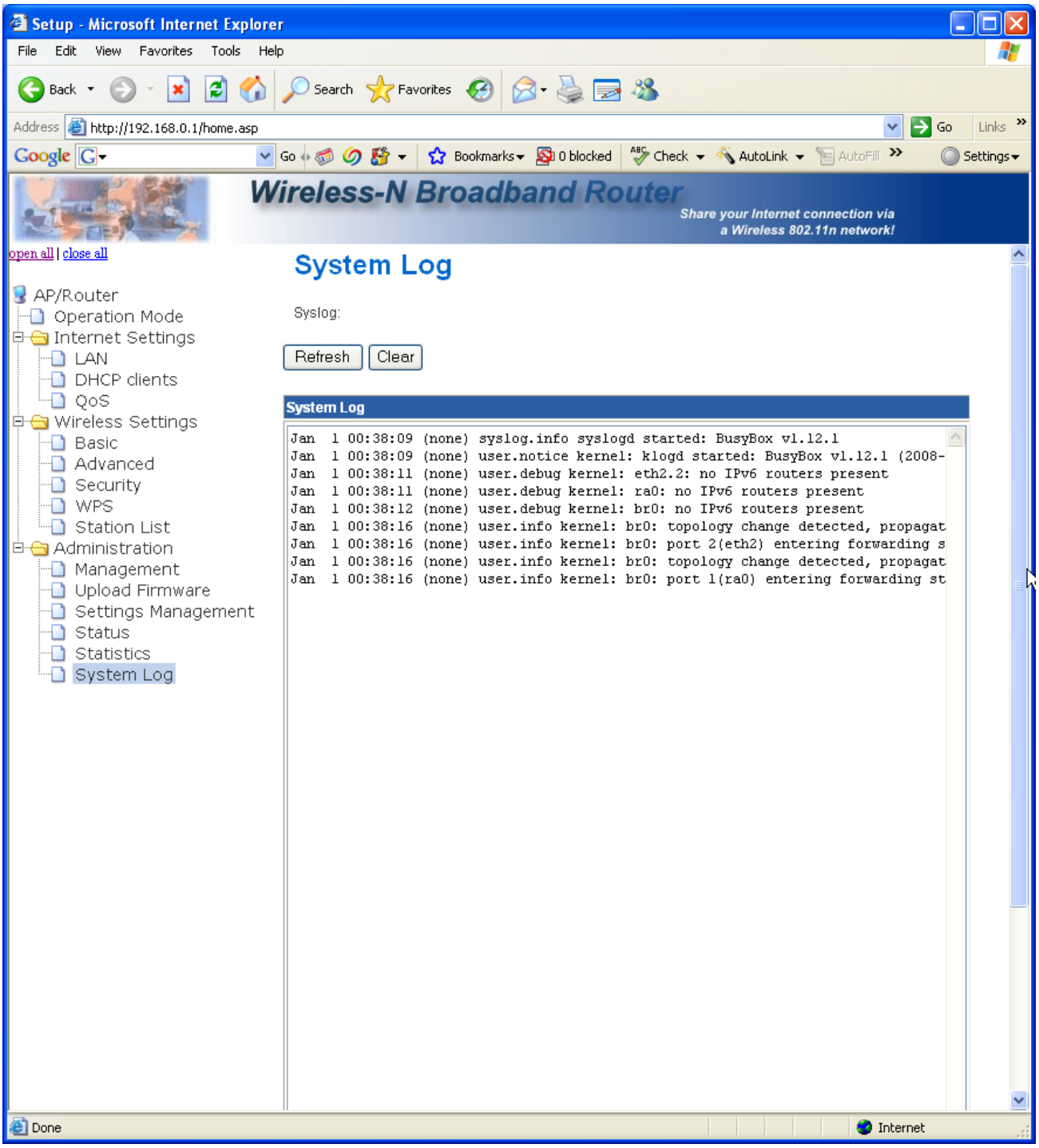
You can check the device status in this page, The firmware version, Internet Configuration and LAN settings.

3.7.5 Statistic



This page allows users to get information of data transferring condition, and monitor the status and performance of this router including interface, receiving/sending packets, and receiving/sending errors.

3.7.6 System Log

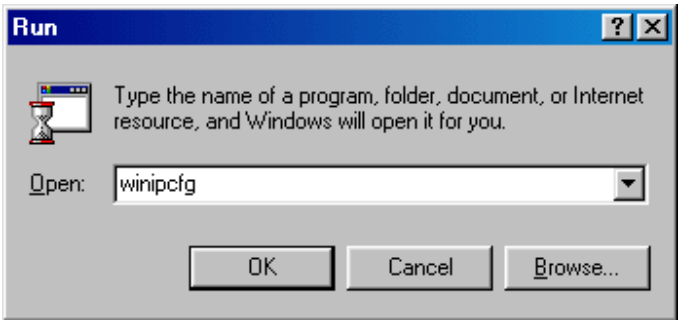


This page shows the system log information.

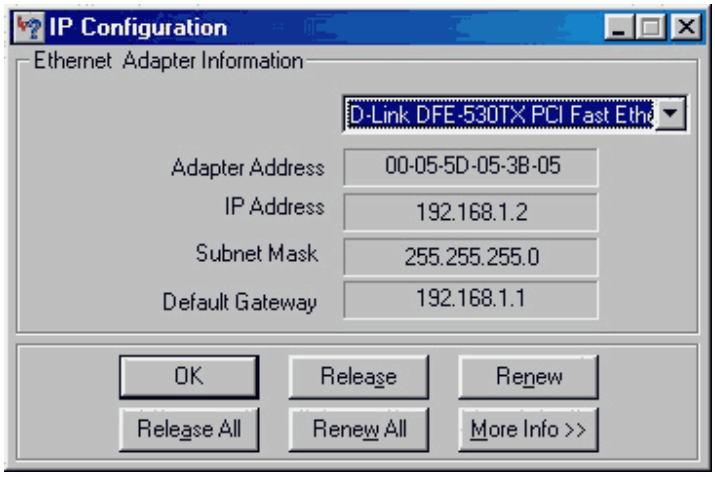
3.8.1 TCP/IP Settings for Windows Operating System

1. How can I find my IP Address in Windows 95, 98, or Me?

- Click on **Start**, then click on **Run**.
- The Run Dialogue Box will appear. Type **winipcfg** in the window as shown then click OK



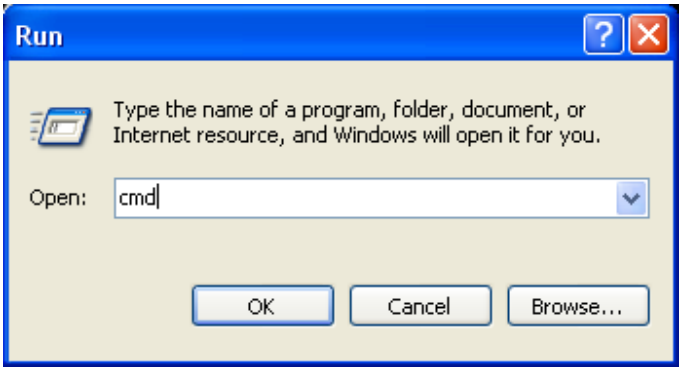
- The **IP Configuration** window will appear, displaying your **Ethernet Adapter Information**.
- Select your adapter from the drop down menu.
- If you do not see your adapter in the drop down menu, your adapter is not properly installed.



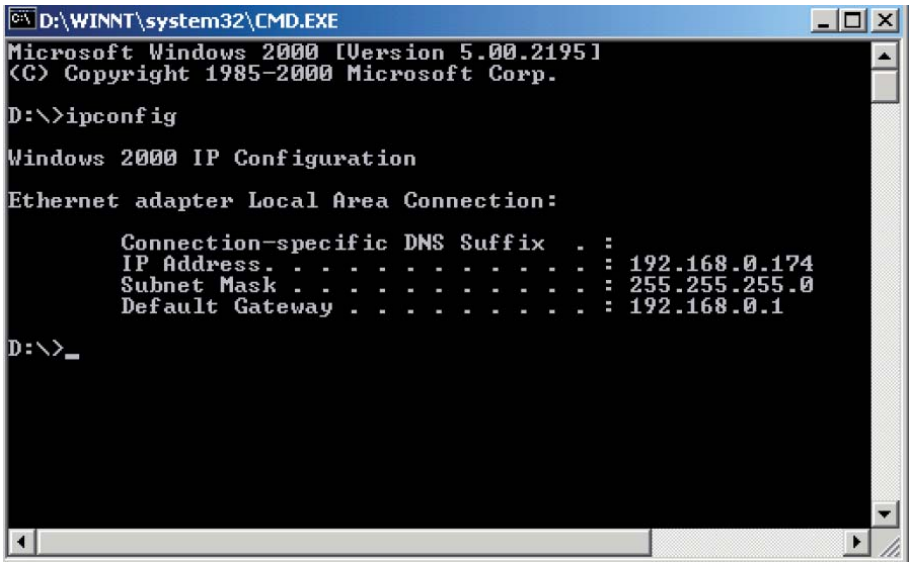
- After selecting your adapter, it will display your IP Address, subnet mask, and default router.
- Click **OK** to close the IP Configuration window.

2. How can I find my IP Address in Windows 2000/XP?

- Click on **Start** and select **Run**.
- Type **cmd** then click **OK**.



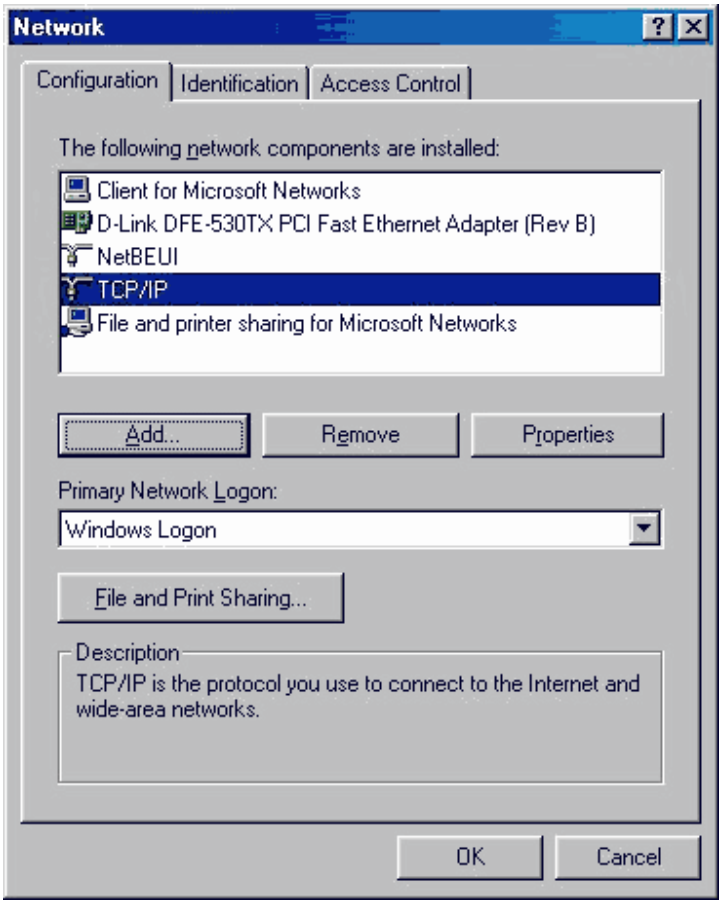
- From the Command Prompt, enter **ipconfig**. It will return your IP Address, subnet mask, and default router.



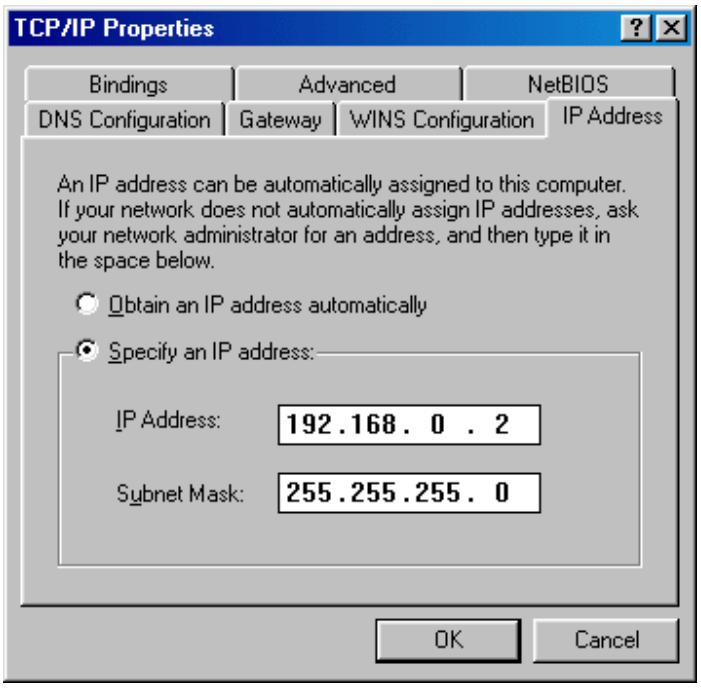
- Type exit to close the command prompt.
- Make sure you take note of your computer´s Default Router IP Address. The Default Router is the IP Address of the router. By default, it should be 192.168.0.1

3. How can I assign a Static IP Address in Windows 98/Me?

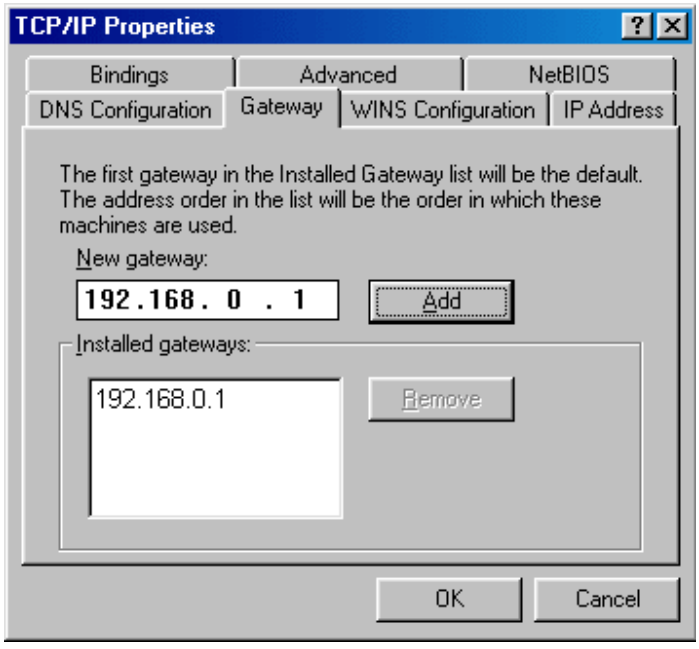
- From the desktop, right-click on the **Network Neighborhood** icon (Win ME - My Network Places) and select **Properties**.
- Highlight **TCP/IP** and click the **Properties** button. If you have more than 1 adapter, then there will be a TCP/IP "Binding" for each adapter. Highlight **TCP/IP > (your network adapter)** and then click **Properties**.



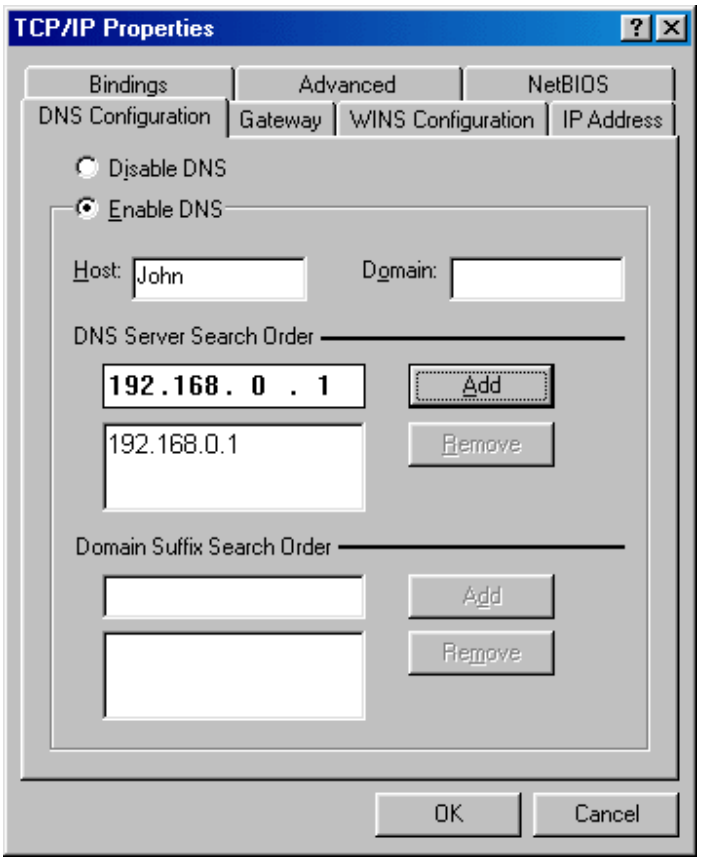
- Click **Specify an IP Address**.
- Enter in an IP Address that is on the same subnet as the LAN IP Address on your router. Example: If the router´s LAN IP Address is 192.168.0.1, make your IP Address 192.168.0.X where X is between 2-99. Make sure that the number you choose is not in use on the network.



- Click on the **Router** tab.
- Enter the LAN IP Address of your router here (192.168.0.1).
- Click **Add** when finished.



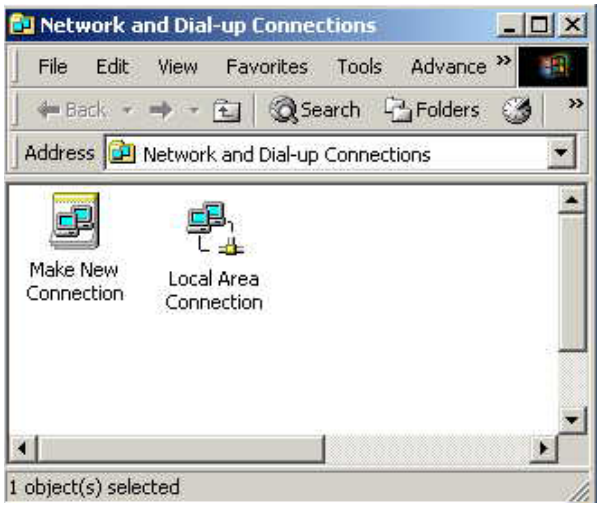
- Click on the **DNS Configuration** tab.
- Click **Enable DNS**. Type in a **Host** (can be any word). Under DNS server search order, enter the LAN IP Address of your router (192.168.0.1). Click **Add**.



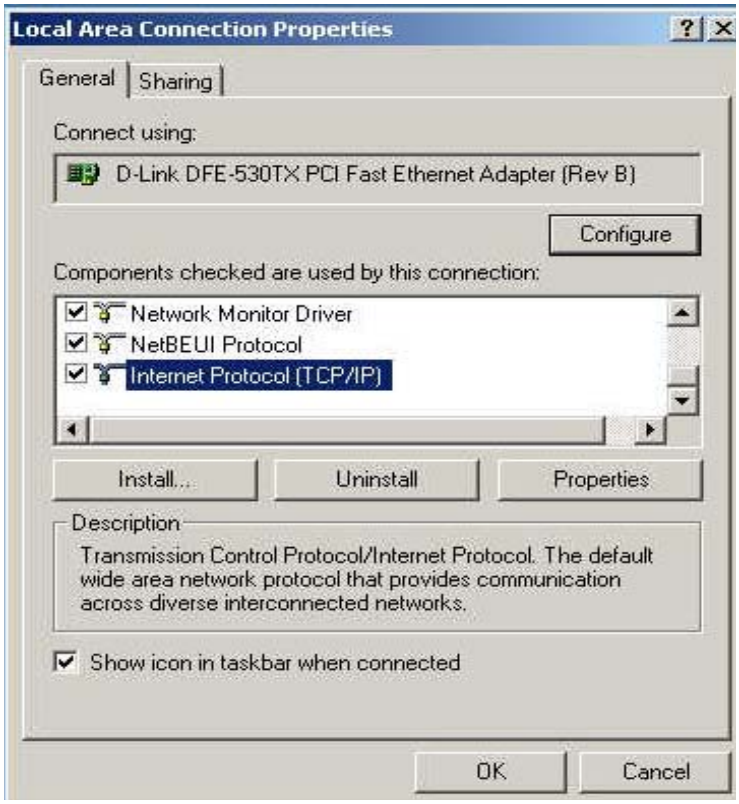
- Click **OK** twice.
- When prompted to reboot your computer, click **Yes**. After you reboot, the computer will now have a static, private IP Address.

4. How can I assign a Static IP Address in Windows 2000?

- Right-click on **My Network Places** and select **Properties**.
- Right-click on the **Local Area Connection** which represents your network card and select **Properties**.



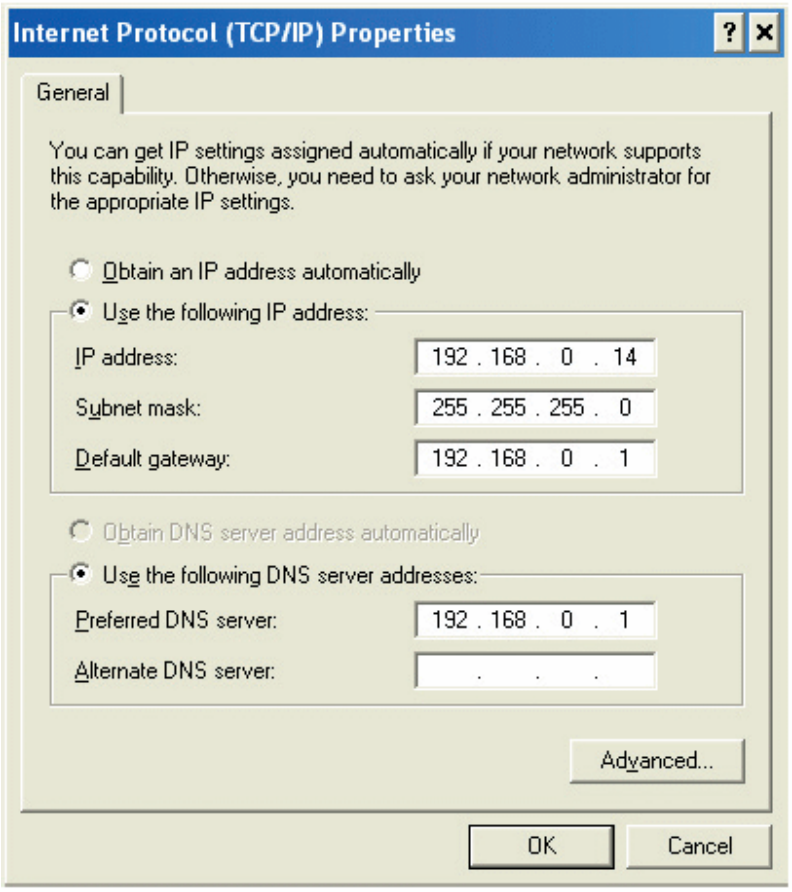
- Highlight **Internet Protocol (TCP/IP)** and click **Properties**.



- Click **Use the following IP Address** and enter an IP Address that is on the same subnet as the LAN IP Address on your router. Example: If the router´s LAN IP Address is 192.168.0.1, make your IP Address 192.168.0.X where X = 2-99. Make sure that the number you choose is not in use on the network.
- Set the **Default Router** to be the same as the LAN IP Address of your router (192.168.0.1).
- Set the **Primary DNS** to be the same as the LAN IP address of your router (192.168.0.1).
- **The Secondary DNS** is not needed or enter a DNS server from your ISP.
- Click **OK** twice. You may be asked if you want to reboot your computer. Click **Yes**.

5. How can I assign a Static IP Address in Windows XP?

- Click on **Start > Control Panel > Network and Internet Connections > Network connections**.
- See the steps for assigning a static IP address in Windows 2000 and continue from there.



- Access the Web management. Open your Web browser and enter the IP Address of your router device in the address bar. This should open the login page for the Web management. Follow instructions to login and complete the configuration.

4-1 Hardware Specification

Standards: IEEE 802.11b/g/Draft-N
Frequency Band: 2.4000 ~ 2.4835GHz (Industrial Scientific Medical Band)
Channel:
FCC (US, Canada) 1 ~11 channel
ETSI (Europe) 1~13 channel
MKKI(Japan) 1~14 channel
Data Rate: 11b: 1/2/5.5/11Mbps
11g: 6/9/12/24/36/48/54Mbps
11n (20MHz): MCS0-15, 32 with Half Guard Interval Support (up to 144Mbps)
11n (40MHz): MCS0-15, 32 with Half Guard Interval Support (up to 300Mbps)
Securities: WEP 64/128, WPA, WPA2
Cisco CCX V1.0, V2.0 & V3.0 Compliance
Antenna: External 2 Antennas with Two TX and Two RX
LEDs: Ethernet /Wireless Link/Activity, Power.
Transmit Power: 11b:19dBm ± 2dBm(PK),17dBm± 2dBm(AV)
11g:24dBm ± 2dBm(PK),14dBm± 2dBm(AV)
11n(20M):24dBm ± 2dBm(PK),14dBm± 2dBm(AV)
11n(40M):23dBm ± 2dBm(PK),13dBm± 2dBm(AV)
Temperature: 32~131°F (0 ~ 55°C)
Humidity: 10-95% (NonCondensing)

Certification: **FCC, CE**

Appendix A Glossary

Address mask
A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Sometimes called subnet mask.

AAL5
ATM Adaptation Layer - This layer maps higher layer user data into ATM cells, making the data suitable for

transport through the ATM network.

ADSL

Asymmetric digital subscriber line.

ATM

Asynchronous Transfer Mode - A cell-based data transfer technique in which channel demand determines packet allocation.

ATM offers fast packet technology, real time; demand led switching for efficient use of network resources.

AWG

American Wire Gauge - The measurement of thickness of a wire.

Bridge

A device connects two or more physical networks and forwards packets between them. Bridges can usually be made to filter packets, that is, to forward only certain traffic. Related devices are: repeaters which simply forward electrical signals from one cable to the other, and full-fledged routers which make routing decisions based on several criteria.

Broadband

Characteristic of any network multiplexes independent network carriers onto a single cable. Broadband technology allows several networks to coexist on one single cable; traffic from one network does not interfere with traffic from another. Broadcast A packet delivery system where a copy of a given packet is given to all hosts attached to the network. Example: Ethernet.

CO

Central Office. Refers to equipment located at a Telco or service provider's office.

CPE

Customer Premises Equipment located in a user's premises.

DHCP (Dynamic Host Configuration Protocol)

DHCP is software that automatically assigns IP addresses to client stations logging onto a TCP/IP network. DHCP eliminates having to manually assign permanent IP addresses to every device on your network. DHCP software typically runs in servers and is also found in network devices such as Routers.

DMT

Discrete Multi-Tone frequency signal modulation

Downstream rate

The line rate for return messages or data transfers from the network machine to the user's premises machine.

DSLAM

Digital Subscriber Line Access Multiplex

Dynamic IP Addresses

A dynamic IP address is an IP address that is automatically assigned to a client station (computer, printer, etc.) in a TCP/IP network. Dynamic IP addresses are typically assigned by a DHCP server, which can be a computer on the network or another piece of hardware, such as the Router. A dynamic IP address may change every time your computer connects to the network.

Encapsulation

The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the physical layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), followed by the application protocol data.

Ethernet

One of the most common local area network (LAN) wiring schemes, Ethernet has a transmission rate of 10 Mbps.

FTP

File Transfer Protocol. The Internet protocol (and program) used to transfer files between hosts.

Hop count

A measure of distance between two points on the Internet. It is equivalent to the number of routers that separate the source and destination.

HTML

Hypertext Markup Language - The page-coding language for the World Wide Web.

HTML browser

A browser used to traverse the Internet, such as Netscape or Microsoft Internet Explorer.

http

Hypertext Transfer Protocol - The protocol used to carry world-wide-web (www) traffic between a www browser computer and the www server being accessed.

ICMP

Internet Control Message Protocol - The protocol used to handle errors and control messages at the IP layer. ICMP is actually part of the IP protocol.

Internet address

An IP address is assigned in blocks of numbers to user organizations accessing the Internet. These addresses are established by the United States Department of Defense's Network Information Center. Duplicate addresses can cause major problems on the network, but the NIC trusts organizations to use individual addresses responsibly. Each address is a 32-bit address in the form of x.x.x.x where x is an eight- bit number from 0 to 255. There are three classes: A, B and C, depending on how many computers on the site are likely to be connected.

Internet Protocol (IP)

The network layer protocol for the Internet protocol suite

IP address

The 32-bit address assigned to hosts that want to participate in a TCP/IP Internet.

ISP

Internet service provider - A company allows home and corporate users to connect to the Internet.

MAC

Media Access Control Layer - A sub-layer of the Data Link Layer (Layer 2) of the ISO OSI Model responsible for media control.

MIB

Management Information Base - A collection of objects can be accessed via a network management protocol, such as SNMP and CMIP (Common Management Information Protocol).

NAT

Network Address Translation - A proposal for IP address reuse, where the local IP address is mapped to a globally unique address.

NVT

Network Virtual Terminal

PAP

Password Authentication Protocol

PORT

The abstraction used by Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host.

POTS

Plain Old Telephone Service - This is the term used to describe basic telephone service.

PPP

Point-to-Point-Protocol - The successor to SLIP, PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits.

PPPoE

PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

Remote server

A network computer allows a user to log on to the network from a distant location.

RFC

Request for Comments - Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFCs can be found at www.ietf.org..

Route

The path that network traffic takes from its source to its destination. The route a datagram may follow can include many routers and many physical networks. In the Internet, each datagram is routed separately.

Router

A system responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this, it uses a routing protocol to gain information about the network and algorithms to choose the best route based on several criteria known as "routing metrics".

Routing table

Information stored within a router that contains network path and status information. It is used to select the most appropriate route to forward information along.

Routing Information Protocol

Routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.

SNMP

Simple Network Management Protocol - The network management protocol of choice for TCP/IP-based Internet.

SOCKET

(1) The Berkeley UNIX mechanism for creating a virtual connection between processes.
(2) IBM term for software interfaces that allow two UNIX application programs to talk via TCP/IP protocols.

Spanning-Tree Bridge Protocol (STP)

Spanning-Tree Bridge Protocol (STP) - Part of an IEEE standard. A mechanism for detecting and preventing loops from occurring in a multi-bridged environment. When three or more LAN's segments are connected via bridges, a loop can occur. Because a bridge forwards all packets that are not recognized as being local, some packets can circulate for long periods of time, eventually degrading system performance. This algorithm ensures only one path connects any pair of stations, selecting one bridge as the 'root' bridge, with the highest priority one as identifier, from which all paths should radiate.

Spoofing

A method of fooling network end stations into believing that keep alive signals have come from and returned to the host. Polls are received and returned locally at either end

Static IP Addresses

A static IP address is an IP address permanently assigned to computer in a TCP/IP network. Static IP addresses are usually assigned to networked devices that are consistently accessed by multiple users, such as Server PCs, or printers. If you are using your Router to share your cable or DSL Internet connection, contact your ISP to see if they have assigned your home a static IP address. You will need that address during your Router's configuration.

Subnet

For routing purposes, IP networks can be divided into logical subnets by using a subnet mask. Values below those of the mask are valid addresses on the subnet.

TCP

Transmission Control Protocol - The major transport protocol in the Internet suite of protocols provides reliable, connection-oriented full-duplex streams.

TFTP

Trivial File Transfer Protocol - A simple file transfer protocol (a simplified version of FTP) that is often used to boot diskless workstations and other network devices such as routers over a network (typically a LAN).

Telnet

The virtual terminal protocol in the Internet suite of protocols - Allows users of one host to log into a remote host and act as normal terminal users of that host.

Transparent bridging

So named because the intelligence necessary to make relaying decisions exists in the bridge itself and is thus transparent to the communicating workstations. It involves frame forwarding, learning workstation addresses and ensuring no topology loops exist (in conjunction with the Spanning-Tree algorithm).

UDP

User Datagram Protocol - A connectionless transport protocol that runs on top of TCP/IP's IP. UDP, like TCP, uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagrams without acknowledgments or guaranteed delivery. Best suited for small, independent requests, such as requesting a MIB value from an SNMP agent, in which first setting up a connection would take more time than sending the data.

UNI signaling

User Network Interface signaling for ATM communications.

Virtual Connection (VC)

A link that seems and behaves like a dedicated point-to-point line or a system that delivers packets in sequence, as happens on an actual point-to-point network. In reality, the data is delivered across a network via the most appropriate route. The sending and receiving devices do not have to be aware of the options and the route is chosen only when a message is sent. There is no pre-arrangement, so each virtual connection exists only for the duration of that one transmission.

WAN

Wide area network - A data communications network that spans any distance and is usually provided by a public carrier (such as a telephone company or service provider).

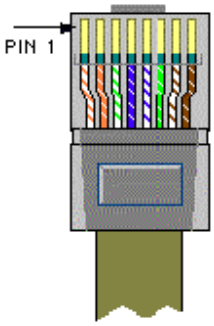
Appendix B Cabling / Connection

Network cables connect PCs in an Ethernet network Category 5, called "Cat5" for short is commonly used type of network cable today.

Cat 5 cables are tipped with RJ-45 connectors, which fit into RJ-45 port.

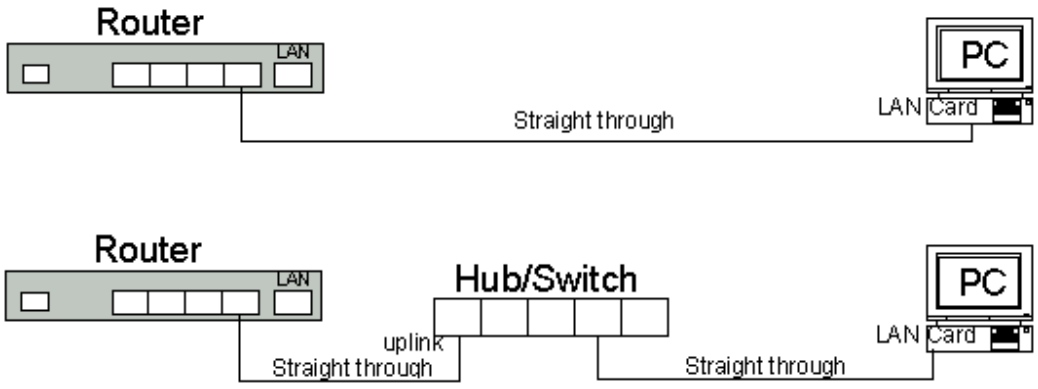
Straight-through vs. Crossover Cables:

Straight-through	
Wire	**Becomes**
1	1
2	2
3	3
6	6



Straight-through	
Wire	**Becomes**
1	1
2	2
3	3
6	6

LAN Connection:



To check LEDs light up when you finish connecting two pieces of hardware.