

Wireless Broadband Firewall Gateway

User's Manual

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

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

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

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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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

Table of Content

CHAPTER 1	1
INTRODUCTION	1
1.1 An Overview of the Product	1
1.2 Package Contents	2
1.3 The Product Features	2
1.4 The Product Application	4
 CHAPTER 2	 5
USING THE PRODUCT	5
2.1 Cautions for Using the Product	5
2.2 The Front LEDs	5
2.3 The Rear Ports	6
2.4 Cabling	6
 CHAPTER 3	 7
CONFIGURATION	7
3.1 Before Configuration	7
3.2 Factory Default Settings	14
3.2.1 Password	14
3.2.2 LAN and WAN Port Addresses	15
3.3 Information from ISP	15
3.4 Configuring with Web Browser	15
3.4.1 LAN	16
3.4.2 WAN	19
3.4.3 System	24
3.4.4 Firewall	28
3.4.5 VPN	39
3.4.6 Virtual Server	40
3.4.7 Advance	41
3.4.8 Status	46
3.4.9 Help	50
3.5 Changing Password	51
3.6 Firmware Upgrade	52
 CHAPTER 4	 53
TROUBLESHOOTING	53
How to do a factory reset?	53
Why do I get IP conflict information in my computer?	53
Why won't my Internet application work?	54
Can I upgrade the gateway's firmware?	54
Can I set a fixed IP address on my PC?	54
Is there a tool to check my PC's TCP/IP settings in MS Windows?	55
How can I test the whole path (PC Gateway outside world) to make sure it works fine?	56
How can I check the active IP settings for my WAN port?	57
Where can I find the WAN port's MAC address?	57
How can I explore a local server to be visible to outside users?	57
What is DMZ host?	58

How to configure my MacOS to surf Internet through the Wireless Broadband Firewall Gateway?	58
How can I do if I forget the password for accessing Gateway?.....	58
How can I do if there is already a DHCP server in LAN?.....	58
How many PCs can share this single Wireless Broadband Firewall Gateway simultaneously?	58
Which connection method should I select in WAN-ISP setting window?	59

APPENDIX A	61
SPECIFICATION	61

APPENDIX B.....	62
INTERNET APPLICATIONS	62

Chapter 1

Introduction

1.1 An Overview of the Product

The Wireless Broadband Firewall Gateway provides SOHO and residential users the ideal solution for sharing a high-speed broadband Internet connection among a 11Mbps wireless network and a 10/100Mbps Fast Ethernet backbone. It integrates robust firewall and routing functions with advanced 802.11b wireless technology, maximizing your network security and efficiency while minimizing the network complexity and maintenance costs.

The product includes functions of an IEEE 802.3 Ethernet-based Broadband Firewall Gateway. It provides four 10/100Mbps Dual Speed Ethernet ports for connection to a home or small office network and one 10Mbps Ethernet port for a DSL Modem, Cable Modem, or other broadband access device.

The product is an integrated Internet IP sharing device with a built-in 4-port 10/100Mbps Base-T NWay Ethernet switch. It is the perfect solution to connect a small group of PCs to a high-speed broadband Internet connection. Multi-users can have high-speed Internet access simultaneously via one single IP address provided by ISP.

This product also serves as an Internet firewall, protecting your network from being accessed by outside users. Not only provide the natural firewall function (Network Address Translation, NAT), it also provides rich firewall features to secure user's network. All incoming data packets are monitored and filtered. Besides, it can also be configured to block internal users from accessing to the Internet.

The product provides three levels of security support. First, it masks LAN users' IP addresses which are invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. Secondly, it can block and redirect certain ports to limit the services that outside users can access. For example, to ensure that games and other Internet applications will run properly, user can open some specific ports for outside users to access internal services in network. Finally, it can also detect and block many Hacker Patterns and not allow hacker into your network.

Integrated DHCP services, client and server, allow up to 253 users to get their IP addresses automatically on boot up from the product. Simply set local machines as a DHCP client to accept a dynamically assigned IP address from DHCP server and reboot. Each time local machine is powered up; the router will recognize it and assign an IP address to instantly connect it to the LAN.

For advanced users, Virtual Server function allows the product to provide limited visibility to local machines with specific services for outside users. An ISP provided IP address can be set to the product and then specific services can be rerouted to specific computers on the local network. For instance, a dedicated web server can be connected to the Internet via the product and then incoming requests for HTML that are received by the product can be rerouted to the dedicated local web server, even though the server now has a different IP address. In this example, the product is on the Internet and vulnerable to attacks, but the server is protected.

Virtual Server can also be used to re-task services to multiple servers. For instance, the product can be set to allow separated FTP, Web, and Multiplayer game servers to share the same Internet-visible IP address while still protecting the servers and LAN users from hackers.

1.2 Package Contents

1. Wireless Broadband Firewall Gateway
2. One CD containing the on-line manual
3. One straight-through CAT5 Ethernet cable
4. One power adapter
5. This Quick Start Guide

1.3 The Product Features

The product provides the following features:

Wireless Ethernet 802.11b access point: Provides a wireless Ethernet 802.11b access point for extending the communication media to WLAN.

Fast Ethernet Switch: A 4-port 10/100Mbps fast Ethernet switch is supported in the LAN site and automatic switching between MDI and MDIX for 10Base-T and 100Base-TX ports is supported. An Ethernet straight or cross-over cable can be used directly, this fast Ethernet switch will detect it automatically.

Network Address Translation (NAT): Allows multi-users to access outside resource such as Internet simultaneously with one IP address/one Internet access account. Besides, many application layer gateway (ALG) are supported such as web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting, MS Messenger, QUAKE and others.

Firewall: Supports SOHO firewall with NAT technology. Automatically detects and blocks the Denial of Service (DoS) attack. The hacker's attack will be recorded associated with timestamp in security logging area. An URL blocking feature is also provided. More firewall function will be always implemented, visit our web site for more information. A real time altering email will be sent to your account for your future action.

Domain Name System (DNS) relay: provides an easy way to map the domain name (a friendly name for user such as www.yahoo.com) and IP address. When local machine sets its DNS server with this router's IP address. Then every DNS conversion request packet from the PC to this router will be forwarded to the real DNS in outside network. After the router gets the reply, then forwards it back to the PC.

Dynamic Domain Name System (DDNS): The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. To use the service, you must first apply an account from this free Web server <http://www.dyndns.org/>.

Virtual Private Network (VPN): Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded PPTP client supported by this router to make a VPN connection. Or user can run the PPTP client in PC and the router already provides IPsec and PPTP pass through function to establish a VPN connection if user likes to run the PPTP client in his local computer.

PPP over Ethernet (PPPoE): Provide embedded PPPoE client function to establish a connection. Users can get greater access speed without changing the operation concept, sharing the same ISP account and paying for one access account. No PPPoE client software is required for local computer. The "Dial-on-Demand" and Idle timer are implemented for better connection usage management.

Virtual Server: User can specify some services to be visible from outside users. The router can detect incoming service request and forward it to the specific local computer to handle it. For example, user can assign a PC in LAN acting as WEB server inside and expose it to the outside network. Outside user can browse inside web server directly while it is protected by NAT. A **DMZ** host setting is also provided to a local computer exposed to the outside network, Internet.

Rich Packet Filtering: Not only filter the packet based on IP address, but also based on Port numbers. It will increase the performance in LAN and WAN, also provide a higher-level security control.

Static and RIP1/2 Routing: Supports an easy static routing table or RIP1/2 routing protocol to support routing capability.

Dynamic Host Control Protocol (DHCP) client and server: In the WAN site, the DHCP client can get an IP address from the Internet Server Provider (ISP) automatically. In the LAN site, the DHCP server can allocate up to 253 client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.

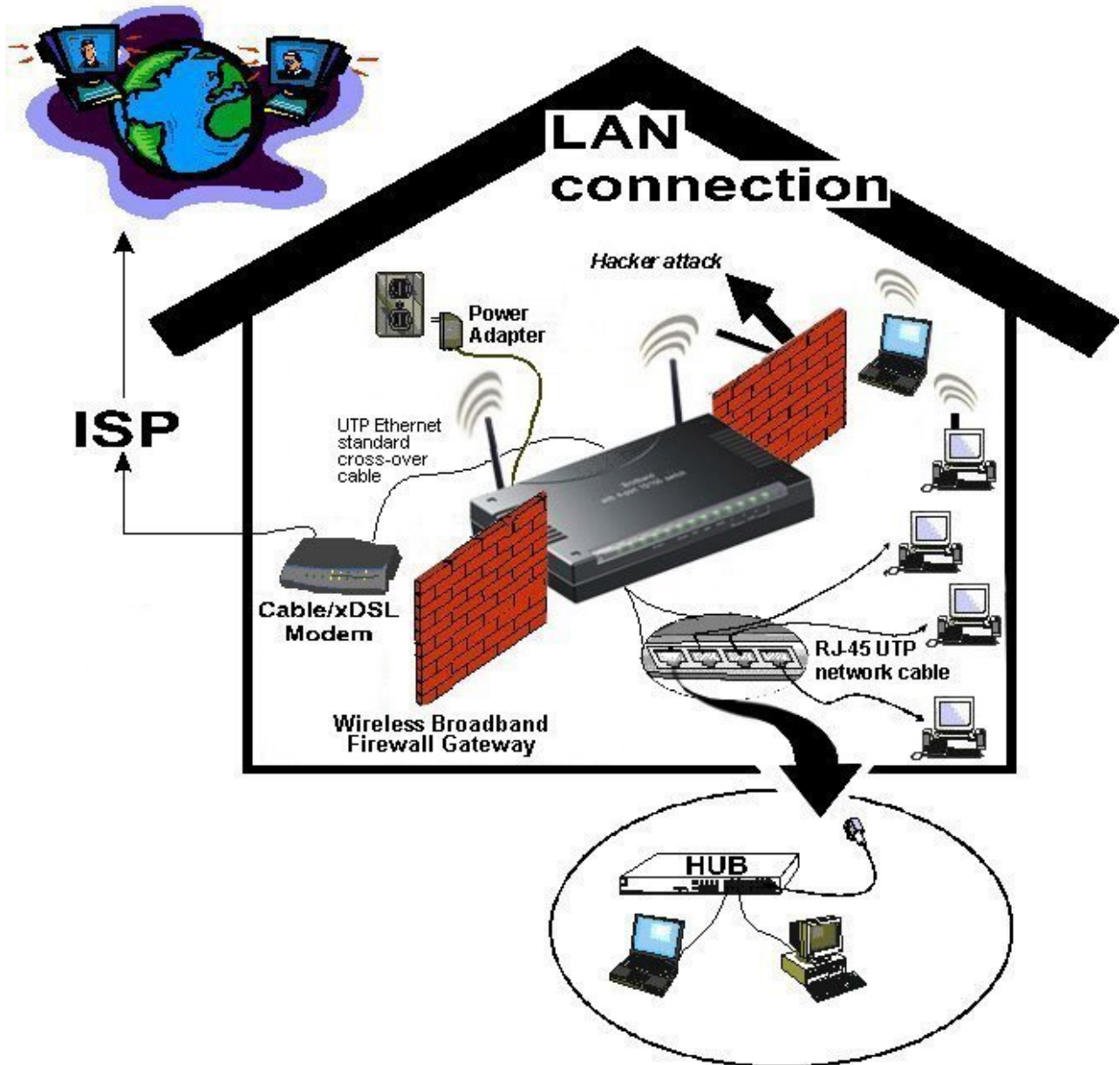
SNTP: An easy way to get the network real time information from SNTP server.

Web based GUI and remote management: supports web based GUI for configuration and management. It is a user-friendly with on-line help, providing necessary information and assist user timing. It also supports remote management capability for remote user to configure and manage this product.

Firmware Upgradeable: device can be upgraded to be the latest firmware through the WEB based GUI.

1.4 The Product Application

Internet



NOTE:

The router provides a 10Mbps Ethernet port (10Base-T) in the WAN site, it will not detect MDI and MDIX automatically. Therefore, an Ethernet cross-over cable should be used to connect to DSL/CABLE modem.

Chapter 2

Using the Product

2.1 Cautions for Using the Product



Do not place the product under high humidity and high temperature.

Do not use the same power source for the product with other equipment.

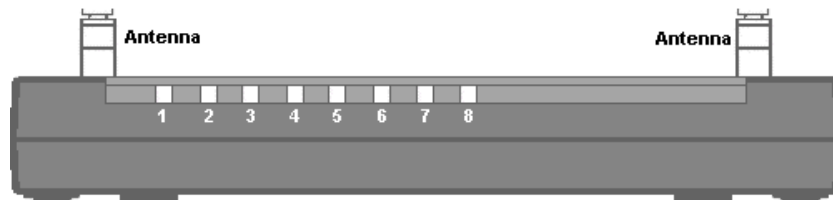
Do not open or repair the case yourself. If the product is too hot, turn off the power immediately and have a qualified serviceman repair it.



Place the product on the stable surface.

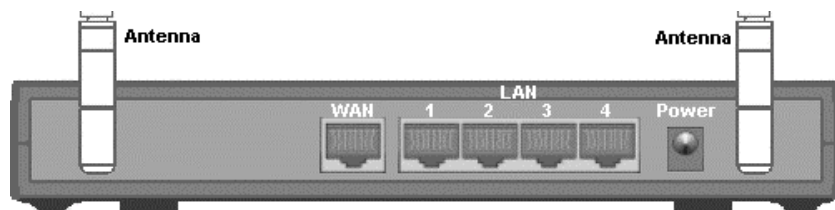
Only use the power adapter that comes with the package.

2.2 The Front LEDs



LED		Meaning
1	PWR	Lit green when power adapter is connected.
2	LAN 1	Lit green when connected at 100 Mbps. Lit orange when connected at 10 Mbps. Flashes when sending/receiving data.
3	LAN 2	
4	LAN 3	
5	LAN 4	
6	WAN	Lit when connected to a WAN device. Flashes when sending/receiving data.
7	PPP/SYS	Lit orange when system ready. Lit green when the PPPoE or PPTP connection is established. Flashes orange when upgrading firmware.
8	WLAN	Lit green when wireless connection is established. Flashes when sending/receiving data.

2.3 The Rear Ports



Port	Connecting Instruction
Power (jack)	Connect the supplied power adapter to this jack.
LAN 1-4 (RJ-45 connector)	Connect a straight-through or crossover Ethernet cable to these four ports when connecting to a LAN of 10Mbps or 100Mbps such as an office or home network.
WAN (RJ-45 connector)	Connect a straight-through Ethernet cable to this port when connecting to a hub. Connect a crossover cable to this port when connecting to a DSL/Cable bridge or modem for establishing WAN connections.

2.4 Cabling

Please refer to **section 1.4 “The Product Application”** first; it gives a clear cable connection diagram.

The most common problem associated with Ethernet is bad cabling. Make sure that all connected devices are turned on. On the top of the product is a bank of LEDs, as a first check verifies that the LAN Link and WAN Link LEDs are lit and green. If they are not, verify that you are using the proper cables.

Chapter 3

Configuration

The product can be configured with your Web browser. The web browser is included as a standard application in following operation systems, UNIX, Linux, Mac OS, Windows 95/98/NT/2000/Me/XP, etc. The product provides a very easy and user-friendly interface for configuration.

3.1 Before Configuration

This section describes the configuration required by LAN-attached PCs that communicate with the product, either to configure the device, or for network access. These PCs must have an Ethernet interface installed properly, be connected to the product either directly or through an external repeater hub, and have TCP/IP installed and configured to obtain an IP address through a DHCP server or a fixed IP address which must be in the same subnet of the product. The default IP address of the product is 192.168.1.254 and subnet mask is 255.255.255.0. The best and easy way is to configure the PC to get an IP address from the product.

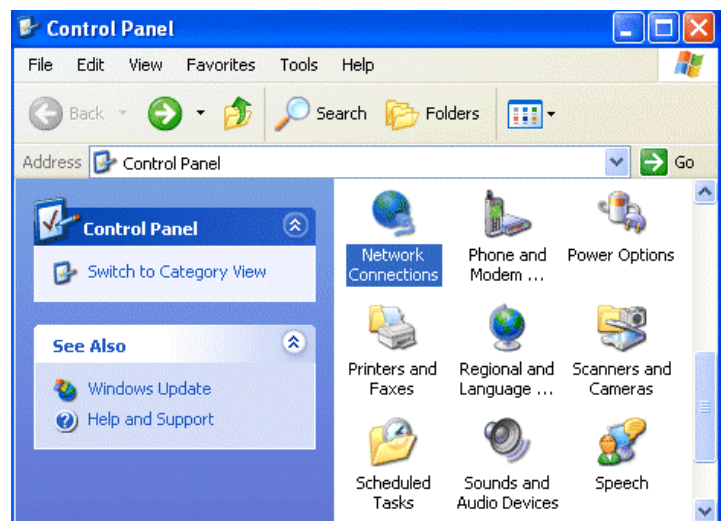
Please follow the steps below for PC's network environment installation. First of all, please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to MS Windows relative manuals.



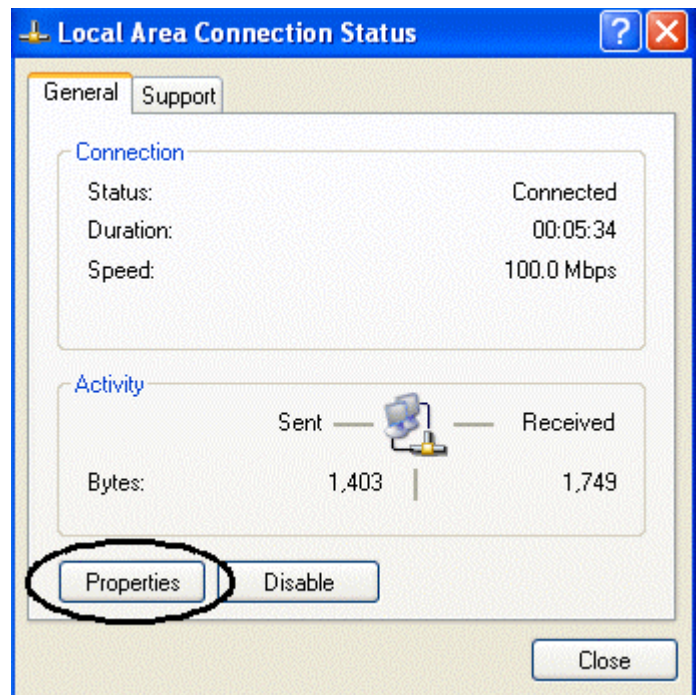
Any TCP/IP capable workstation can be used to communicate with or through the product. To configure other types of workstations, please consult the manufacturer's documentation.

Configuring PC in Windows XP

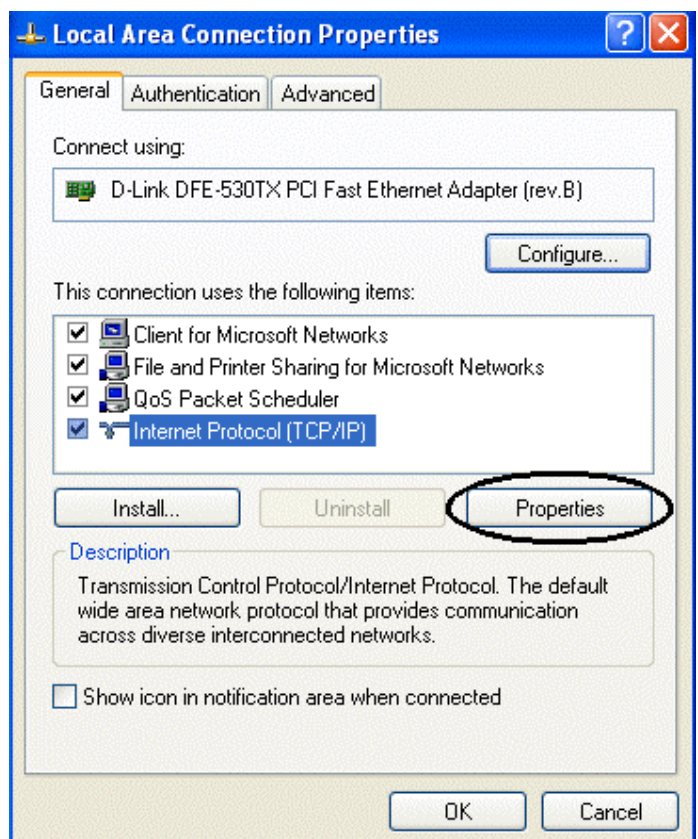
1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections**.
2. Double-click **Local Area Connection**.



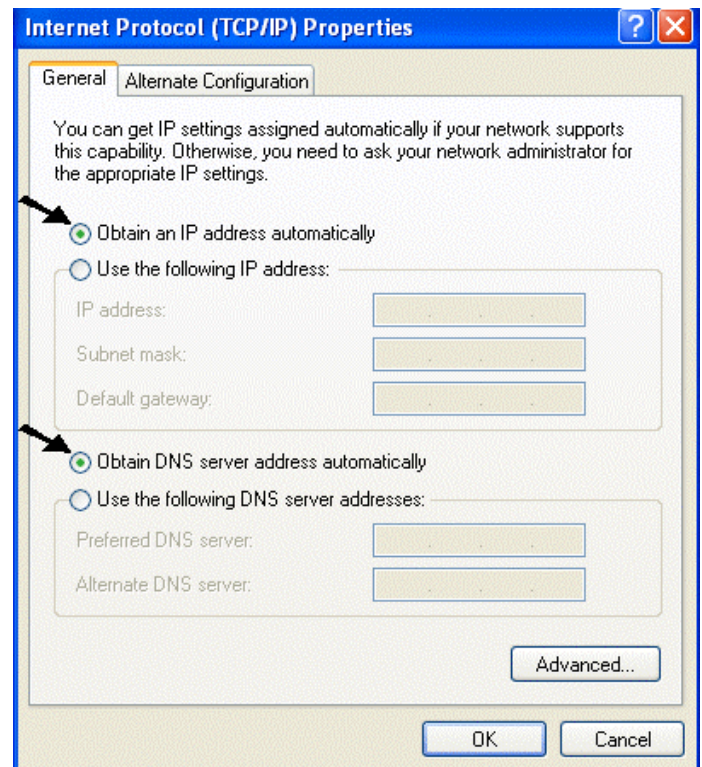
3. In the **Local Area Connection Status** window, click **Properties**.



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



5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.

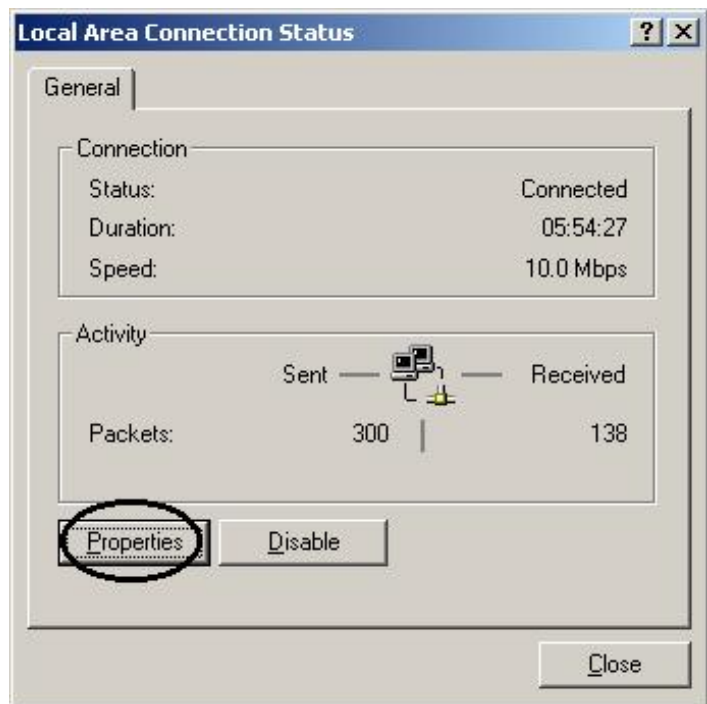


Configuring PC in Windows 2000

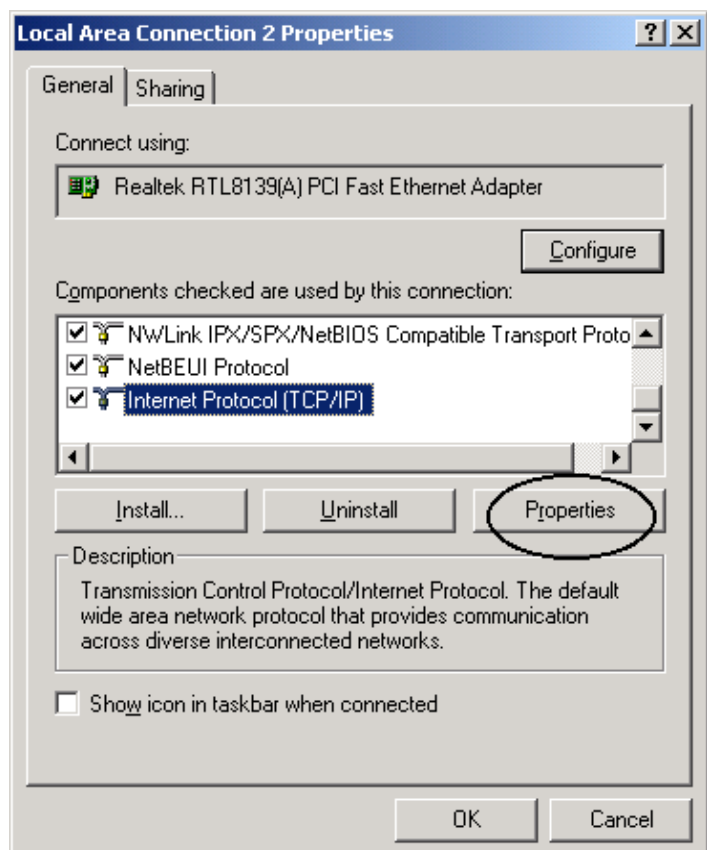
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.
2. Double-click **Local Area Connection**.



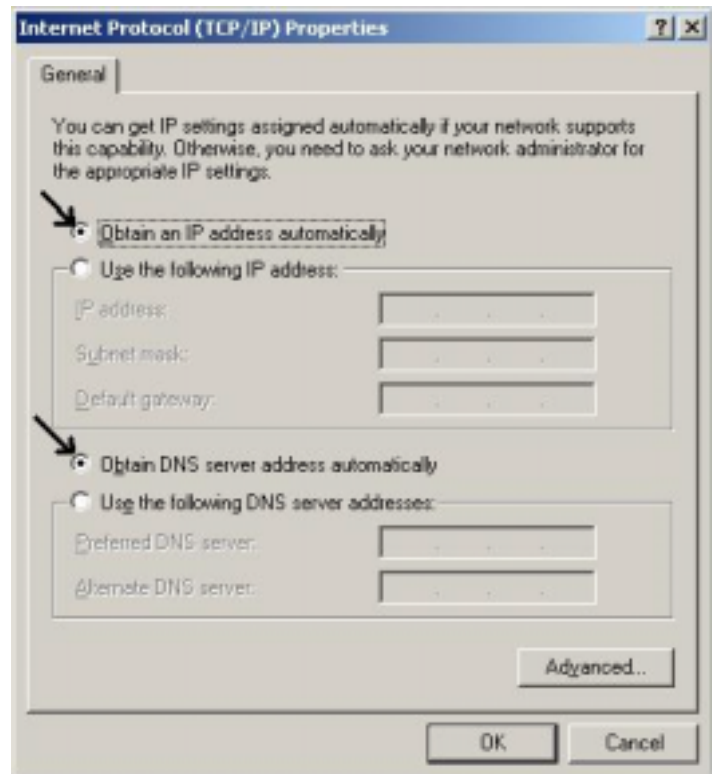
3. In the **Local Area Connection Status** window, click **Properties**.



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

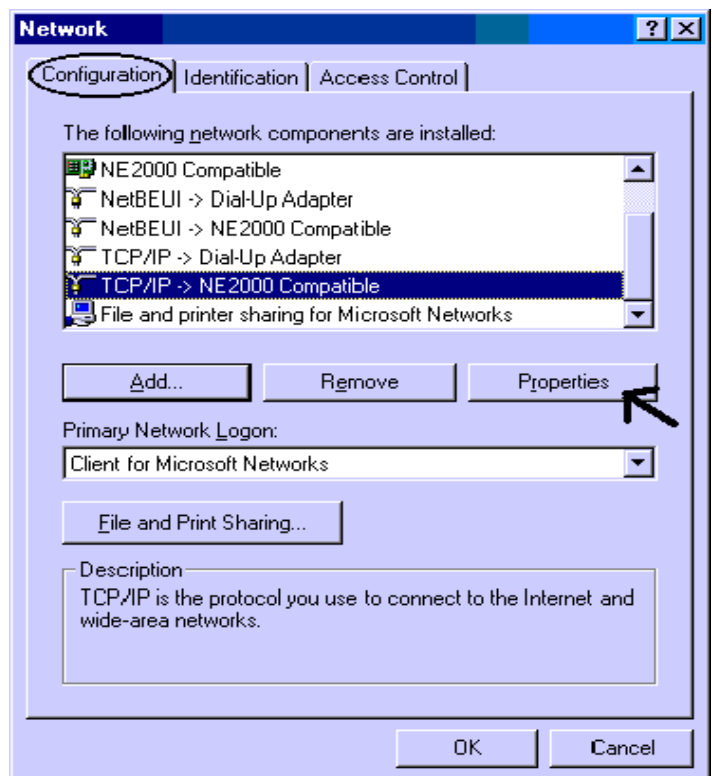


5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.

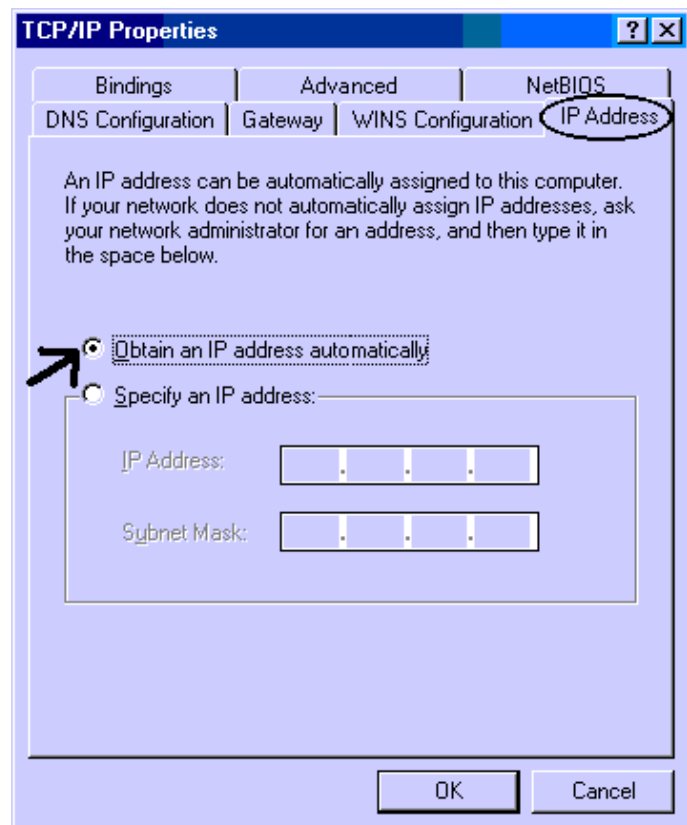


Configuring PC in Windows 95/98/ME

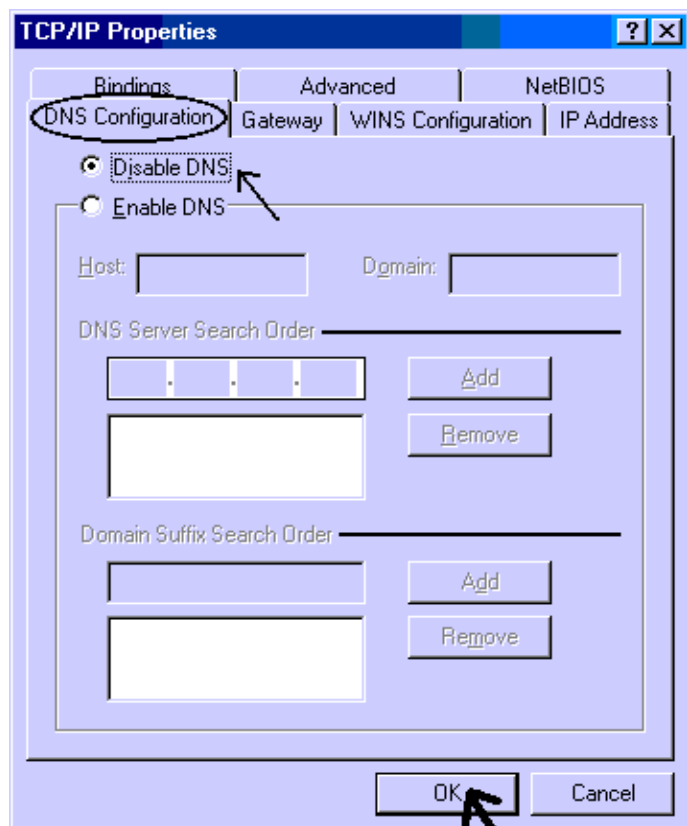
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.
2. Select **TCP / IP -> NE2000 Compatible**, or the name of your Network Interface Card (NIC) in your PC.
3. Click **Properties**.



4. Select the **IP Address** tab. In this page, click the **Obtain an IP address automatically** radio button.

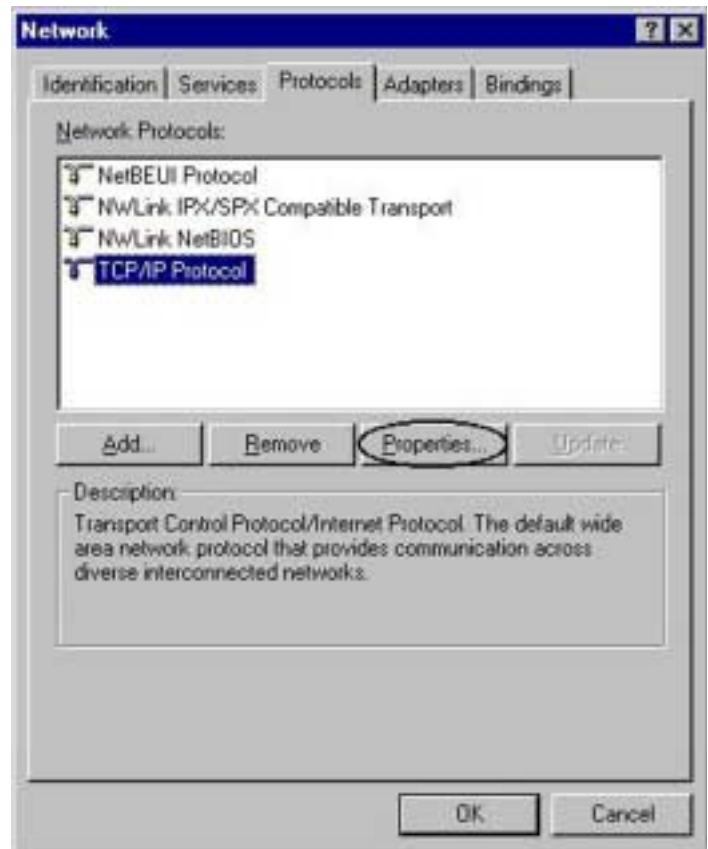


5. Then select the **DNS Configuration** tab.
6. Select the **Disable DNS** radio button and click **OK** to finish the configuration.

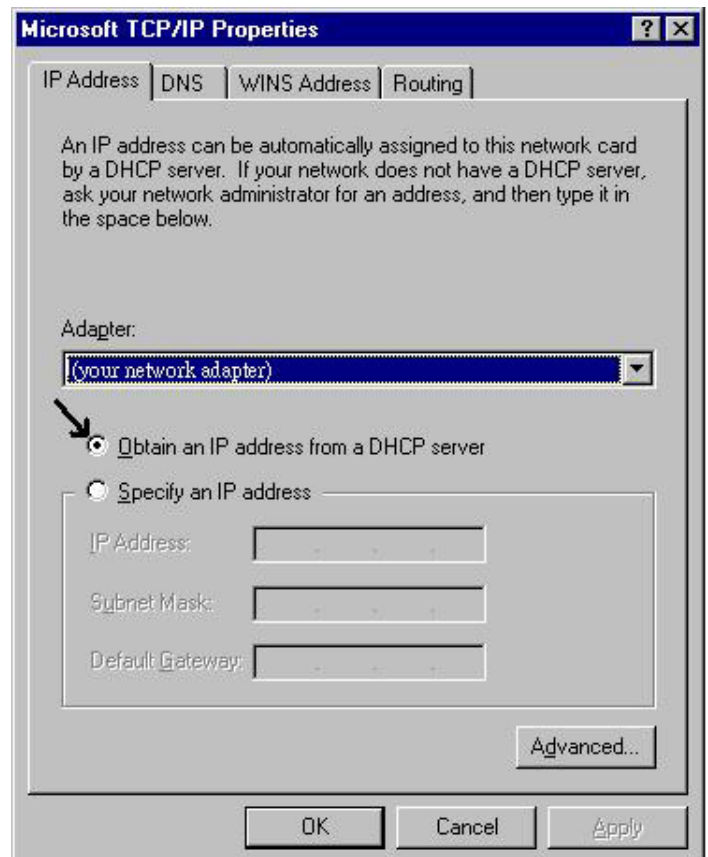


Configuring PC in Windows NT4.0

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Protocols** tab.
2. Select **TCP/IP Protocol** and click **Properties**.



3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**.



3.2 Factory Default Settings

Before you configure the product, you need to know the following default settings.

1. Web Configurator

Password : <BLANK>

BLANK means user does not need to input any characters.

2. Device IP Network settings in LAN site

IP Address : 192.168.1.254

Subnet Mask : 255.255.255.0

3. ISP setting in WAN site

Obtain an IP address automatically

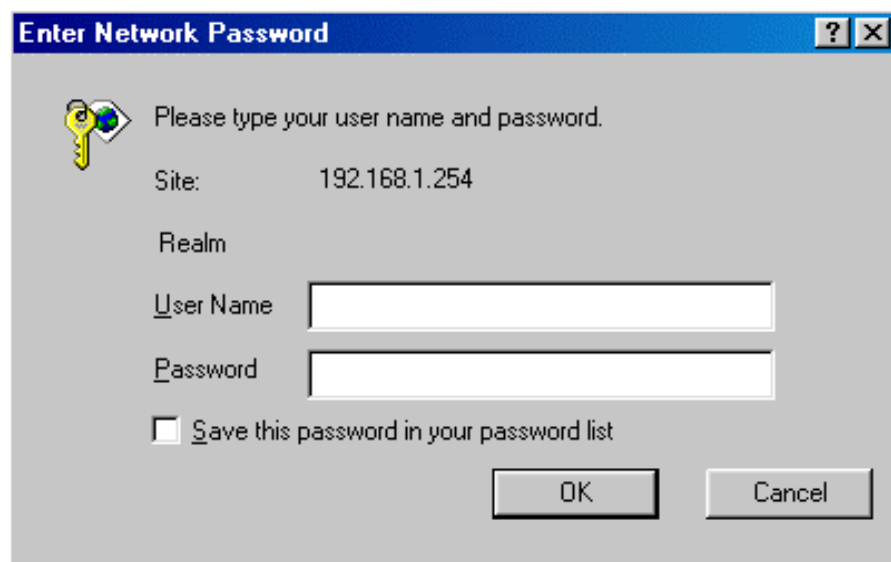
4. DHCP server

DHCP server is enabled.

IP address pool from IP Address : 192.168.1.100 to IP Address : 192.168.1.199

3.2.1 Password

The password is left blank as the default setting. When configuring your device with Web browser, just click “OK”, and then you are logged in for the first time. It is recommended that you set a password for security and management purpose. The product maintains the password only. It means the product only checks the password even you enter characters in the User Name field.



If you ever forget the password to log in, you should contact the dealer where you bought this product.

3.2.2 LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown below.

LAN Port		WAN Port
IP address	192.168.1.254	Obtain an IP address automatically. This IP address is assigned by ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199 (Actually, it can supports up to 253 users.)	

3.3 Information from ISP

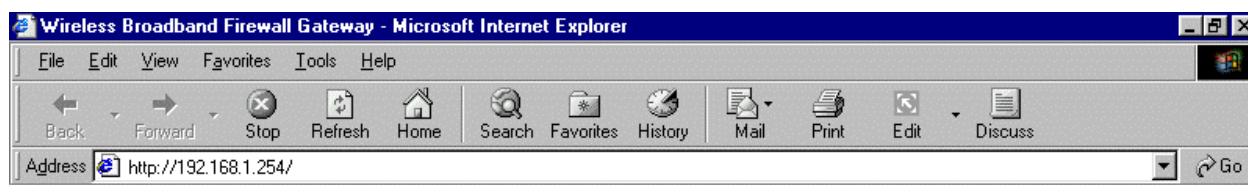
Before you start configuring this device, you have to check with your ISP what kind of service is provided such as PPPoE, Fixed IP, obtain an IP address automatically or PPTP client.

Gather the information as illustrated in the following table and keep it for reference.

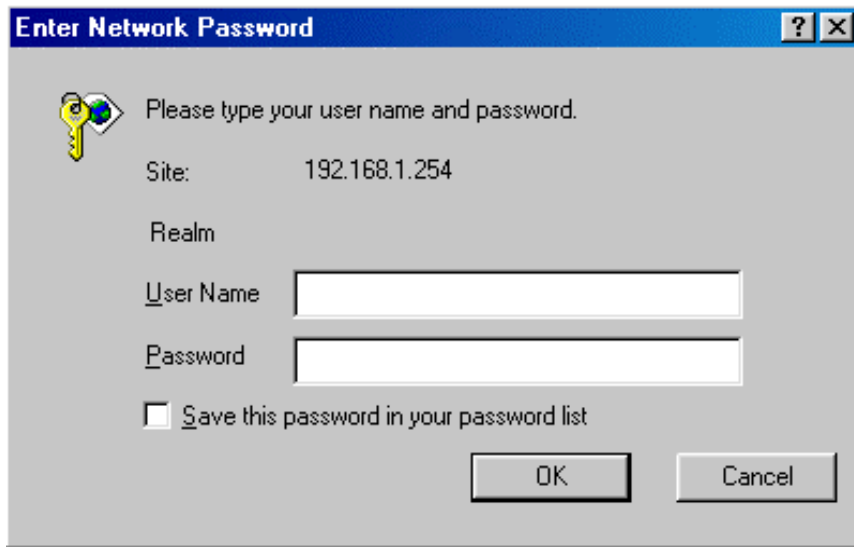
PPPoE	Username, Password, Service Name, Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed)
Fixed IP	IP address, Subnet mask, Gateway address, Domain Name System (DNS) IP address (it is fixed IP address)
Obtain an IP Address Automatically	Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed)
PPTP Client	Username, password, PPTP server's IP address and Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed)

3.4 Configuring with Web Browser

Open the web browser, enter the local port IP address of this device, which default at **192.168.1.254**, and click “Go” to get the login page.

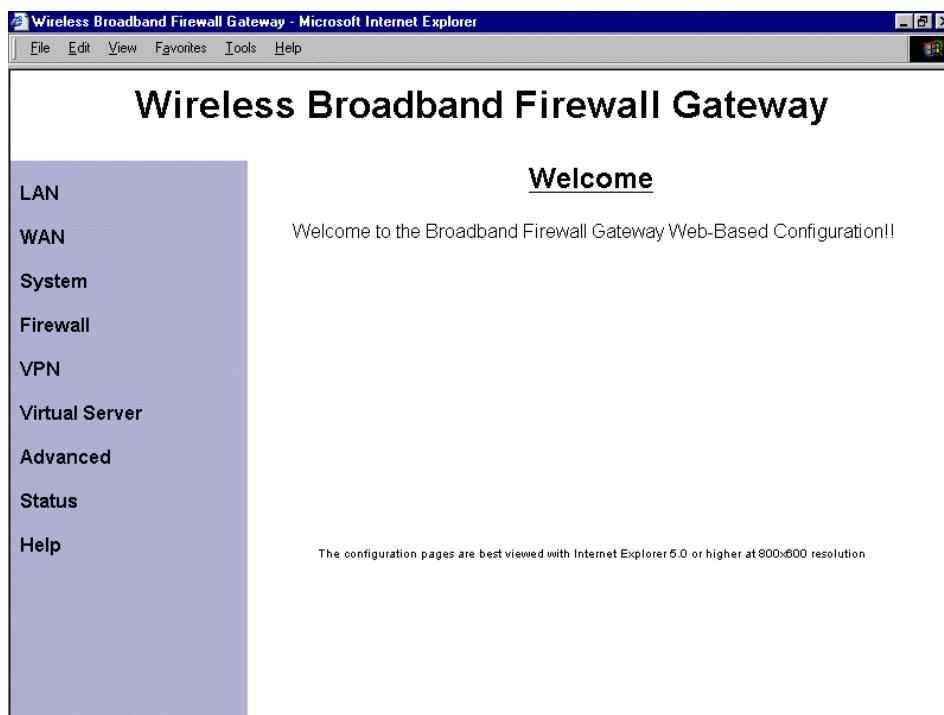


No user name is required. The default password is left blank. If you have set a password, enter that and click **“OK”** to continue.



The dialog box titled "Enter Network Password" has a blue header bar with a question mark icon and a close button. The main area is light gray. It contains a key icon and the text "Please type your user name and password." Below this, the "Site:" field is populated with "192.168.1.254". There are empty text boxes for "Realm", "User Name", and "Password". A checkbox labeled "Save this password in your password list" is unchecked. At the bottom right are "OK" and "Cancel" buttons.

At the configuration homepage, the left navigation pane where bookmarks are provided links you directly to the desired setup page, including **LAN**, **WAN**, **System**, **Firewall**, **VPN**, **Virtual Server**, **Advanced**, **Status** and **Help**.

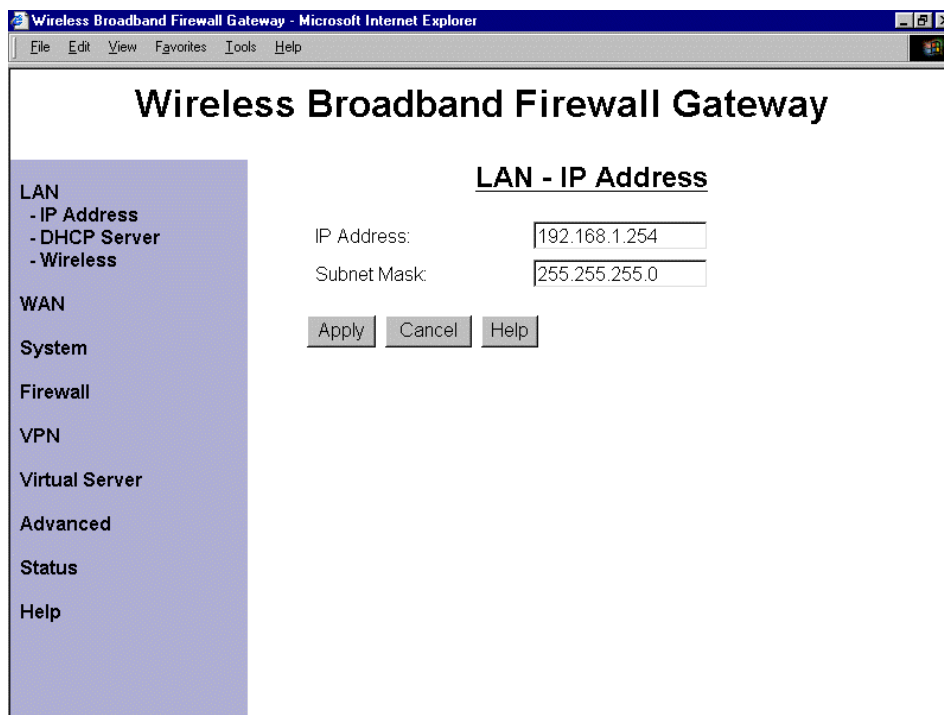


Click on the desired item to expand the page in the main navigation pane.

3.4.1 LAN

This screen contains settings for LAN interface attached to the LAN port.

IP Address



Wireless Broadband Firewall Gateway

LAN

- IP Address
- DHCP Server
- Wireless

WAN

System

Firewall

VPN

Virtual Server

Advanced

Status

Help

LAN - IP Address

IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

Apply Cancel Help

IP Address: Default at 192.168.1.254.

This is the device IP address in LAN site. If you plan to change it to another IP address to a different range of IP subnet. Please make sure your PC is also located at the same IP subnet. Otherwise, you may not be able to access the product.

Subnet Mask: Default at 255.255.255.0.



*If you ever forget the LAN IP address, we provide an utility running in MS Windows to find it automatically. It is included in the installation CD, named **RouterFinder.EXE**. (The PC with RouterFinder.EXE and device should locate at the same local area network, LAN.)*

DHCP Server

The screenshot shows a web browser window titled "Wireless Broadband Firewall Gateway - Microsoft Internet Explorer". The main heading is "Wireless Broadband Firewall Gateway". On the left is a navigation menu with the following items: LAN, - IP Address, - DHCP Server, - Wireless, WAN, System, Firewall, VPN, Virtual Server, Advanced, Status, and Help. The "LAN - DHCP Server" page is active. It features a sub-heading "LAN - DHCP Server" and two radio buttons: "Enable" (selected) and "Disable". Below these is the text "Specify IP address pool". There are two input fields: "From :" with the value "192.168.1.100" and "To :" with the value "192.168.1.199". At the bottom are three buttons: "Apply", "Cancel", and "Help".

Ⓐ Disable: Check to disable the product to distribute IP Addresses to the local network.

If you check this selection, **Disable**, remember to specify a static IP address, subnet Mask, and DNS setting for each of your local computers. Be careful not to assign the same IP address to different computers.

Ⓐ Enable: Check to enable the product to distribute IP Addresses, subnet mask and DNS setting to computers. Hence, the following fields will be activated.

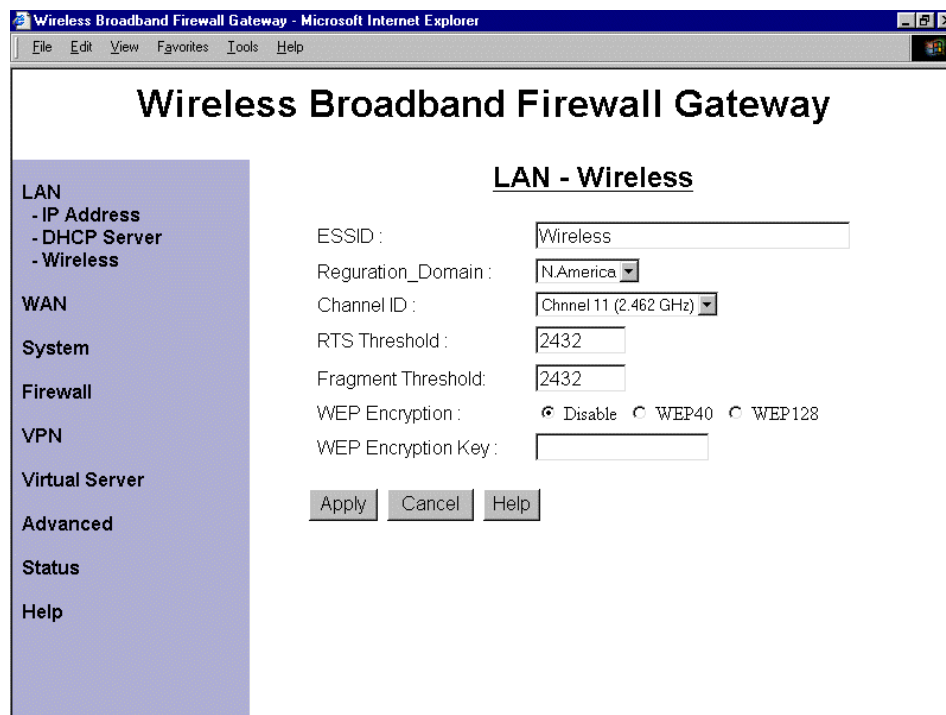
Specify IP address pool

From: Enter the start address of this local IP network address pool. The pool is a piece of continuous IP address segment. The default value is **192.168.1.100**.

To: Enter the last address of this local IP network address pool that you want the DHCP server to assign IP addresses to. The default value is **192.168.1.199**.

With this case, the DHCP pool is from 192.168.1.100 to 192.168.1.199. Therefore, the local computer will get an IP address located at this range randomly.

Wireless



ESSID: Enter the unique ID given to the Access Point (AP) built in the wireless broadband firewall gateway. To connect to this device, your wireless clients must have the same ESSID as that of this device.

Reguration_Domain: There are five Reguration_Domain for you to choose, including **N.America**, **Europe**, **France**, and **Spain**. Then, the Channel ID will be different based on this setting.

Channel ID: Select the ID of channel you would like to use.

RTS Threshold: Considering collision may happen when two wireless mediums send data at the same time, the RTS (Request to Send) protocol provides a solution to prevent data collisions. The RTS mechanism will be activated if the packet size exceeds the threshold value you set.

Fragment Threshold: In the wireless communication, shorter packets may have better reliability. The fragmentation mechanism makes it possible for you to split the packet if your wireless broadband firewall gateway often transmits large files in wireless network. This mechanism will be activated if the packet size exceeds the threshold value you set.

WEP Encryption: To prevent unauthorized wireless stations from accessing data transmitted over the network, the wireless broadband firewall gateway offers highly secure data encryption, known as WEP. If you require high security in transmission, there are two alternatives, WEP 40 and WEP 128, for your selection.

WEP Encryption Key: Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as that of the device.

3.4.2 WAN

The screens below contain settings for the WAN interface toward Internet.

ISP

There are four ways to Obtain an IP Address Automatically (DHCP Client), PPPoE, Fixed IP, and PPTP Client for the device to have a public IP address and then to access Internet. You have to check with your ISP about which way is adopted.

Obtain an IP Address Automatically



Configure this WAN interface to use DHCP client protocol to get an IP address from ISP automatically. In other words, the ISP provides an IP address to the wireless broadband firewall gateway dynamically when login.

Router Name: Enter the router name provided by your ISP. The maximum input is **20** alphanumeric characters (case sensitive).

Domain Name: Enter the domain name provided by your ISP. The maximum input is **20** alphanumeric characters (case sensitive).

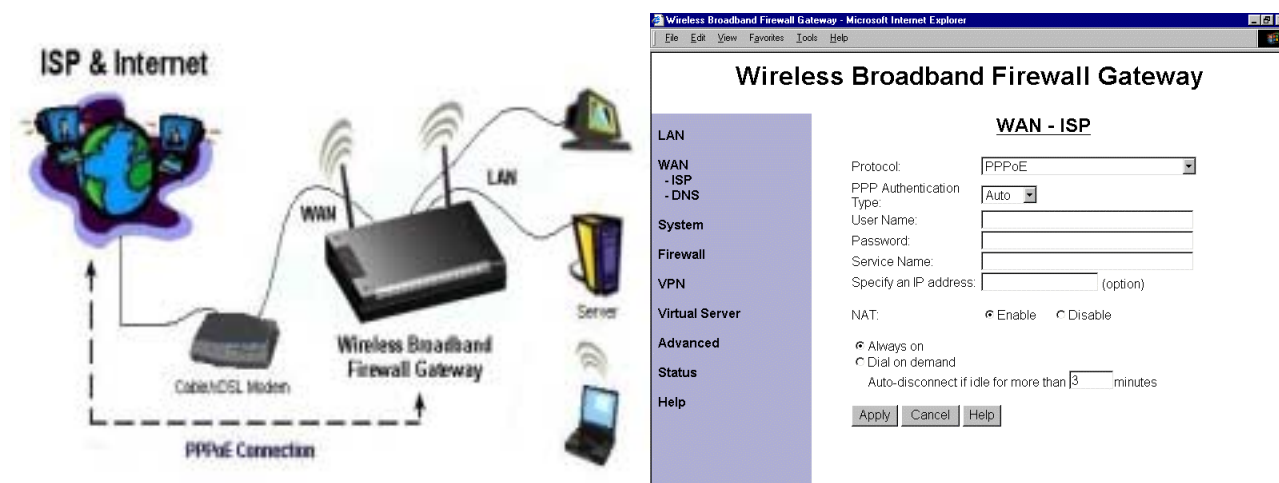
MAC Address: Specify the MAC address if your ISP needs it. The Default MAC address is router's MAC address.

NAT: The NAT feature allows multiple users to access Internet through a single IP account, sharing the single IP address from ISP. If users in the LAN site have public IP addresses and can access Internet directly, the NAT function can be disabled.



*The **Router Name**, **Domain Name** and **MAC Address** fields are needed for some ISPs. Please check it with your ISP. If you and your ISP do not know it, please leave it as default.*

PPPoE



PPPoE (PPP over Ethernet) is known as a dial-up DSL or cable service. It is designed to integrate the broadband services into the current widely deployed, easy-to-use, and low-cost dial-up-access networking infrastructure. Therefore, users can get greater access speed without changing the operation concept, sharing the same ISP account and paying for one access account. No PPPoE client software is required for local computer if you select this configuration.

PPP Authentication Type: Default at **Auto**.

User Name: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

Service Name: This item is for identification purpose. If it is required, your ISP will provide you the information. Maximum input is **20** alphanumeric characters.

Specify an IP address: Specify the router IP address if your ISP needs to use it.

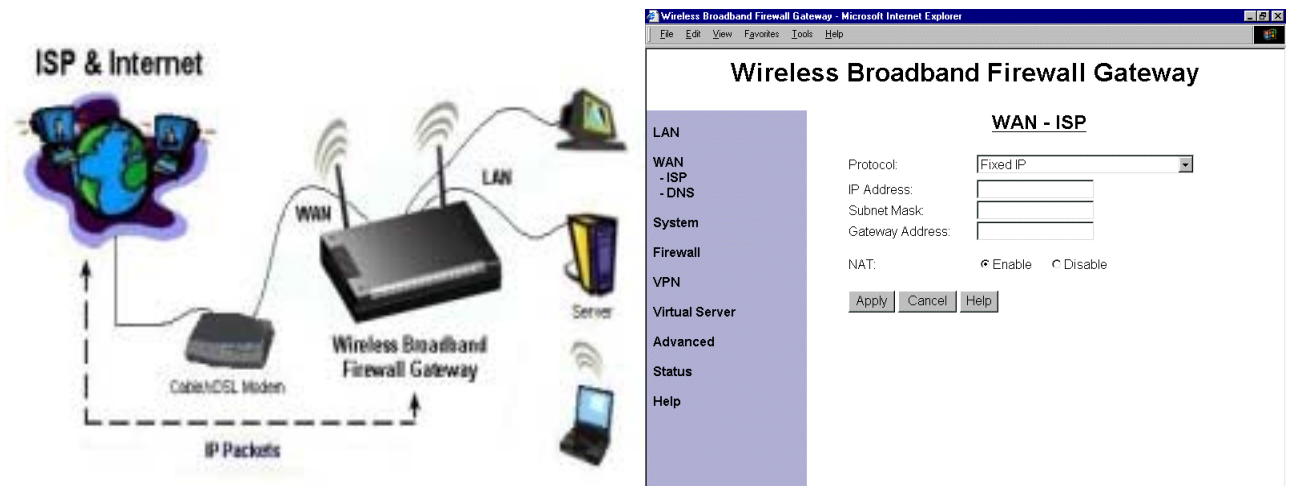
NAT: The NAT feature allows multiple users to access Internet through a single IP account, sharing the single IP address. If users in the LAN site have public IP addresses and can access Internet directly, the NAT function can be disabled.

☉ Always on: Check this radio button if you want to establish a PPPoE session when starting up. It will also automatically re-establish the PPPoE session when disconnected by ISP.

☉ Dial on demand: Check this radio button if you want to establish a PPPoE session only when there is a packet requesting for going out to the Internet.

Auto-disconnect if idle for more than minutes: Auto-disconnect the wireless broadband firewall gateway when there is no activity on the line for a predetermined period of time. You can input any number from **0 to 999**. The default value is **3** minutes.

Fixed IP



Configure this WAN interface with a specific IP address. This IP address should be given from ISP directly.

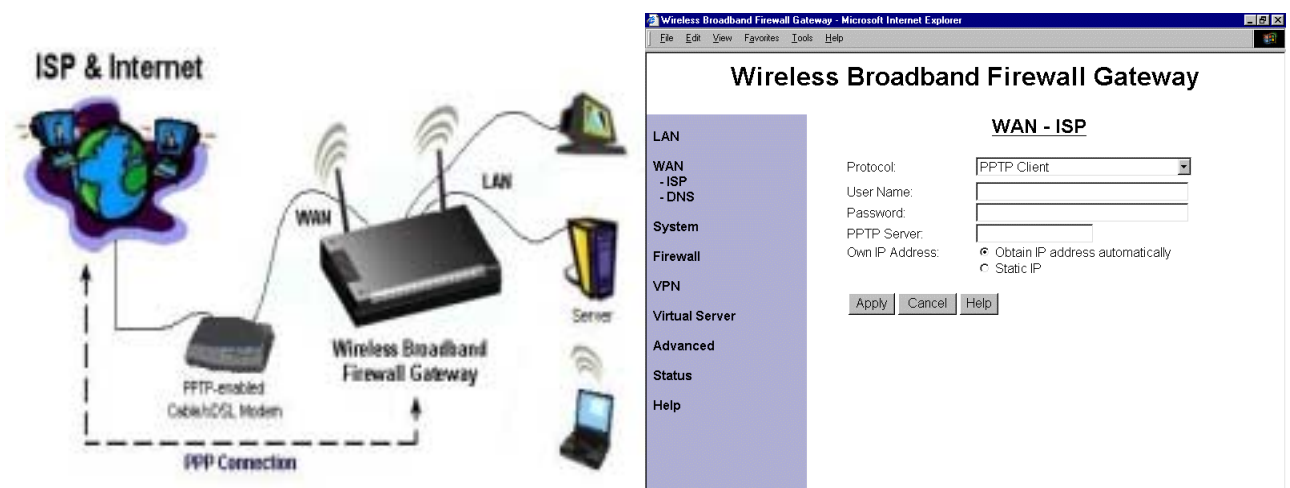
IP Address: Enter the information provided by your ISP.

Subnet Mask: Enter the information provided by your ISP.

Gateway Address: Enter the information provided by your ISP.

NAT: The NAT feature allows multiple users to access Internet through a single IP account, sharing the single IP address. If users in the LAN site have public IP addresses and can access Internet directly, the NAT function can be disabled.

PPTP Client



Some DSL/Cable modems only support PPTP tunnel method to access Internet such as Alcatel's DSL modem. Therefore, configure this WAN interface to use PPTP client carrying PPP information to make a tunnel with the DSL modem, then DSL modem will forward PPP information to ISP to establish a connection. When it is established, users can share this connection to access Internet.

Username: Enter the username, which can be up to **128** alphanumeric characters (case sensitive).

Password: Enter the password, which can be up to **128** alphanumeric characters (case sensitive).

PPTP Server: Enter the IP address of the PPTP Server.

Own IP Address: Choose **Obtain IP address automatically**, or choose **Static IP**. If Static IP is selected, enter the IP address below.

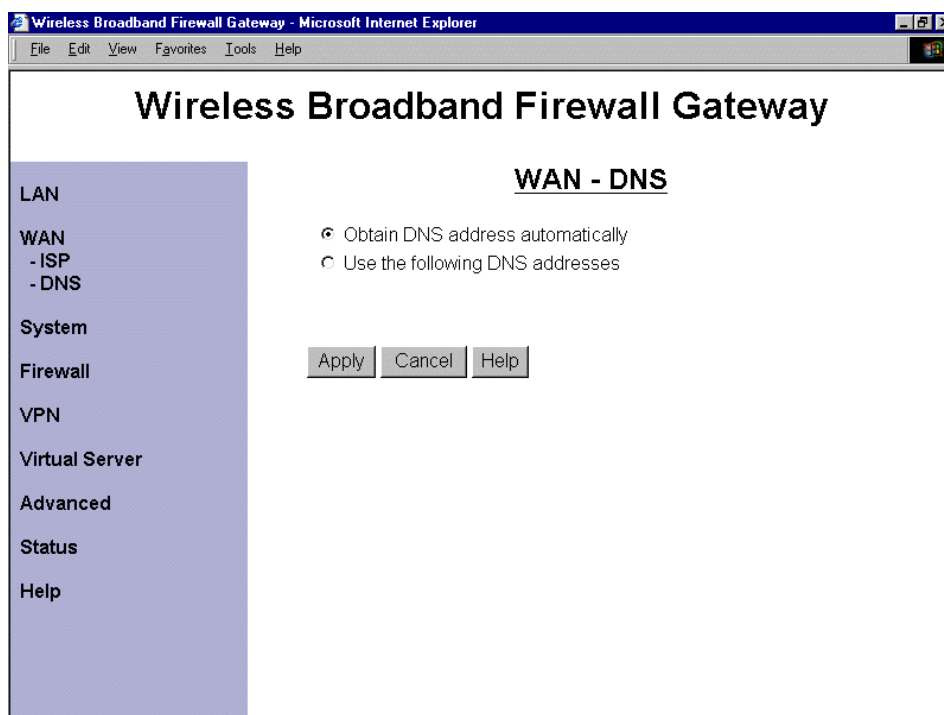


If you select WAN-ISP interface to be PPTP client, you will not see the VPN selection in the left pane after you reboot the device. Because the protocol stack of VPN is PPTP too, we did not implement the PPTP client over PPTP client mechanism. But if you select the other three methods to access Internet, we do allow a VPN (PPTP) connection to be established based on these three methods.

DNS

A Domain Name System (DNS) contains a mapping table for domain name and IP address. In the Internet, every host has a unique and friendly name such as www.yahoo.com and IP address. The IP address is very hard to remember, so that you may just enter the friendly name www.yahoo.com and DNS converts it to its equivalent IP address.

You can obtain Domain Name System (DNS) IP address automatically if ISP provides it when you logon. This **Obtain DNS address automatically** selection is set as default when you choose Obtain an IP Address Automatically, PPPoE, or PPTP Client as your WAN - ISP protocol.



Or your ISP may provide you with an IP address of DNS. If this is the case, you must enter the DNS IP address. Moreover, if you set Fixed IP as your ISP protocol, you can only enter the DNS IP Address instead of obtaining the address automatically.

The screenshot shows a web browser window titled "Wireless Broadband Firewall Gateway - Microsoft Internet Explorer". The main heading is "Wireless Broadband Firewall Gateway". On the left is a vertical navigation menu with the following items: LAN, WAN, - ISP, - DNS, System, Firewall, VPN, Virtual Server, Advanced, Status, and Help. The "WAN" item is selected. The main content area is titled "WAN - DNS". It contains two radio buttons: "Obtain DNS address automatically" (which is selected) and "Use the following DNS addresses". Below these are two text input fields: "Preferred DNS Address:" and "Alternate DNS Address:". At the bottom of the form are three buttons: "Apply", "Cancel", and "Help".

3.4.3 System

Password

The screenshot shows a web browser window titled "Wireless Broadband Firewall Gateway - Microsoft Internet Explorer". The main heading is "Wireless Broadband Firewall Gateway". On the left is a vertical navigation menu with the following items: LAN, WAN, System, - Password, - Time Zone, - Upgrade, - Factory Setting, - Reboot, - Logout, Firewall, VPN, Virtual Server, Advanced, Status, and Help. The "System" item is selected, and the "Password" sub-item is also selected. The main content area is titled "System - Password". It contains three text input fields: "Current Password:", "New Password:", and "Confirm New Password:". At the bottom of the form are three buttons: "Apply", "Cancel", and "Help".

In factory setting, there is no password protection when user accesses the product. It is recommended that you change the default password <BLANK> to ensure that someone cannot adjust your settings without your permission. <BLANK> means there is no password. Every time you change your password, please record the password and keep it at a safe place.

Please note that the maximum input for password is **16** alphanumeric characters long. Since it is **case sensitive**, be sure that you remember whether a letter is in upper or lower case and make sure that your Caps Lock is off.

Time Zone

Wireless Broadband Firewall Gateway

System - Time Zone

Choose your local time zone:

(GMT+01) Prague, Brussels, Copenhagen, Madrid

☒ Automatically adjust clock for daylight saving changes

SNTP Server IP Address:

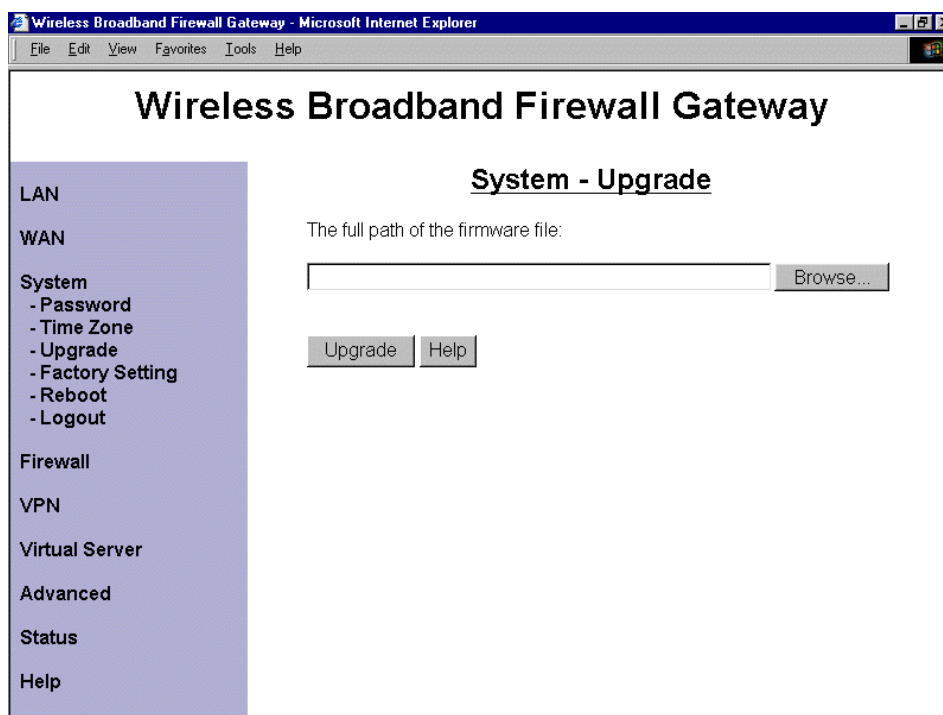
Apply Cancel Help

The wireless broadband firewall gateway does not have a real time clock on board; instead, it uses the simple network time protocol (SNTP) to get the current time from the SNTP server in outside network. Please choose your local time zone and click Apply button. You will get the correct time information after you really establish a connection to Internet. The current time of selected time zone will be shown in the Status – System window.

Automatically adjust clock for daylight saving changes: It is optional for different time zone area.

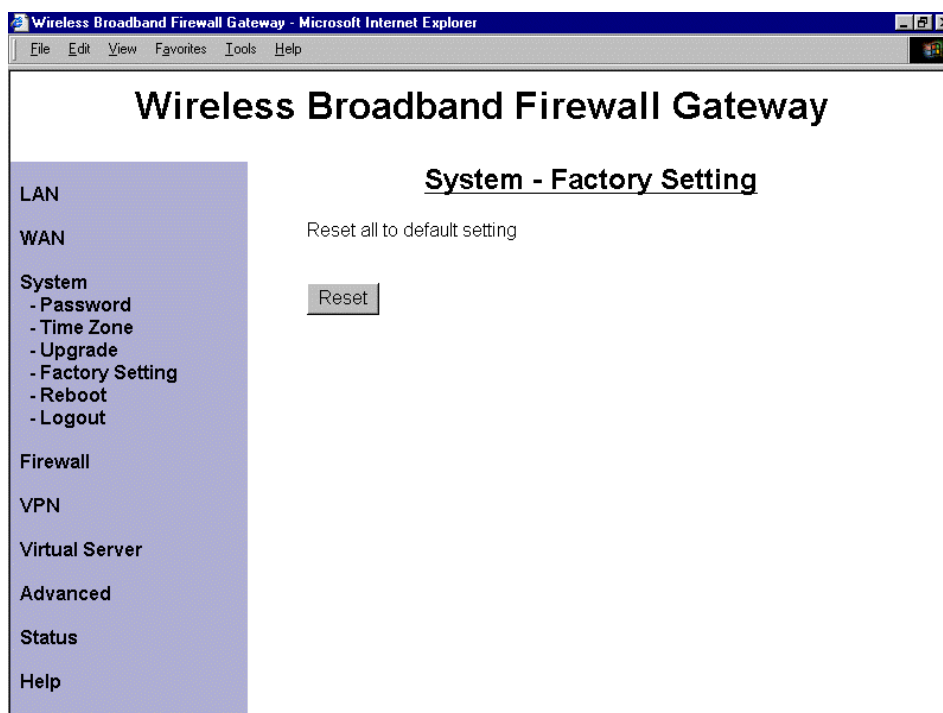
SNTP Server IP Address: Specify the IP address if you want to use your familiar SNTP server.

Upgrade



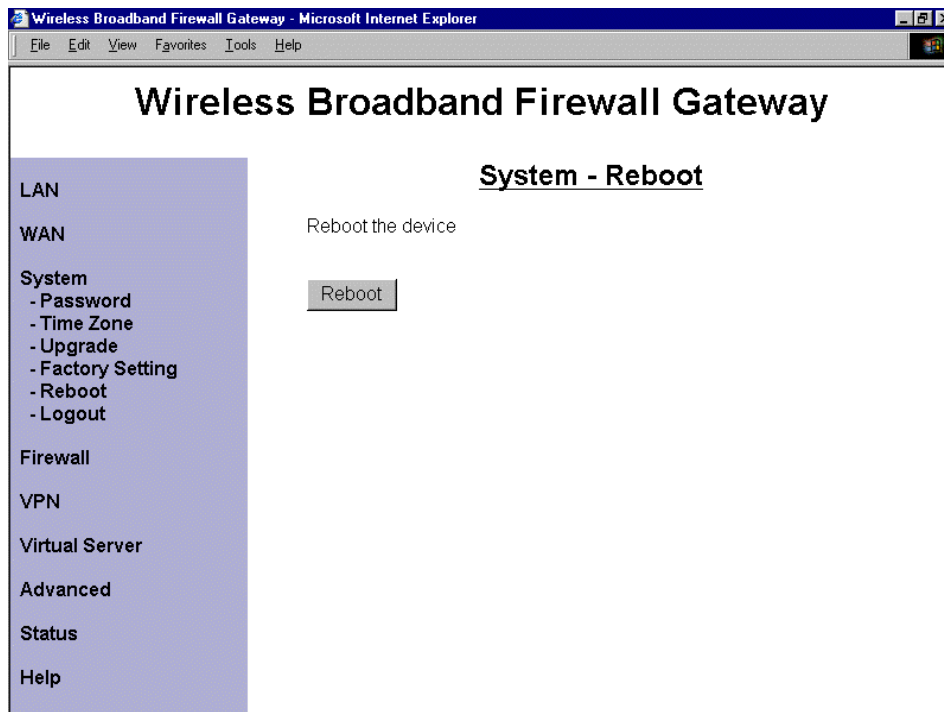
To upgrade the firmware of the product, you should download or copy the firmware to your local environment first. Press the **“Browse...”** button to specify the path of the firmware file. Then, click **“Upgrade”** to start upgrading. When the procedure is completed, the router will reset automatically to make the new firmware work.

Factory Setting



If for any reason, you have to reset this product back to factory default settings, be careful that the current settings will be lost and the settings are reset back to its default value. The factory default values is detailed in the *section 3.2 “Factory Default Settings”*.

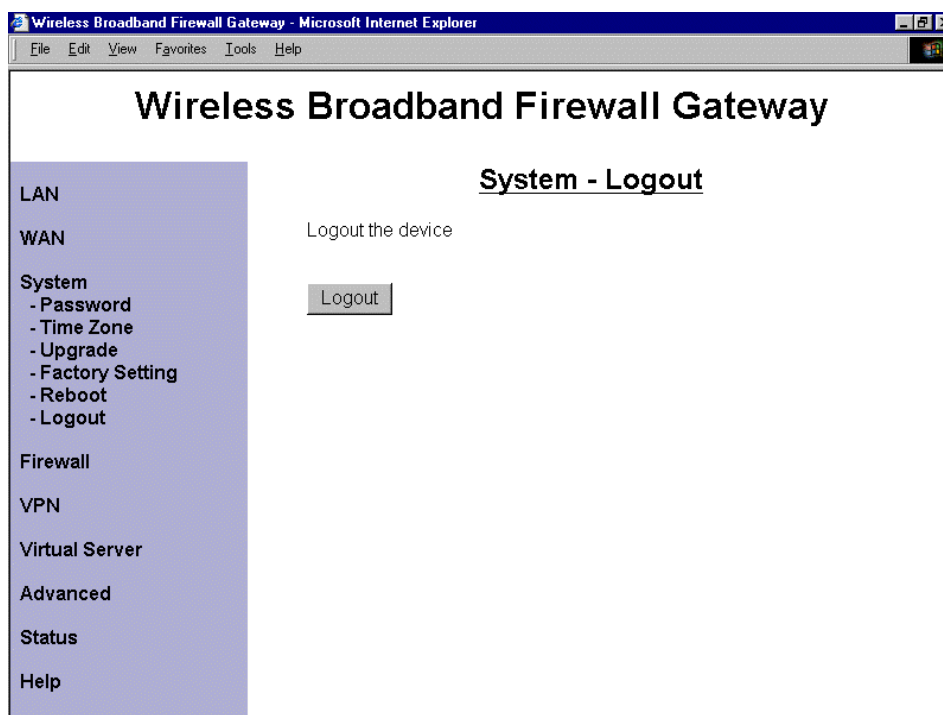
Reboot



In case the router stops responding correctly or in some other way stops functioning, you can perform the reboot. Your setting won't be changed. Performing the reboot, click on the **Reboot** button. Each time you reboot your wireless broadband firewall gateway, the following figure will appear. Please wait for auto-reconnection.



Logout

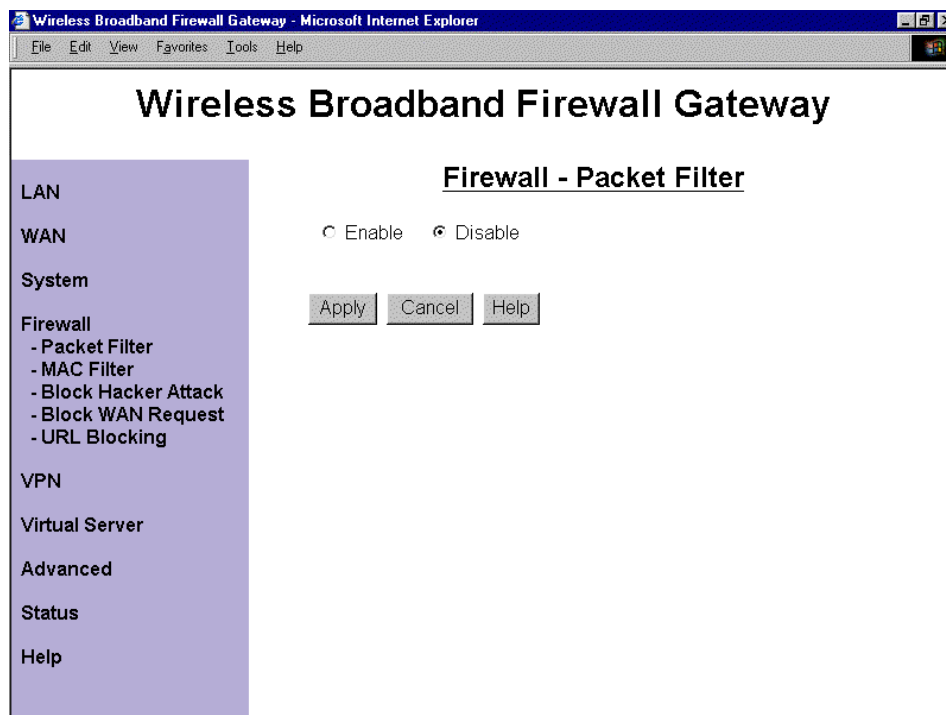


Logout the device when you finish configuring the wireless broadband firewall gateway.

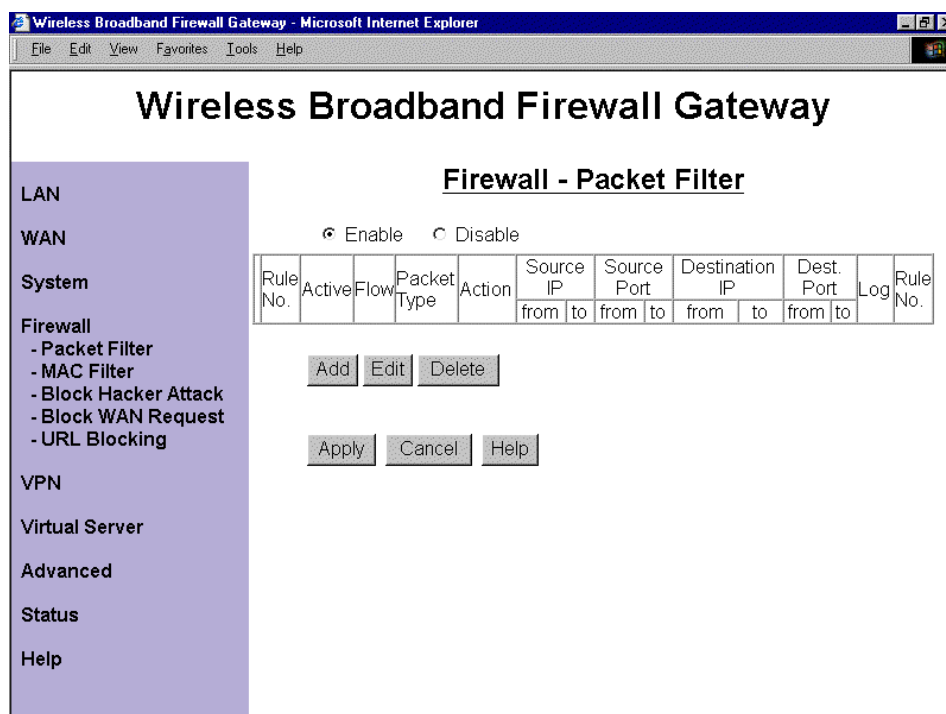
3.4.4 Firewall

User can decide to enable this firewall function including Packet Filter, Block Hacker Attack, and Block WAN request features for better security control or not. But be noted, it wastes network processor computation power. The performance will be lower about 5% to 10%. More firewall features will be added continually, please visit our web site to download latest firmware.

Packet Filter



Packet filtering function enables you to configure your Wireless Broadband Firewall Gateway to block specified internal/external user (**IP address**) from Internet access, or you can disable specific service request (**Port number**) to /from Internet. You must check the “**Enable**” radio button to make the following figure appear for further configuration.



This configuration program allows you to set up different filter rules up to 10 for different users based on their IP addresses or their network Port number. The relationship among all filters is “**or**” operation,

which means the device checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.

Add: Click this button to add a new packet filter rule. After click, next figure will appear.

Edit: Check the Rule No. you want to edit. Then, click the “Edit” button.

Delete: Check the Rule No. you want to delete. Then, click the “Delete” button.

Wireless Broadband Firewall Gateway - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Wireless Broadband Firewall Gateway

Firewall - Packet Filter

LAN

WAN

System

Firewall

- Packet Filter
- MAC Filter
- Block Hacker Attack
- Block WAN Request
- URL Blocking

VPN

Virtual Server

Advanced

Status

Help

Rule 1 ☒ Outgoing ☐ Incoming

Active: Packet Type:

Log: Action When Matched:

Source IP Address: From: To:

Destination IP Address: From: To:

Source Port: From: To:

Destination Port: From: To:

Apply Cancel Help

Outgoing Incoming: Determine whether the rule is for outgoing packets or for incoming packets.

Active: Choose “Yes” to enable the rule, or choose “No” to disable the rule.

Packet Type: Specify the packet type (TCP, UDP, ICMP or any) that the rule will be applied to.

Select **TCP** if you want to scope for the connection-based application service on the remote server using the port number. Or select **UDP** if you want to scope for the connectionless application service on the remote server using the port number.

Log: Choose “Yes” if you want to generate logs when the filter rule is applied to a packet.

Action When Matched: If any packet matches this filter rule, **Forward** or **Drop** this packet.

Source IP Address: Enter the incoming or outgoing packet’s source IP address(es).

Source Port: Check the TCP or UDP packet’s source port number(s).

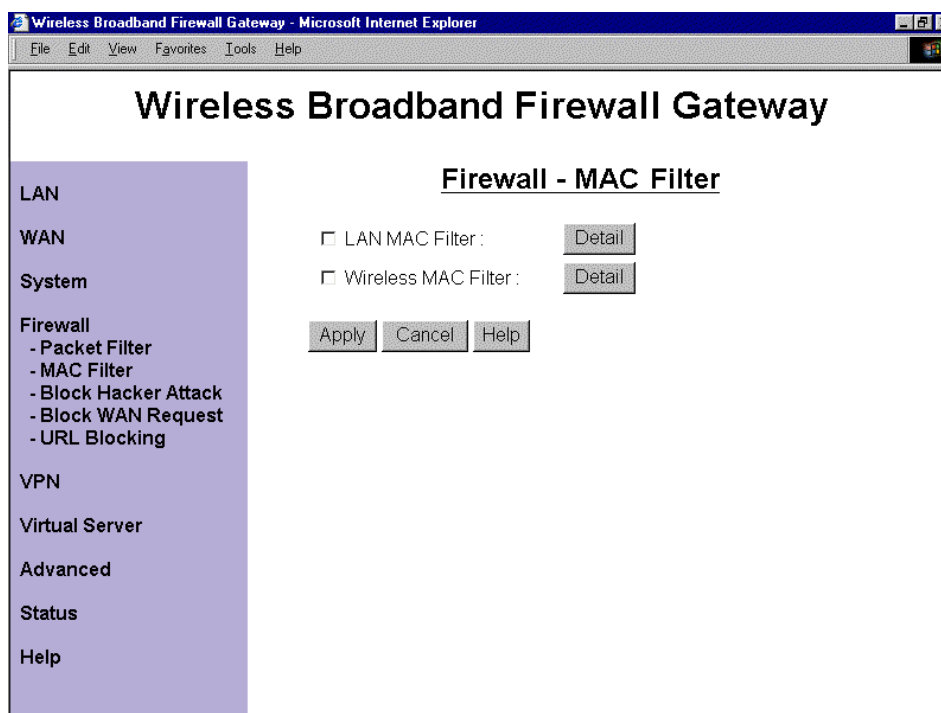
Destination IP Address: Enter the incoming or outgoing packet’s destination IP address(es).

Destination Port: Check the TCP or UDP packet’s destination port number(s).



If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of filtered private IP range in order to avoid conflicts because you do not know which PC in LAN is assigned to which IP address. The easiest and safest way is that the filtered IP address is assigned to specific PC that is not allowed to access outside resource such as Internet. You configure the filtered IP address manually to this PC, but it is still in the same subnet with the router.

MAC Filter



MAC filtering function enables you to configure your Wireless Broadband Firewall Gateway to block specified internal user (**MAC address**) from Internet access. The product provides two kinds of MAC filter.

LAN MAC Filter: Check if you want to enable the LAN MAC Filtering function and click the **Detail** button for further configuration.

Wireless MAC Filter: Check if you want to enable the Wireless MAC Filtering function and click the **Detail** button for further configuration.

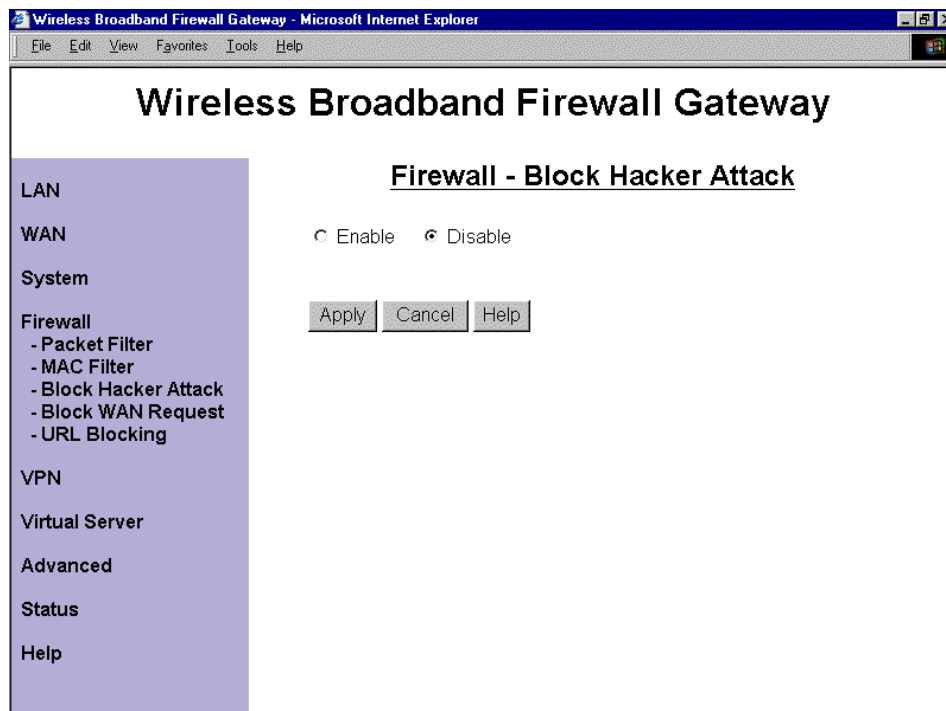
MAC Address: Enter the MAC address you want to configure. Then, click the “Add” button to add this MAC address into the following list. If you want to eliminate the MAC address you have already set from the address list, select the MAC address in the list table and click the “Delete” button. The MAC address will no longer exist.

MAC Address List

☉ **include:** Select this radio button if you want the MAC addresses in the list to be blocked from accessing the Internet.

☉ **exclude:** Select this radio button if you want to block all the PCs in the LAN from Internet access except for those with MAC address listed in the list.

Block Hacker Attack



The Wireless Broadband Firewall Gateway can automatically detect and block the DoS (Denial of Service) attack if user enables this function.

This kind of attack is not to achieve the confidential data of this network; instead, it aims to crush specific equipment or the entire network. If this happens, the users will not be able to access the network resources. The following hacker patterns are implemented.

- **Ping of Death (Length > 65535)**
- **Land Attack (Same source / destination IP address)**
- **IP with zero length**
- **Sync flooding**
- **Smurf Attack (ICMP Echo with x.x.x.0 or x.x.x.255)**
- **Snork Attack**
- **UDP port loop-back**
- **TCP NULL scan**

The screenshot shows a web browser window titled 'Wireless Broadband Firewall Gateway - Microsoft Internet Explorer'. The main heading is 'Wireless Broadband Firewall Gateway'. On the left is a navigation menu with items: LAN, WAN, System, Firewall (selected), VPN, Virtual Server, Advanced, Status, and Help. The 'Firewall' section is expanded, showing sub-items: Packet Filter, MAC Filter, Block Hacker Attack (selected), Block WAN Request, and URL Blocking. The main content area is titled 'Firewall - Block Hacker Attack'. It contains the following controls: a radio button for 'Enable' (selected) and a radio button for 'Disable'; a checkbox for 'Alert Mail'; an 'E-mail address:' label followed by a text input field; an 'SMTP server:' label followed by a text input field; and three buttons at the bottom: 'Apply', 'Cancel', and 'Help'.

Alert Mail: Check if you want to be informed by emails when hackers attack the router.

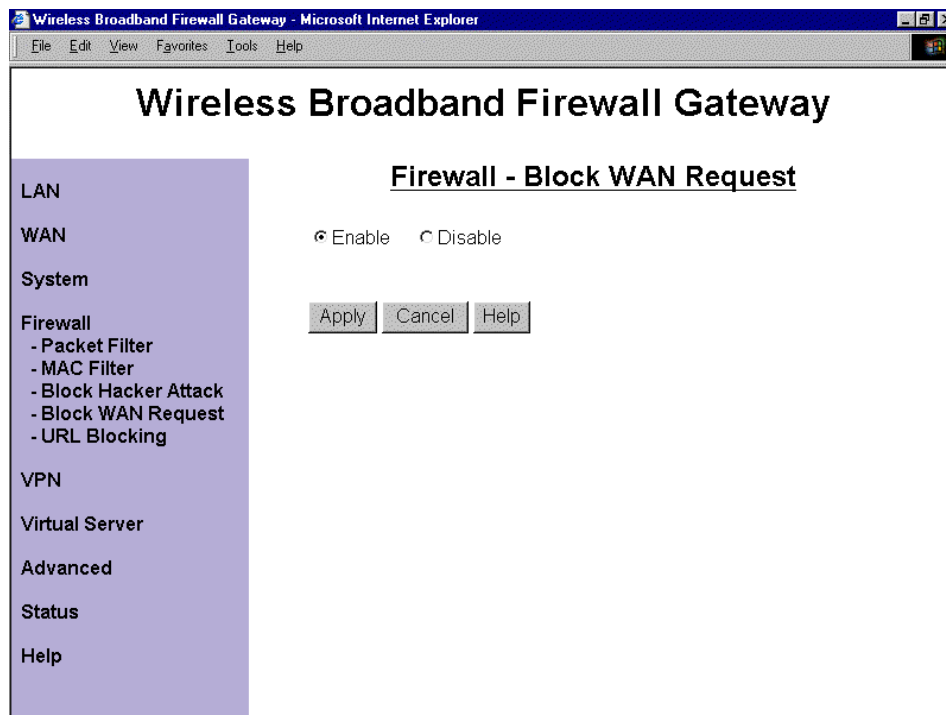
E-mail address: The alert mail will be sent to this address.

SMTP server: Enter the SMTP server of the above E-mail address.

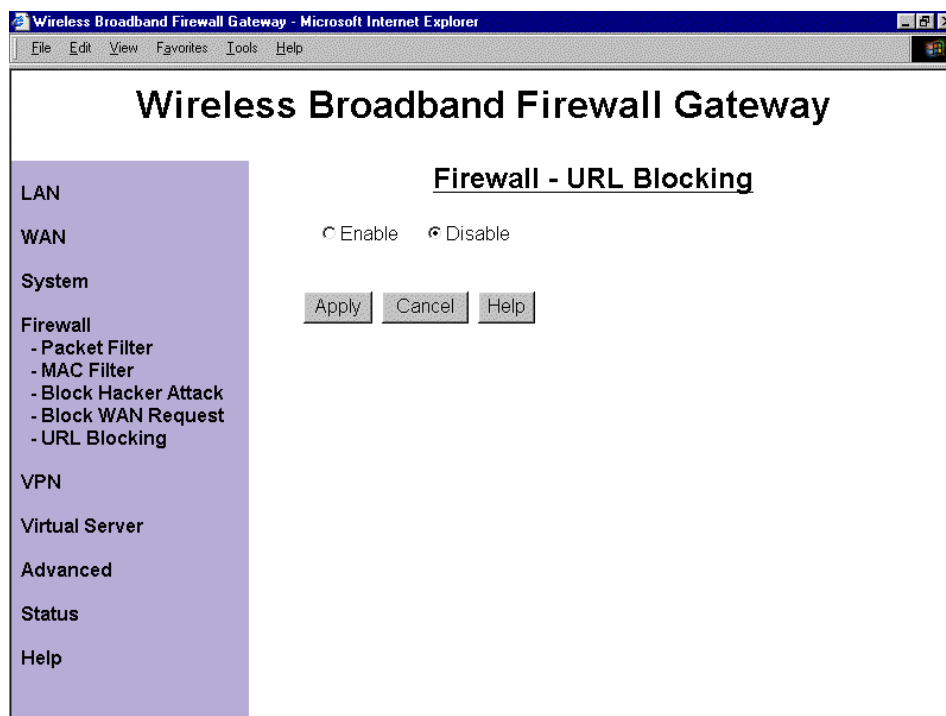
Block WAN Request

The screenshot shows the same web browser window as the previous one, but the configuration page is 'Firewall - Block WAN Request'. The navigation menu is identical. The 'Firewall' section is expanded, and 'Block WAN Request' is selected. The main content area is titled 'Firewall - Block WAN Request'. It contains the following controls: a radio button for 'Enable' and a radio button for 'Disable' (selected); and three buttons at the bottom: 'Apply', 'Cancel', and 'Help'.

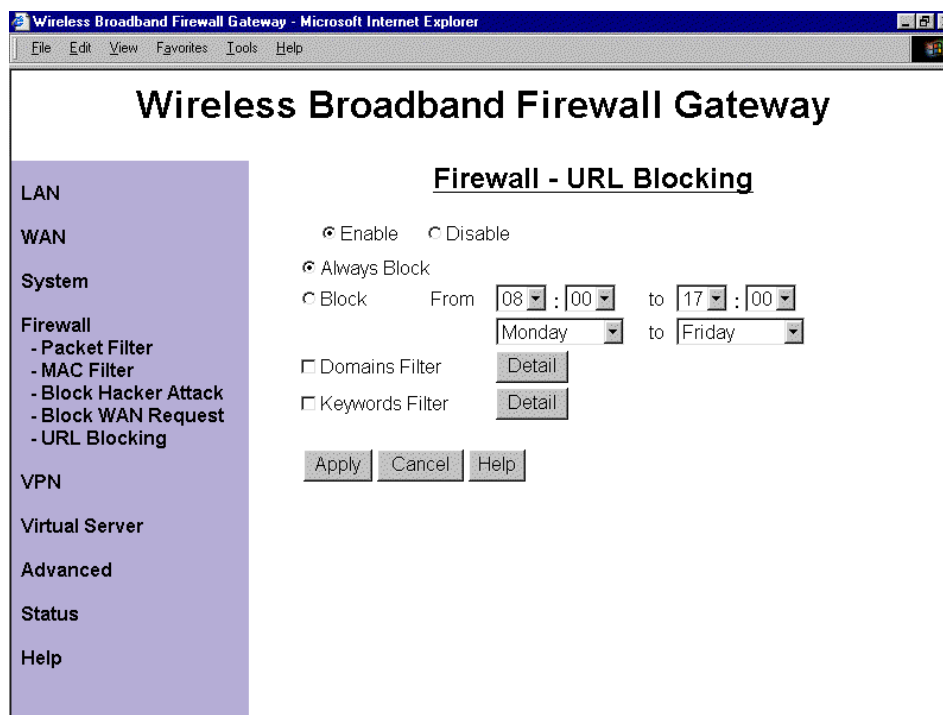
Check “Enable” if you want to exclude outside PING request from reaching on this router.



URL Blocking



URL blocking function enables you to avoid your LAN PCs from accessing some URLs. You must check the “**Enable**” radio button to make the following figure appear for further configuration.



☉ Always Block

☉ Block (From to)

Specify the time domain for the URL blocking function to take effect. If you want to implement this function all the time, select the radio button beside **Always Block**. Otherwise, select the radio button beside **Block** and scrolling down the list to specify your desired time field.

Domains Filter: Check if you want to enable the Domains Filtering function and click the **Detail** button for further configuration.

Keywords Filter: Check if you want to enable the Keywords Filtering function and click the **Detail** button for further configuration.

Domains Filter

The screenshot shows the 'Wireless Broadband Firewall Gateway' web interface in Microsoft Internet Explorer. The left sidebar contains a navigation menu with the following items: LAN, WAN, System, Firewall (with sub-items: - Packet Filter, - MAC Filter, - Block Hacker Attack, - Block WAN Request, - URL Blocking), VPN, Virtual Server, Advanced, Status, and Help. The main content area is titled 'Firewall - URL Blocking' and 'Domains Filtering'. It features two side-by-side panels: 'Trusted Domain' and 'Forbidden Domain'. Each panel has a 'Domain:' text input field, an 'Add' button, a 'Domain List' text area, and a 'Delete' button. At the bottom of the interface, there is a checkbox labeled 'Disable all web traffic except for Trusted Domains' and three buttons: 'Apply', 'Cancel', and 'Help'.

If the router is configured to allow internal users to access only certain specified domains, check the **Disable all web traffic except for Trusted Domains** and add domain name into the domain list. If the router is configured to allow internal users to access all websites except for some forbidden domain, add the forbidden domain name into the domain list. Users will no longer be able to access the websites from the LAN.

To add a domain name, enter its host name, such as www.bad-site.com into the text field under **Domain:** and click **Add**. The domain will be shown in the **Domain List**. Do not enter the complete URL of the site; that is, do not include <http://>. All subdomains are allowed. For instance, taking “yahoo.com” as the trusted domain means that www.yahoo.com, my.yahoo.com, and sports.yahoo.com will also be trusted.

To remove a site that was previously added, select its name in the list box, and click the **Delete** button to eliminate it from the list.

Keywords Filter

Wireless Broadband Firewall Gateway - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Wireless Broadband Firewall Gateway

LAN
WAN
System
Firewall
- Packet Filter
- MAC Filter
- Block Hacker Attack
- Block WAN Request
- URL Blocking
VPN
Virtual Server
Advanced
Status
Help

Firewall - URL Blocking

Keywords Filtering

Block WEB URLs which contain these keywords

Keyword:

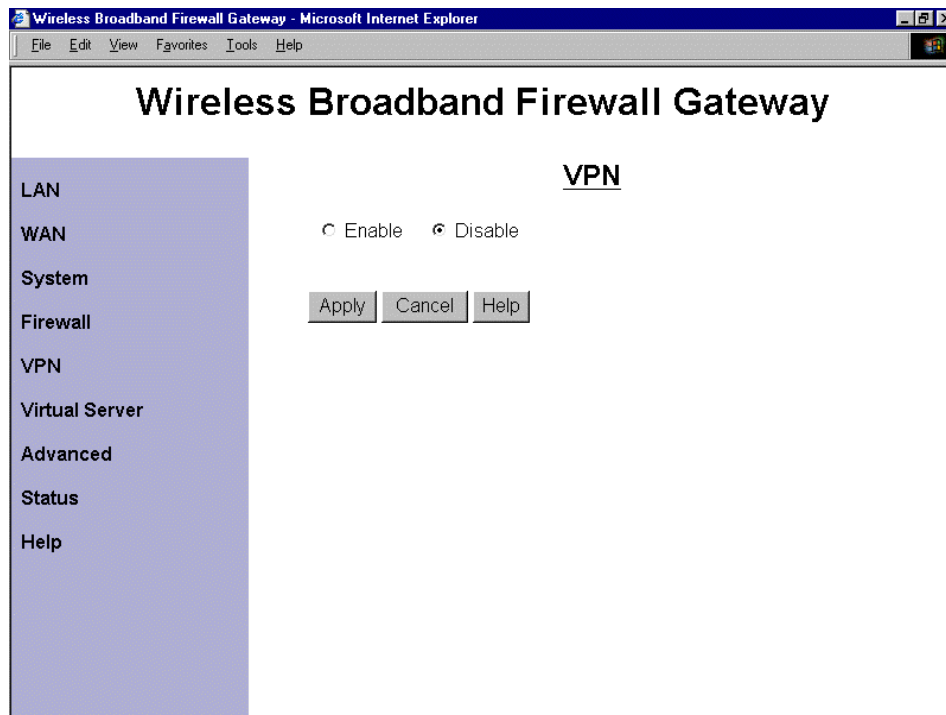
Keyword List

The router allows the administrator to block some WEB URLs containing certain keywords in this page. For example, if the keyword “xxx” is listed, the URL <http://www.new-site.com/xxx.html> would be blocked, even if it is not included in the domain filtering list. Keywords presented as site name are also blocked; that is, <http://www.xxxsite.com> cannot be accessed from LAN.

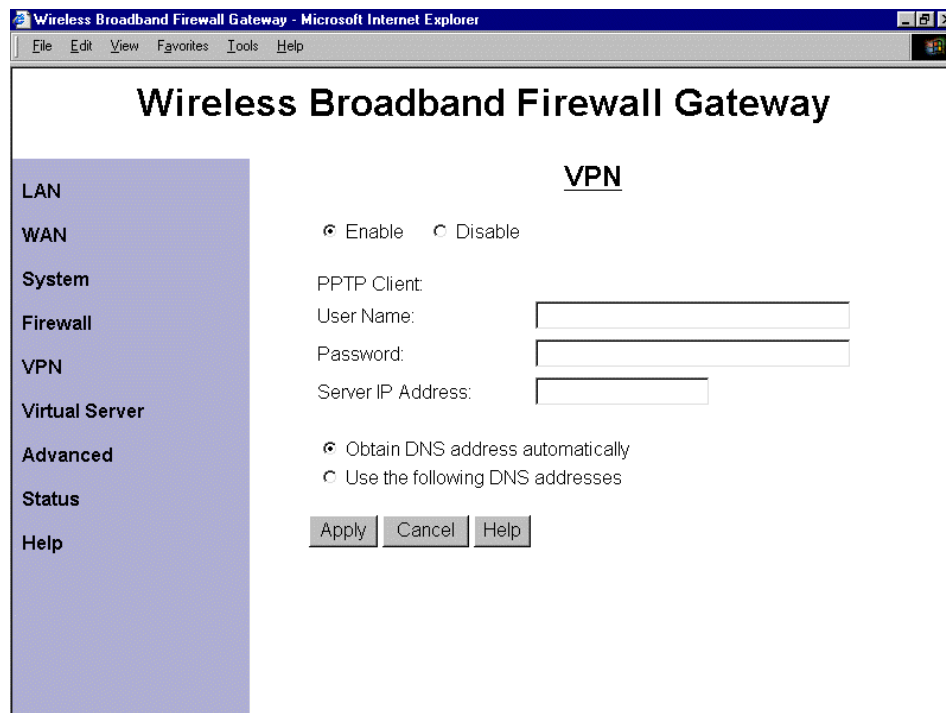
To add a keyword, enter it in the **Keyword** field and click **Add**.

To remove a keyword that was previously added, select it in the list box, and click the **Delete** button to eliminate it from the list.

3.4.5 VPN



VPN (Virtual Private Network) is a secured Internet protocol to allow users to access the company internal network resources outside the company network. If you want to make this function take effect, check the “Enable” button. Hence, the following fields will be activated.



Username: Enter the username. Maximum input is **128** alphanumeric characters (case sensitive).

Password: Enter the password. Maximum input is **128** alphanumeric characters (case sensitive).

Server IP Address: Enter the IP address of the PPTP Server.

You can obtain Domain Name System (DNS) IP address automatically if PPTP server provides it when you logon. Or your remote PPTP server may provide you with an IP address of DNS. If this is the case, you must enter the DNS IP address provided. Please refer to WAN-DNS section for more details. When you establish a VPN tunnel, the active DNS server is this one listed here, not that one listed in WAN-DNS section. Because you have established the tunnel with remote PPTP server, your network is connected to remote network directly. All the outgoing packets from your network will be sent to the remote network; therefore, you have to set DNS provided by remote network for domain name and IP address conversion.

This VPN function can connect and establish a PPTP tunnel to remote PPTP server on WAN. So, the router must connect to ISP first, and then use the PPTP client to establish a VPN connection.

3.4.6 Virtual Server

Wireless Broadband Firewall Gateway

Virtual Server

Item	Type	Service Port	Map To	IP Address	Enable
1	TCP		---	192.168.1	<input type="checkbox"/>
2	TCP		---	192.168.1	<input type="checkbox"/>
3	TCP		---	192.168.1	<input type="checkbox"/>
4	TCP		---	192.168.1	<input type="checkbox"/>
5	TCP		---	192.168.1	<input type="checkbox"/>
6	TCP		---	192.168.1	<input type="checkbox"/>
7	TCP		---	192.168.1	<input type="checkbox"/>
8	TCP		---	192.168.1	<input type="checkbox"/>

DMZ IP Address: 192.168.1

Apply Cancel Help

Being a natural Internet firewall, the product protects your network from being accessed by outside users. When it needs to allow outside users to access internal servers, e.g. Web server, FTP server, E-mail server or News server, this product can act as a virtual server. You can set up a local server with specific port number that stands for the service, e.g. Web (80), FTP (21), Telnet (23), SMTP (25), POP3 (110), DNS (53), ECHO (7), NNTP (119). When an incoming access request to the router for specified port is received, it will be forwarded to the corresponding internal server.

For example, if you set the **Service Port** number 80 (Web) to be mapped to the **IP Address** 192.168.1.2, then all the http requests to the router from outside users will be forwarded to the local server with IP address of 192.168.1.2.

Select **TCP** if you want to scope for the connection-based application service on the remote server using the port number. Or select **UDP** if you want to scope for the connectionless application service on the remote server using the port number.

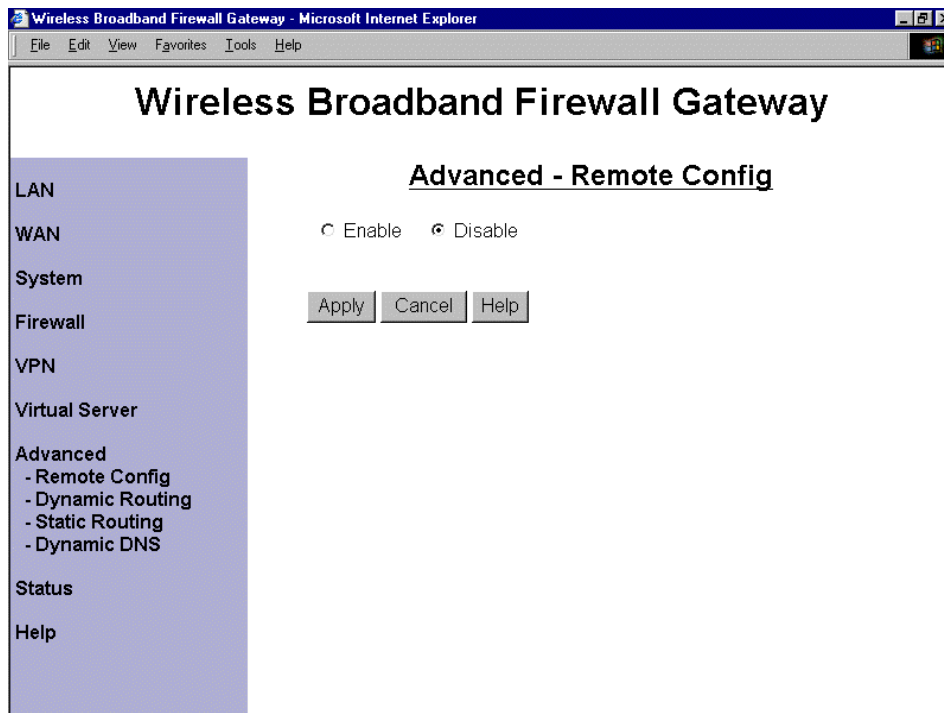
DMZ IP Address: Regarding the DMZ Host, it is a local computer exposed to the Internet. Therefore, an incoming packet will be checked by Firewall and NAT algorithms in the product, then passed to the DMZ host when packet is not sent from hacker and not matched by virtual server list.



If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easy way is that the IP address assigned to each virtual server should not fall into the range of IP addresses that are to be issued by the DHCP server. You configure the virtual server IP address manually, but it is still in the same subnet with the router.

3.4.7 Advance

Remote Config



Check “Enable” if you want to configure your wireless broadband firewall gateway from any PC in the Internet world with a web browser, such as Internet Explorer.

Wireless Broadband Firewall Gateway - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Wireless Broadband Firewall Gateway

Advanced - Remote Config

☒ Enable ☐ Disable

Specify the port for remote login

Port: (Range: 52520~65535)

Specify the IP addresses for remote login (Max. 254)

Start IP:

End IP:

Apply Cancel Help

LAN

WAN

System

Firewall

VPN

Virtual Server

Advanced

- Remote Config
- Dynamic Routing
- Static Routing
- Dynamic DNS

Status

Help

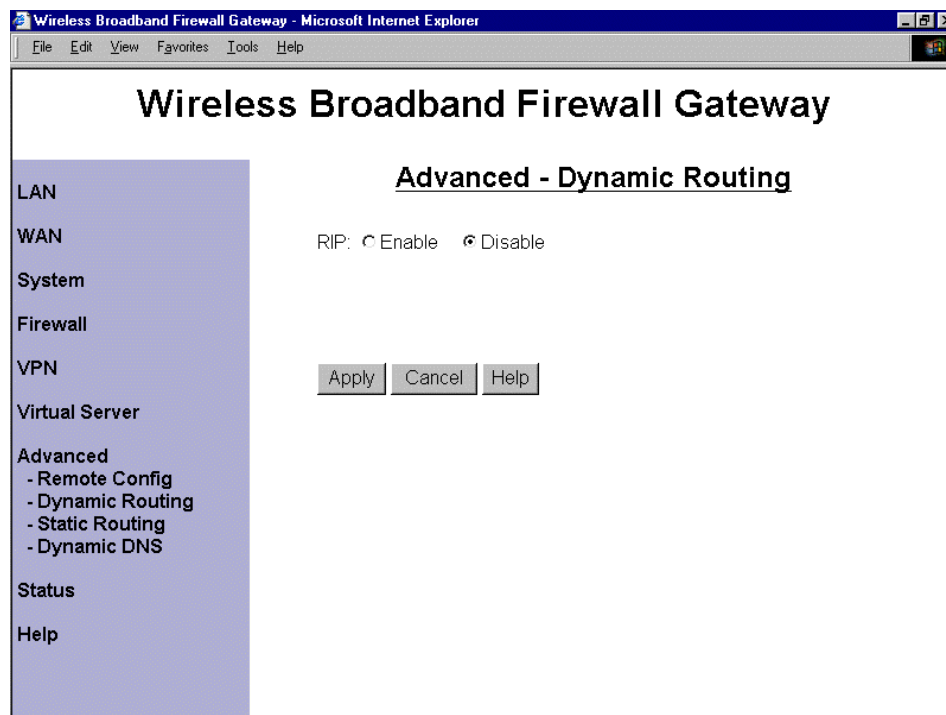
To configure this router remotely, use the URL "*http://WAN IP address:52520*" where WAN IP address is the IP address of the router's WAN port. You can find the value in the System Status. "**52520**" is the default port number; please use your own port if you change the default value.

If for any reason you want to limit the IP addresses for remote login, please enter the **Start IP** and the **End IP** address. But be noted that the range is not allowed to exceed 254.

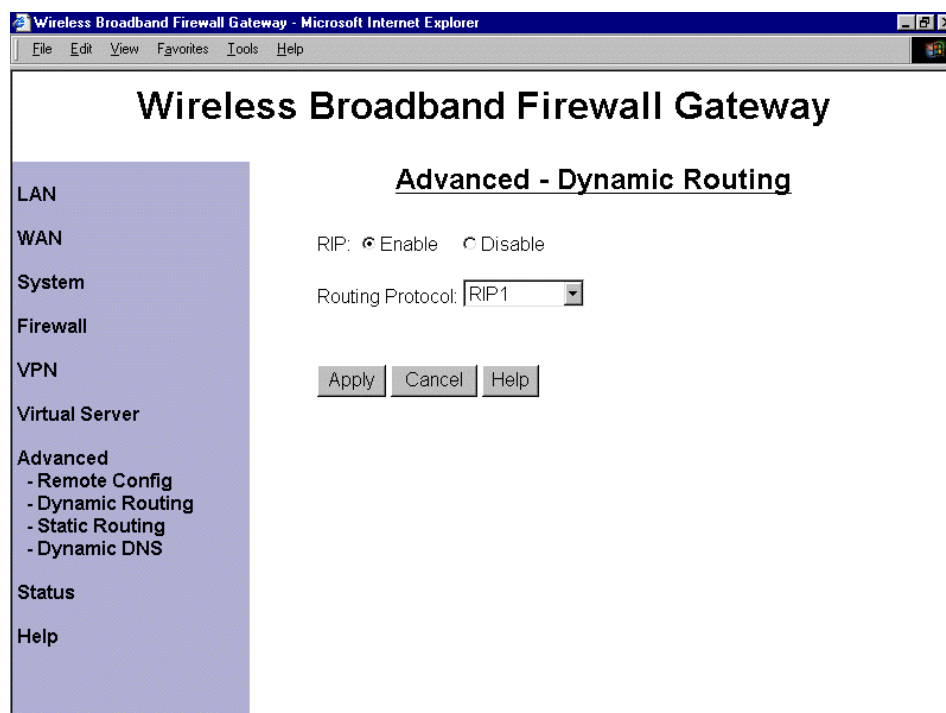


*If the NAT function is disabled, the URL should be "*http://LAN IP address*" where LAN IP address is the IP address of the router's LAN port. You can find the value in the System Status.*

Dynamic Routing



The dynamic routing function of the router can be used to allow the router to automatically adjust to physical changes in the network's layout. The router uses the dynamic RIP protocol. It regularly broadcasts routing information to other routers on the network. Choose the protocol RIP1 or RIP1+RIP2 you want the router to use to transmit / receive data on / from the network.



Static Routing

The screenshot shows the 'Wireless Broadband Firewall Gateway' configuration interface in Microsoft Internet Explorer. The left sidebar contains a tree view with the following items: LAN, WAN, System, Firewall, VPN, Virtual Server, Advanced (expanded), Status, and Help. Under the 'Advanced' section, the following sub-items are listed: - Remote Config, - Dynamic Routing, - Static Routing (selected), and - Dynamic DNS. The main content area is titled 'Advanced - Static Routing'. It features a table with the following headers: Item, Destination Subnet, Dest. Subnet Mask, and Gateway Address. Below the table are three buttons: Add, Edit, and Delete. At the bottom of the main area are three buttons: Apply, Cancel, and Help.

If you have another router with a LAN-to-LAN connection, you may create a static routing on the router that is the gateway to Internet.

Add: Click this button to add a new static routing. When you click this button, the next figure appears.

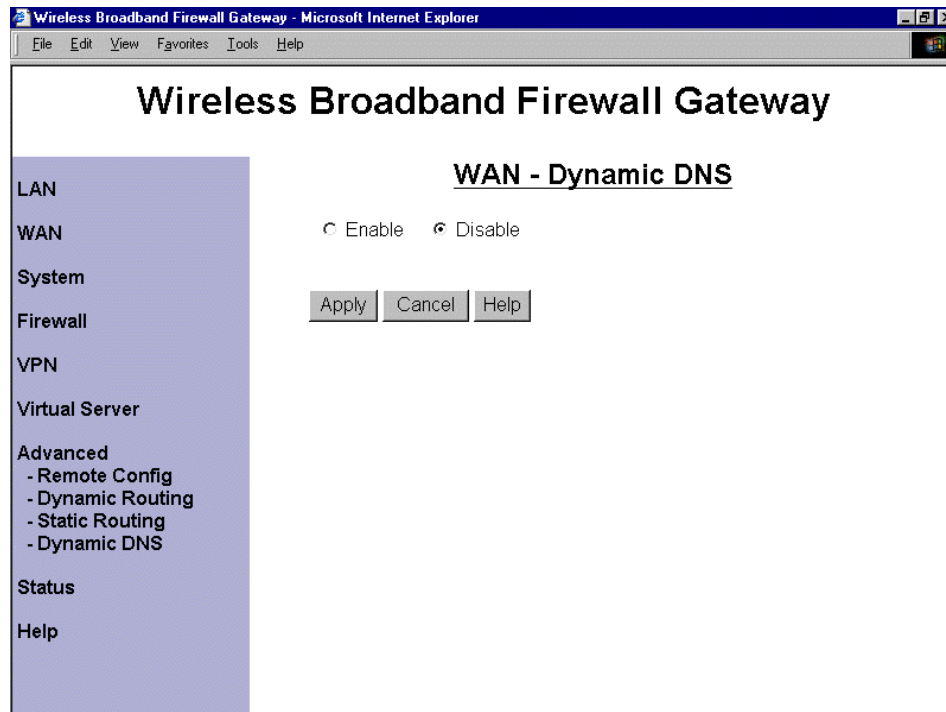
Edit: Check the item you want to edit. Then, click the “Edit” button.

Delete: Check the item you want to delete. Then, click the “Delete” button.

This screenshot shows the same 'Wireless Broadband Firewall Gateway' configuration interface, but with the 'Add' button clicked. The 'Advanced - Static Routing' section now displays a form for adding a new static routing entry. The form includes the following fields: Item (with the value '1'), Destination Subnet (with the value '0.0.0.0'), Dest. Subnet Mask (with the value '0.0.0.0'), and Gateway Address (with the value '0.0.0.0'). Below these fields are three buttons: OK, Cancel, and Help.

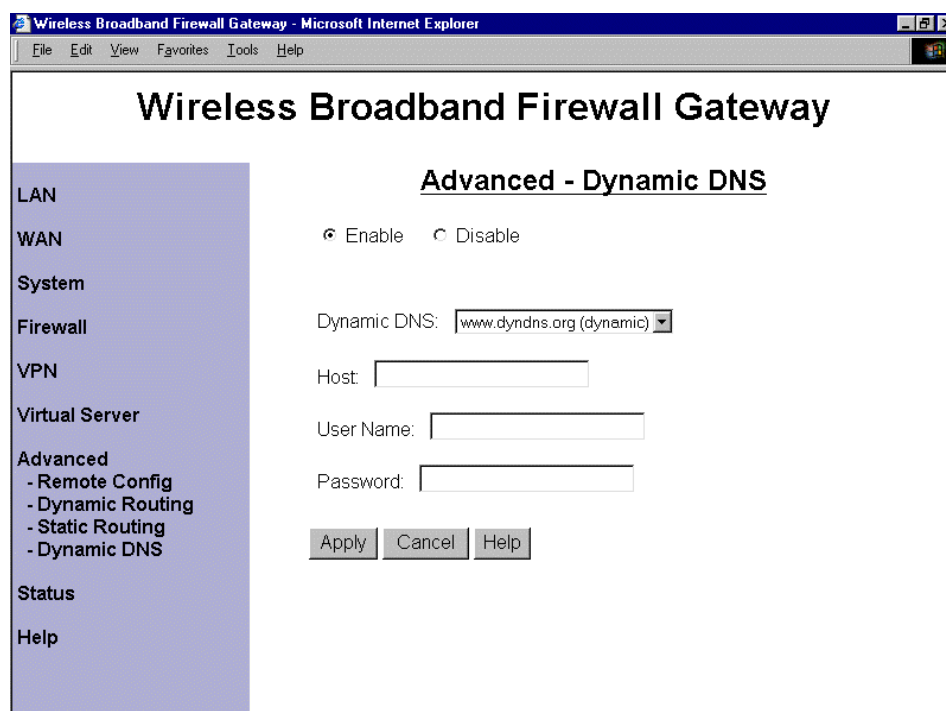
Destination Subnet / Dest. Subnet Mask / Gateway Address: Fill in these fields required by this Static Routing function.

Dynamic DNS



With Dynamic DNS service, a domain name can be translated into a dynamic IP address, which is often issued by ISP for dial-up service. A local server, such as Web server, Email server or FTP server, can then be easily accessed without knowing the changing IP address.

Check the “Enable” button to access the Dynamic DNS service.



You may sign up Dynamic DNS service at <http://www.dyndns.org> and there you can also register domain names.

Host: Enter one domain name you have registered.

User Name: Enter the username used for sign-up.

Password: Enter the password used for sign-up.

3.4.8 Status

System Status

Display the current LAN and WAN connection status.

The first line under the WAN segment displays the ISP protocol you set. You can see the status of connection from its right-side column.

If you choose “Obtain an IP Address Automatically” as your protocol, there will be a **“Renew”** button beside the connection status description. Click this **“Renew”** button whenever you want to get a new IP Address rather than the existent one. There are three connection statuses in total under this ISP protocol, including disconnected, connecting, and connected.

Current Time		
LAN		
IP Address		192.168.1.254
Subnet Mask		255.255.255.0
DHCP Server		Enabled
Tx Packets		0
Rx Packets		0
WAN		
Obtain an IP Address Automatically	Disconnected	<input type="button" value="Renew"/>
IP Address		
Gateway Address		
First DNS Address		
Second DNS Address		
NAT		Enabled

As for “PPPoE” protocol, its right column seems some kind different. When the PPPoE status is disconnected, you can click the **“Connect”** button to logon your ISP. You will see the system status changing from connecting, authenticating to connected if the procedure of connecting works smoothly. When you want to disconnect from your ISP under connected status, just click the **“Disconnect”** button.

Wireless Broadband Firewall Gateway - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Wireless Broadband Firewall Gateway

LAN

WAN

System

Firewall

VPN

Virtual Server

Advanced

Status

- System Status
- Device Info
- System Logs
- Security Logs
- ARP Cache Table
- DHCP Table

Help

Status - System Status

Current Time		
LAN		
IP Address	192.168.1.254	
Subnet Mask	255.255.255.0	
DHCP Server	Enabled	
Tx Packets	0	
Rx Packets	0	
WAN		
PPPoE	Disconnected	<input type="button" value="Connect"/>
IP Address		
Gateway Address		
First DNS Address		
Second DNS Address		
NAT	Enabled	

In the “PPTP Client” protocol, you can press the “Connect” button when the line is disconnected or press the “Disconnect” button when the line is connected.

Wireless Broadband Firewall Gateway - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Wireless Broadband Firewall Gateway

LAN

WAN

System

Firewall

VPN

Virtual Server

Advanced

Status

- System Status
- Device Info
- System Logs
- Security Logs
- ARP Cache Table
- DHCP Table

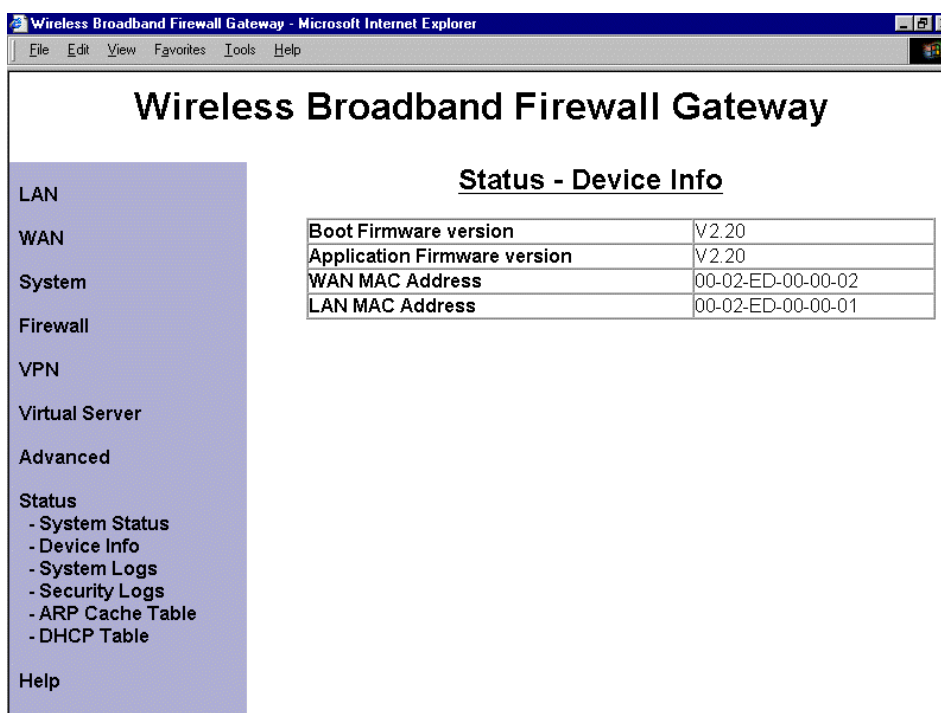
Help

Status - System Status

Current Time		
LAN		
IP Address	192.168.1.254	
Subnet Mask	255.255.255.0	
DHCP Server	Enabled	
Tx Packets	0	
Rx Packets	0	
WAN		
PPTP Client	Disconnected	<input type="button" value="Connect"/>
IP Address		
Gateway Address		
First DNS Address		
Second DNS Address		
NAT	Enabled	

This page will refresh automatically every 15 seconds, which enables you to get the most updated status of your system. You can also click the “**Refresh**” button to get the latest information of system status manually.

Device Info

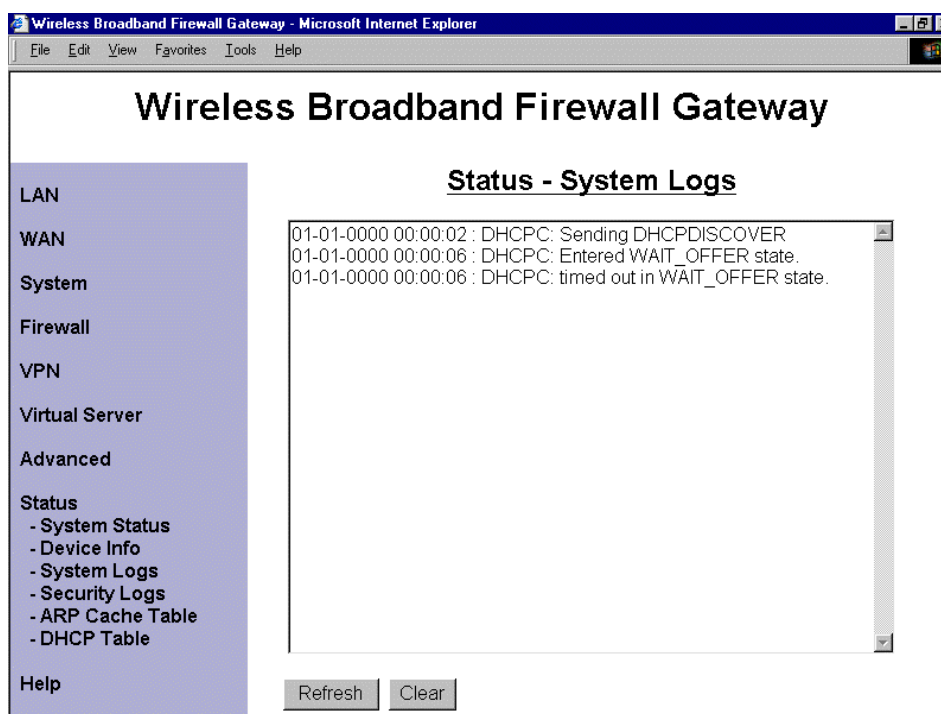


The screenshot shows a web browser window titled "Wireless Broadband Firewall Gateway - Microsoft Internet Explorer". The main heading is "Wireless Broadband Firewall Gateway". On the left is a navigation menu with items: LAN, WAN, System, Firewall, VPN, Virtual Server, Advanced, Status (expanded), and Help. The "Status" menu item is expanded, showing sub-items: - System Status, - Device Info, - System Logs, - Security Logs, - ARP Cache Table, and - DHCP Table. The "Device Info" sub-item is selected, displaying a table with the following data:

Status - Device Info	
Boot Firmware version	V2.20
Application Firmware version	V2.20
WAN MAC Address	00-02-ED-00-00-02
LAN MAC Address	00-02-ED-00-00-01

Display the current Firmware version and MAC addresses of your wireless broadband firewall gateway.

System Logs



The screenshot shows the same web browser window, but the "System Logs" sub-item is selected in the "Status" menu. The main heading is "Wireless Broadband Firewall Gateway". The "Status - System Logs" section displays a list of log entries in a text area:

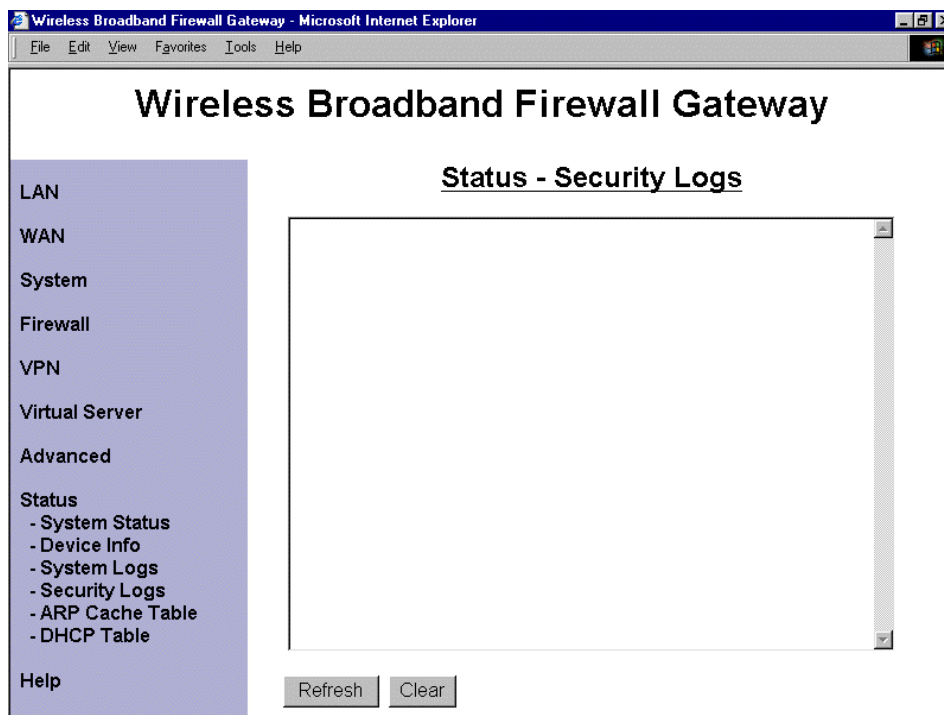
```
01-01-0000 00:00:02 : DHCPD: Sending DHCPDISCOVER
01-01-0000 00:00:06 : DHCPD: Entered WAIT_OFFER state.
01-01-0000 00:00:06 : DHCPD: timed out in WAIT_OFFER state.
```

Below the log entries are two buttons: "Refresh" and "Clear".

Display the system logs cumulated till the present time. You can trace the historical information through this function.

Refresh: Click “Refresh” to get the latest information of system logs.

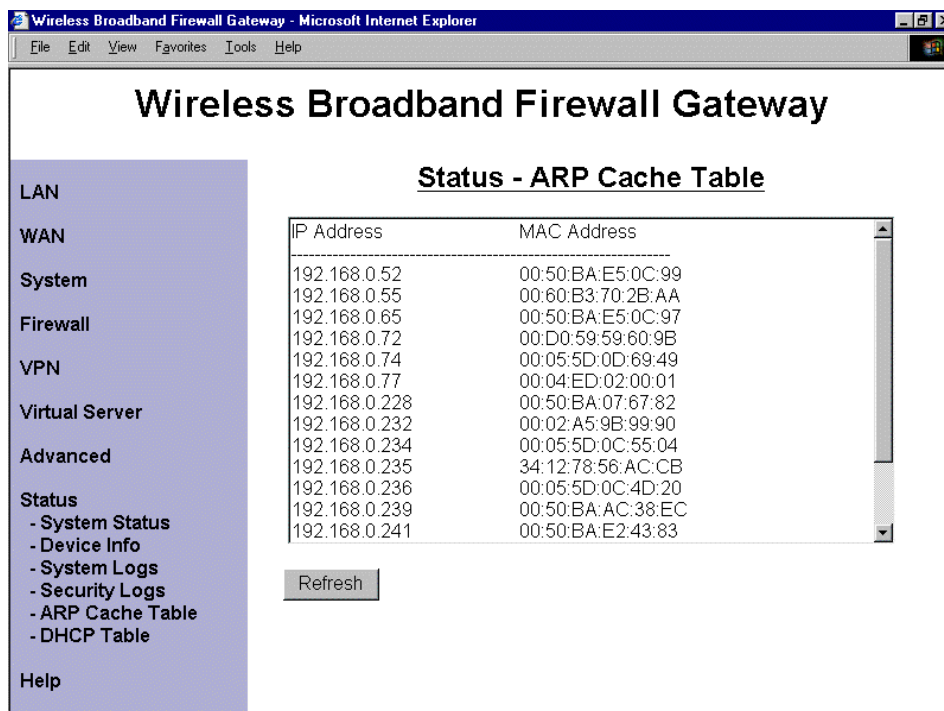
Security Logs



Display the information of security logs. If hacker attacks your sever, he will be isolated by the firewall function and the router will record related information. Hence, you know where the hacker comes from.

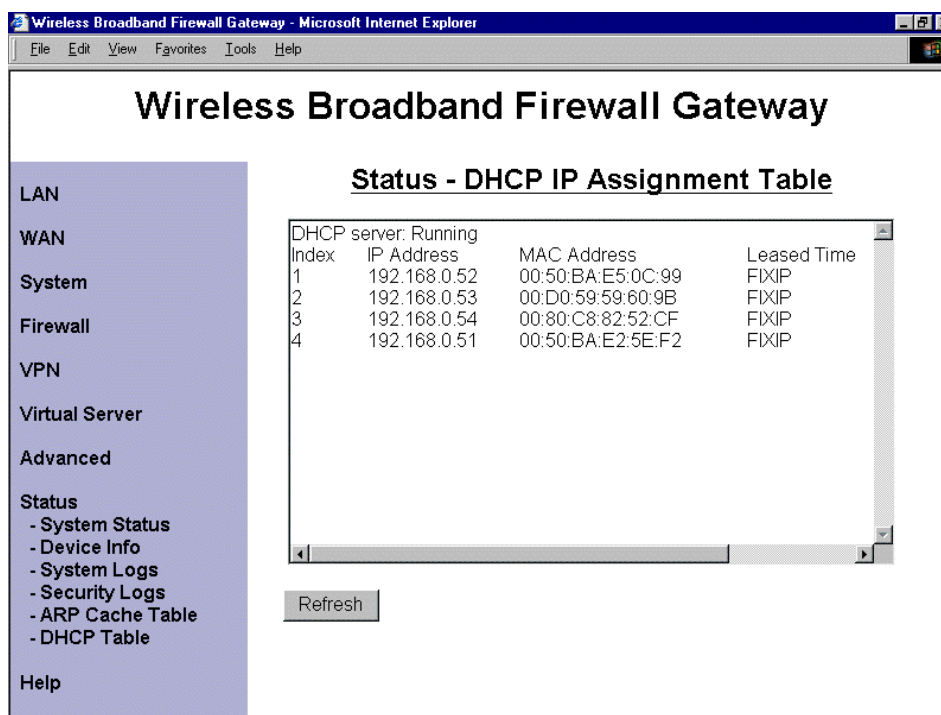
Refresh: Click “Refresh” to get the latest information of system logs.

ARP Cache Table



From this table, you can see the IP address of each PC in your LAN as well as its associated MAC address.

DHCP IP Assignment Table



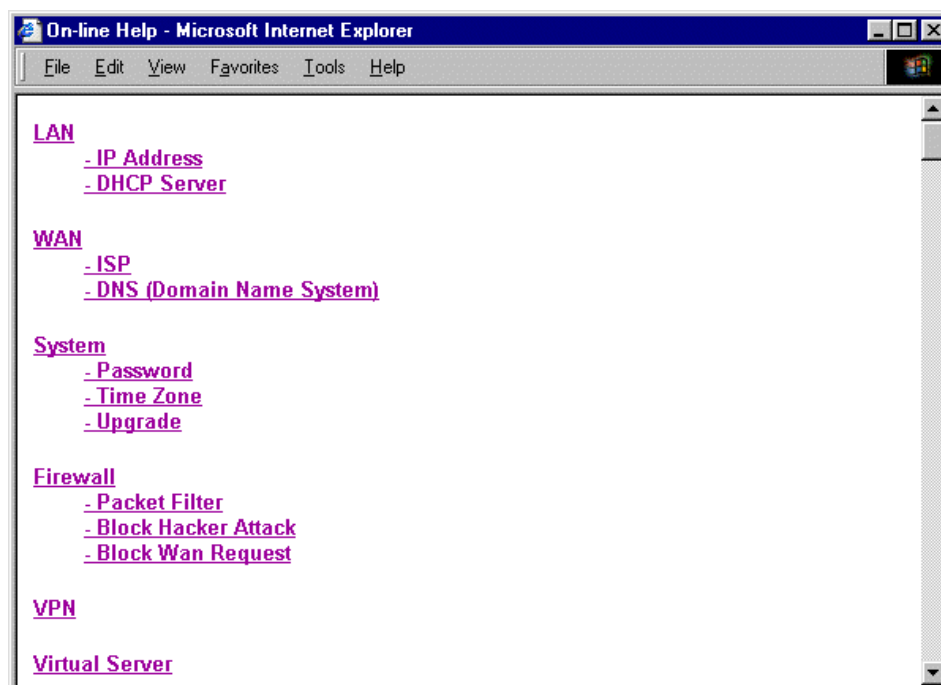
The screenshot shows a web browser window titled "Wireless Broadband Firewall Gateway - Microsoft Internet Explorer". The main content area is titled "Wireless Broadband Firewall Gateway" and "Status - DHCP IP Assignment Table". On the left is a navigation menu with links: LAN, WAN, System, Firewall, VPN, Virtual Server, Advanced, Status, and Help. The "Status" link is expanded, showing sub-links: - System Status, - Device Info, - System Logs, - Security Logs, - ARP Cache Table, and - DHCP Table. The main content area displays the DHCP server status as "Running" and a table of assigned IP addresses.

Index	IP Address	MAC Address	Leased Time
1	192.168.0.52	00:50:BA:E5:0C:99	FIXIP
2	192.168.0.53	00:D0:59:59:60:9B	FIXIP
3	192.168.0.54	00:80:C8:82:52:CF	FIXIP
4	192.168.0.51	00:50:BA:E2:5E:F2	FIXIP

Below the table is a "Refresh" button.

If you enable the DHCP server function of this device, you can see the assigned IP addresses and their associated MAC addresses from this table.

3.4.9 Help



The screenshot shows a web browser window titled "On-line Help - Microsoft Internet Explorer". The main content area displays a list of hyperlinks organized by category. The categories are LAN, WAN, System, Firewall, VPN, and Virtual Server. Each category has a list of sub-links.

Category	Sub-links
LAN	- IP Address, - DHCP Server
WAN	- ISP, - DNS (Domain Name System)
System	- Password, - Time Zone, - Upgrade
Firewall	- Packet Filter, - Block Hacker Attack, - Block Wan Request
VPN	
Virtual Server	

After click on the hyperlink of "Help" in the left pane, the following html page will jump out. This page would be a good reference as you precede the configuration.

3.5 Changing Password

Wireless Broadband Firewall Gateway

System - Password

Current Password:

New Password:

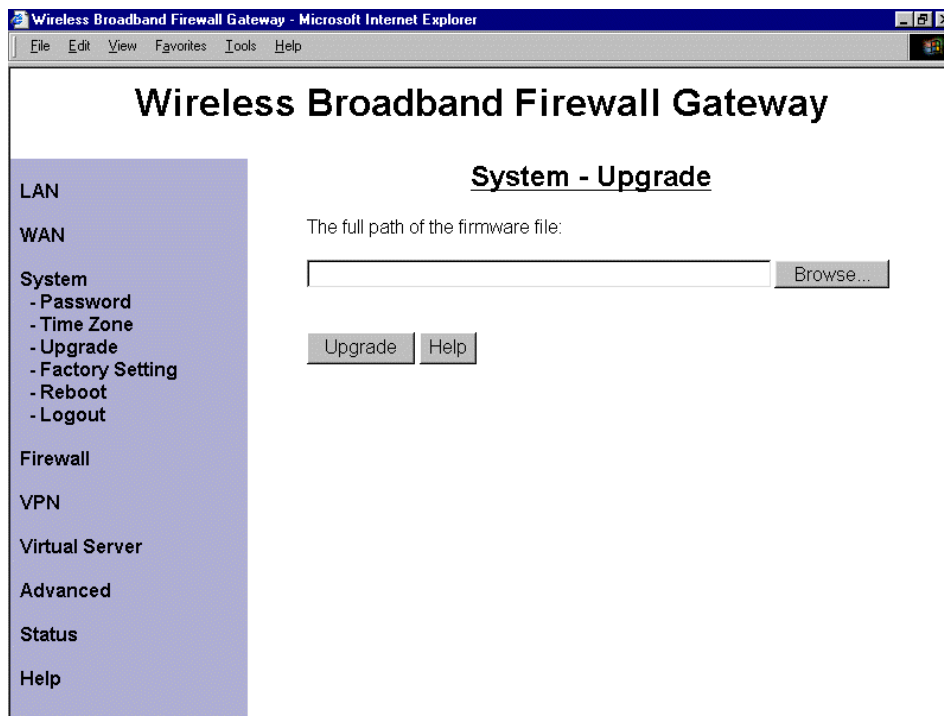
Confirm New Password:

Apply Cancel Help

In factory setting, there is no password protection when user accesses the product. It is recommended that you change the default password <BLANK> to ensure that someone cannot adjust your settings without your permission. <BLANK> means there is no password. Every time you change your password, please record the password and keep it at a safe place.

Please note that the maximum input for password is **16** alphanumeric characters long. Since it is **case sensitive**, be sure that you remember whether a letter is in upper or lower case and make sure that your Caps Lock is off.

3.6 Firmware Upgrade



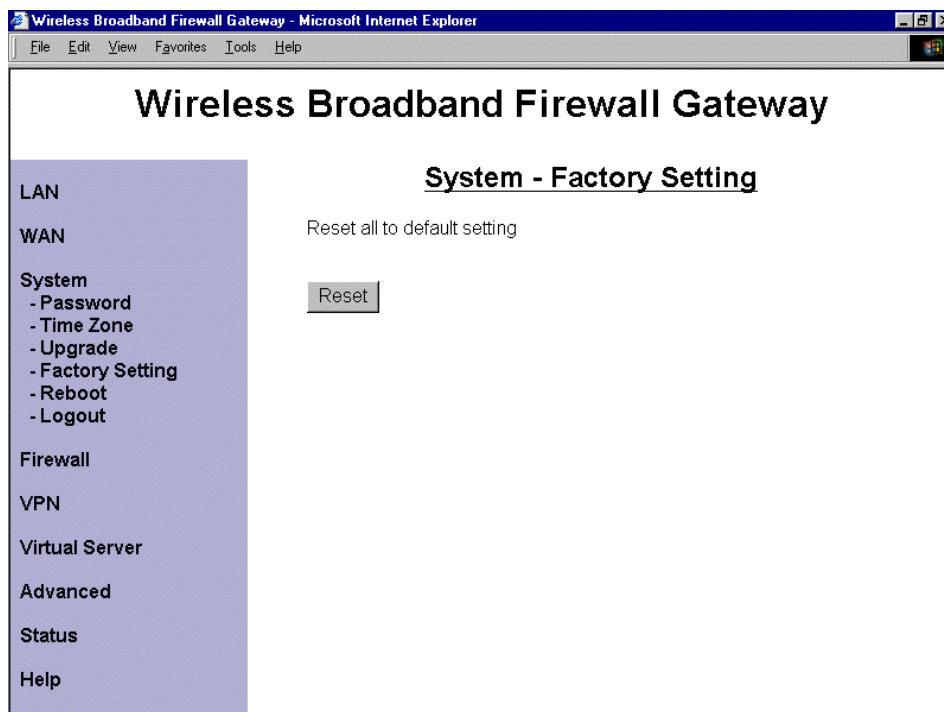
To upgrade the firmware of the product, you should download or copy the firmware to your local environment first. Press the **“Browse...”** button to specify the path of the firmware file. Then, click **“Upgrade”** to start upgrading. When the procedure is completed, the router will reset automatically to make the new firmware work.

Chapter 4

Troubleshooting

If the Wireless Broadband Firewall Gateway is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider. This could save you time and effort but if the symptoms persist, then consult your service provider.

How to do a factory reset?



If for any reason, you have to reset this device to factory default settings, be careful that the current settings will be lost and the settings are reset back to its default state. The factory default values are detailed in *section 3.2 “Factory Default Settings.”*

To reset to factory default settings, go to the Web configuration window. Enter **Factory Setting** under **System**, and then click **<Reset>** to begin the process.

Why do I get IP conflict information in my computer?

When you see the message box prompted for IP address conflict in your computer, it could be caused by rebooting the router or by two or more workstations occupying the same IP address. Please run the “**winipcfg**” utility to release all current configurations first, and then renew all if your computer is set to get an IP address automatically. The router will assign a new IP address to your computer if DHCP server is enabled in the router. Furthermore, please double check each workstation’s IP address from duplicate

IP. The “winipcfg.exe” is used for Win95, 98, and ME. For WinNT, 2000 and XP, please enter “ipconfig.exe”.

Why won't my Internet application work?

To protect your computer from Hackers, the product uses port blocking algorithm. A port likes a door into your computer. Each service on the Internet has an associated port. The product protects your computer by closing certain ports off so that malicious programs can't access your computer. Sometimes, however, you are using an application on purpose that uses one of these blocked ports. In this case you will have to manually open the port to allow the application to work properly.

Some applications that may be affected are

*Some **Email Programs***

*Some **Multi-Player Games***

*Some **Internet Phone/Video Conferencing Applications***

Also, there are some applications that require reverse connection over the Internet. In other words, when you are connected to these applications, you have to open your ports for forth and back connection.

The first thing you will need to do is determining what port or ports the application uses. Typically the fastest way to find this information is to go to the software maker's web site. Go to their support section and look for information related to NAT, Proxy Server, or Firewall. This information will typically list 1 to 3 ports that need to be opened for proper operation of the software. If you can't find the necessary information, call the software maker and ask what ports need to be opened for the software to work through a firewall.

Can I upgrade the gateway's firmware?

We provide two firmwares, one (*.bfw) is for boot code and the other (*.afw) is application code. Usually, you do not need to upgrade boot code in stead there is a specific description to upgrade boot code first for upgrading application code. You can refer *section 3.6 “Firmware Upgrade”* to use web-based GUI to upgrade firmware.

Can I set a fixed IP address on my PC?

Yes, you can configure your PC with fixed IP address. Specially, you need to setup a server explored to outside world. But be carefully not to put fixed IP addresses into the DHCP IP pool. It may cause trouble. Again, this fixed IP address must be located within the same subnet as gateway IP setting.

For example, in the Windows 98, Go to Start -> Control Panel -> Network -> TCP/IP -> Properties -> **IP address** Tab, enter IP address as 192.168.1.1 (where gateway IP address is 192.168.1.254, subnet mask is 255.255.255.0, DHCP server's IP address pool from 192.168.1.100 to 192.168.1.199) and subnet mask as 255.255.255.0.

Next, in the **DNS Configuration** tab, enter your ISP DNS addresses or gateway's IP address (192.168.1.254). The Wireless Broadband Firewall Gateway has DNS relay function. It will relay your DNS request to real DNS server and send the result back to sender.

Finally, in the **Gateway** tab, enter the gateway's IP address (192.168.1.254) in this field and click Add button.

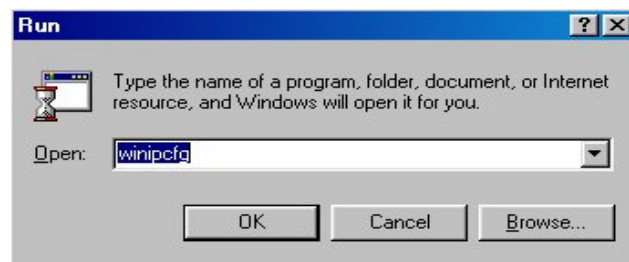
Is there a tool to check my PC's TCP/IP settings in MS Windows?

There are two programs we can use to display your current PC's TCP/IP settings.

WINIPCFG.EXE

For Win95, 98, ME, the WINIPCFG program is used to gather information about the TCP/IP connections that are active on your system. It cannot be used to dynamically adjust TCP/IP connections. You can also renew leases (if allowed by the network), and get the current IP address assignments through this program.

1. From Windows, go to **Start → Run**, enter **WINIPCFG**, and click **“OK”**.

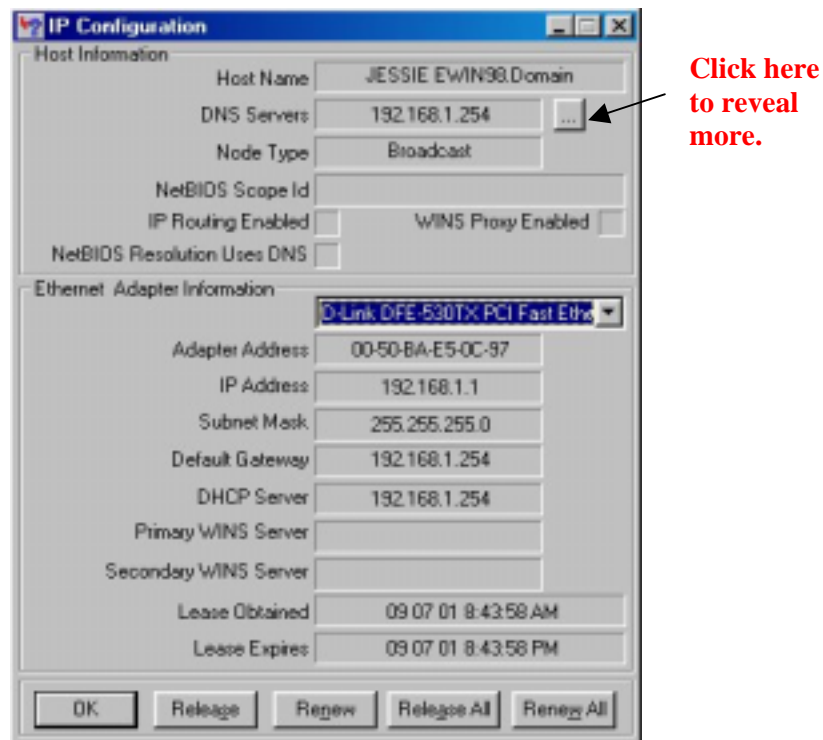


2. The following figure displays the adapter address and current TCP/IP address. Select the correct Ethernet adapter that is installed in this computer at the “Ethernet Adapter Information”.



Select the correct Ethernet adapter.

3. Click the **“More Info >>”** button to get detailed configuration information.



4. On the top, the “Host Name” and “DNS server” of the computer are configured to call when it is looking for a named resource. The default gateway is the server through which the client connects to the Internet. The DHCP Server identifies the network server (i.e. the router) that assigns IP addresses to computers on the network.

If the product is working properly, the following should be apparent from this screen:

- 1) The Client should have an IP address within the prescribed range.
- 2) The “DHCP” and “Default Gateway” should list the product’s local port address (the device’s IP address).
- 3) The DNS server IP addresses should match the DNS server IP addresses set in the device.

IPCONFIG.EXE

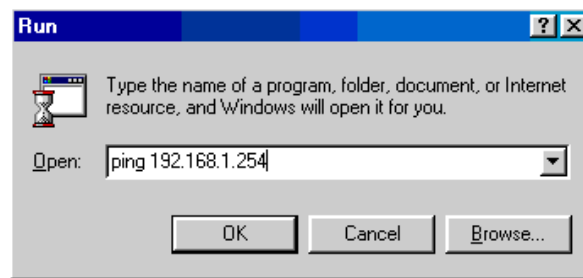
For WinNT, Win2000 and WinXP, go to **Start → Programs → Accessories → Command Prompt** to open the Command Prompt. Type in **IPCONFIG /ALL** and hit “Enter” to see the adapter’s information. Type in **IPCONFIG /RELEASE** to release all adapters’ IP address and **IPCONFIG /RENEW** to renew IP addresses. For a list of the **IPCONFIG** commands, type in **IPCONFIG /?**.

How can I test the whole path (PC Gateway outside world) to make sure it works fine?

There is a simple tool named PING. Send this command to desired IP station and should be immediately echoed back. Therefore it acts as a loopback. If you can receive the echo back successfully, the path is OK.

For example, you can enter PING command in MS-DOS prompt (or after choosing START_ RUN from the Start menu) as below in sequence.

✦ PC to Router (e.g. ping 192.168.1.254)



If there is no reply from gateway, please verify the PC, cables, HUB/Switch and gateway.

✦ PC to external station with IP address (e.g. ping 168.95.192.1)

If there is no reply from external station, please verify the gateway, cables, DSL/Cable modem, and connection protocols.

✦ PC to external station with domain name (e.g. ping www.yahoo.com)

If there is no reply from external station, please verify the DNS setting in PC or gateway.

How can I check the active IP settings for my WAN port?

You may use the Web-based GUI to check the WAN port status, **Status -> System Log**, and then you will see whole process inside the Wireless Broadband Firewall Gateway including the WAN port IP address and related information.

Where can I find the WAN port's MAC address?

When you need this WAN port MAC address, you can refer the MAC label in the enclosure. But the easiest way is to use Web-based GUI to check it. Please enter **Status -> Device Information** or **WAN -> ISP -> Obtain an IP address automatically**, then you will see the MAC address for WAN port. Usually, some cable operators need this information for registration. This function is available in Application Firmware Version 1.17 and later version.

How can I explore a local server to be visible to outside users?

When being a natural Internet firewall (NAT + Advanced Firewall), the Wireless Broadband Firewall Gateway protects your network from being accessed by outside users. There is only one IP address visible to outside users who are not able to access the specific server in your LAN. When you need to allow outside users to access local servers, e.g. Web server, FTP server, E-mail server or News server. You can set up a local server with specific port number that stands for the service, e.g. Web (80), FTP (21), Telnet (23), SMTP (25), POP3 (110), DNS (53), ECHO (7), NNTP (119). Details are described in **section 3.4.6 "Virtual Server"**. When an incoming access request to the router for specified port is received, it will be forwarded to the corresponding internal server.

For example, if you set the Service Port number 80 (Web) to be mapped to the IP Address 192.168.1.2, then all incoming requests with router's public IP address from outside users will be forwarded to the local server with IP address of 192.168.1.2.

What is DMZ host?

Regarding the DMZ Host (private IP address), it is a local computer exposed to the Internet. Therefore, an incoming packet will be checked by Firewall and NAT algorithms in the Wireless Broadband Firewall Gateway, and then passed to the DMZ host when packet is not sent by hacker and not limited by virtual server list. Besides, there are some IP protocols that do not have port number information. There is no way to use Virtual Server setting to forward incoming packet. Therefore, DMZ host is the easy to forward this kind of packets. If you enable and set virtual server and DMZ host, the precedence is Virtual Server and then DMZ. For example, the incoming packet will be checked with Firewall rules, Virtual Server rules and then DMZ host.

How to configure my MacOS to surf Internet through the Wireless Broadband Firewall Gateway?

Please make sure the MacOS open transport networking protocols is installed.

We will suggest that the Wireless Broadband Firewall Gateway has DHCP server enabled and MacOS gets an IP address automatically because MacOS will get the other information at that same time, such as DNS IP address, subnet mask and Gateway IP address.

Click the Apple Manual -> Control Panel -> TCP/IP, and then

- + Select **Connect via** : Ethernet
- + Select **Configure** : Using DHCP server

If you select **Configure** as Manually, then you have to enter

- + **IP Address** : 192.168.1.1
- + **Subnet mask** : 255.255.255.0
- + **Router address**: 192.168.1.254
- + **Name server addr**: ISP's DNS IP addr or 192.168.1.254

Please refer above *Question 5 "Can I set a fixed IP address on my PC?"* for configuring manually.

How can I do if I forget the password for accessing Gateway?

If you ever forget the password to log in, you should contact the dealer where you bought this product.

How can I do if there is already a DHCP server in LAN?

If there are two DHCP servers existing in the same network, it may cause conflict and generate trouble. In this situation, we suggest to disable DHCP server in gateway and configure your PC manually as described in *Question 5 "Can I set a fixed IP address on my PC?"*.

How many PCs can share this single Wireless Broadband Firewall Gateway simultaneously?

Basically, it is depended on your subnet mask setting in gateway. For example, if you set 255.255.255.0 for subnet mask, gateway will allow up to 253 users to share the outgoing bandwidth. This is also the default setting in gateway.

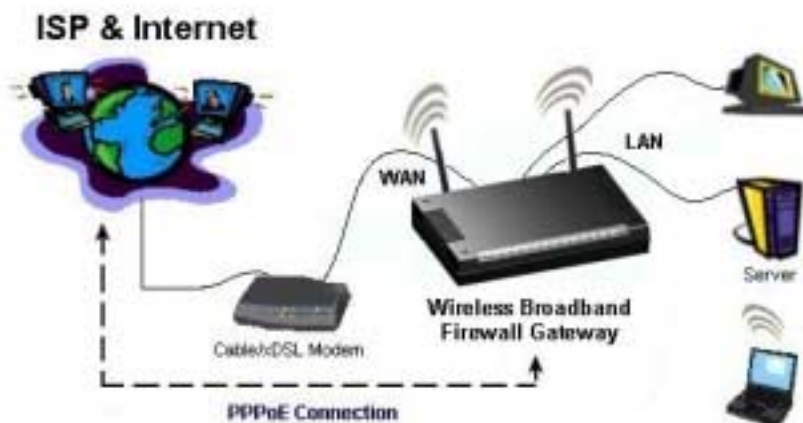
Which connection method should I select in WAN-ISP setting window?

The wireless broadband firewall gateway supports four kinds of access method to establish a connection as below.

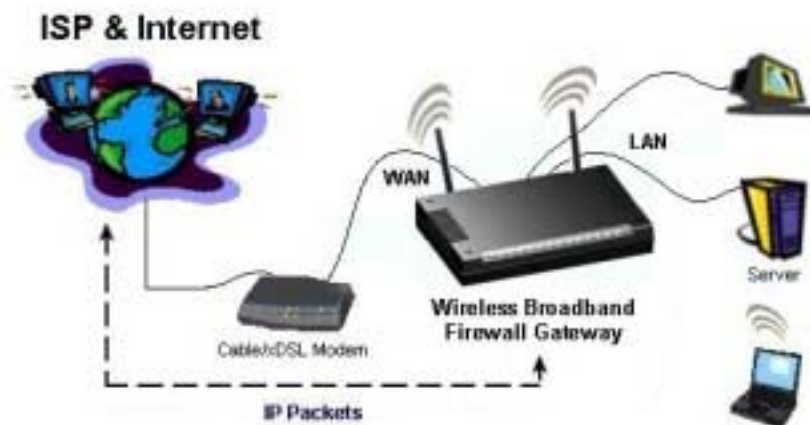
PPPoE	Username, Password, Service Name, Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed)
Fixed IP	IP address, Subnet mask, Gateway address, Domain Name System (DNS) IP address (it is fixed IP address)
Obtain an IP Address Automatically	Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed)
PPTP Client	Username, password, PPTP server's IP address and Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed)

The connection diagram is shown as below. Please check with your ISP to get more information and refer *section 3.4.2 “WAN”* to configure the wireless broadband firewall gateway and enjoy surfing the Internet.

PPPoE connection diagram



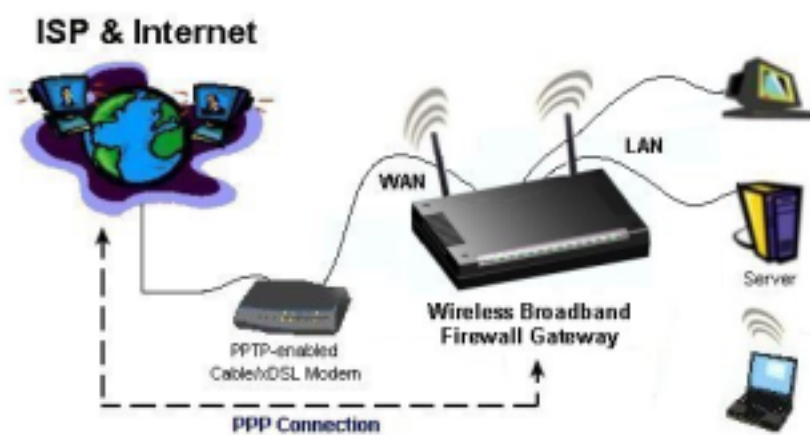
Fixed IP connection diagram



Obtain an IP address automatically connection diagram



PPTP Client connection diagram



APPENDIX A

Specification

Protocols	IP, NAT, ARP, ICMP, DHCP, PPPoE, PPTP client
LAN Port	RJ-45, four 10/100Base-T N-way, auto-sensing Ethernet ports, automatic switching between MDI and MDIX.
WAN Port	RJ-45, one 10Base-T N-way Ethernet port to external DSL/Cable Modem, or other network equipment.
WLAN Port	Comply to wireless standard, 802.11b and WiFi certified module. Support 11Mbps, 5.5Mbps, 2Mbps, 1Mbps data rate and auto-fallback support. Wired Equivalent Privacy (WEP) data encryption
LED Indicators	PPP/SYS, WAN, LAN x 4 (10/100Mbps), Power, WLAN
Input Power	5V DC @1.2A
Max. Power Consumption	6 watt
Agency and Regulatory	FCC part 15 Class B, VCCI, CE
Physical Dimension	210 x 148 x 30 mm ³ (L x W x H) 210 x 185 x 125 mm ³ with antennas extended
Weight	500g
Operating Temperature	0 to 45
Storage Temperature	-10 to 70
Operating Humidity	5%-95% non-condensing

APPENDIX B

Internet Applications

There are many popular Internet applications, we list some of them here to configure the port numbers in NAT and virtual server functions to enable the services, please refer below for details.

Application	Settings for Outgoing Connection	Setting for Incoming connection
ICQ98a,99b	None	None
Netmeeting 2.1 & 3.0	None	1503 (tcp) 1720 (tcp)
AOE	2300-2400 (tcp) 2300-2400 (udp) 47624 (tcp)	2300-2400 (tcp) 2300-2400 (udp) 47624 (tcp)
VDO Live	None	None
mIRC	None	None
Cu-Seeme	7648 (tcp) 7648 (udp) 24032 (udp)	7648 (tcp) 7648 (udp) 24032 (udp)
PCAnywhere	5632 (udp) 22 (udp) 5631 (tcp) 65301 (tcp)	5632 (udp) 22 (udp) 5631 (tcp) 65301 (tcp)