BIPAC 6500

Broadband VPN Firewall Router

with 4-port 10/100M Switch

User Manual

Table of Content

Chapter 1
Introduction

1.1 An Overview of BIPAC 6500

BIPAC 6500 functions as an IEEE 802.3 Ethernet-based router. It provides four 10/100Mbps Dual Speed Ethernet ports for connection to a home or small office network and one 10/100Mbps 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 N-Way 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 of the Cable/xDSL modem.

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; BIPAC 6500 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. BIPAC 6500
2. One CD containing the on-line manual and application program
3. One Quick Start Guide
4. One CAT5 cable
5. One power adapter

1.3 BIPAC 6500 Features

BIPAC 6500 provides the following features:

Network Protocols and Features

• PPPoE, PPTP and DHCP client connection to ISP

• NAT, static routing and RIP-1/2

• Supports multiple Application Level Gateway (ALG) algorithms for multimedia applications, such as ICQ, NetMeeting, MS Messenger, QUAKE, Real Player, etc.

• Universal Plug and Play compliant (UPnP)

• Dynamic Domain Name System (DDNS)

• Virtual Server and DMZ

• SNTP and DNS relay

Management

• Easy Web-based GUI for remote and local management

• Firmware upgraded and configuration data upload and download via Web-based GUI

• Support DHCP server to manage local IP network easily

• Real-time attack alert and system log

Firewall

• Built-in NAT firewall

• Prevent DoS attacks including IP Spoofing, Land Attack, Smurf Attack, Ping of Death, TCP SYN Flooding, etc.

• Packet filtering – port, source IP address, destination IP address, MAC address

• URL filtering – string or domain name detection in URL string

Virtual Private Network (VPN)

• Embedded IPSec & PPTP client

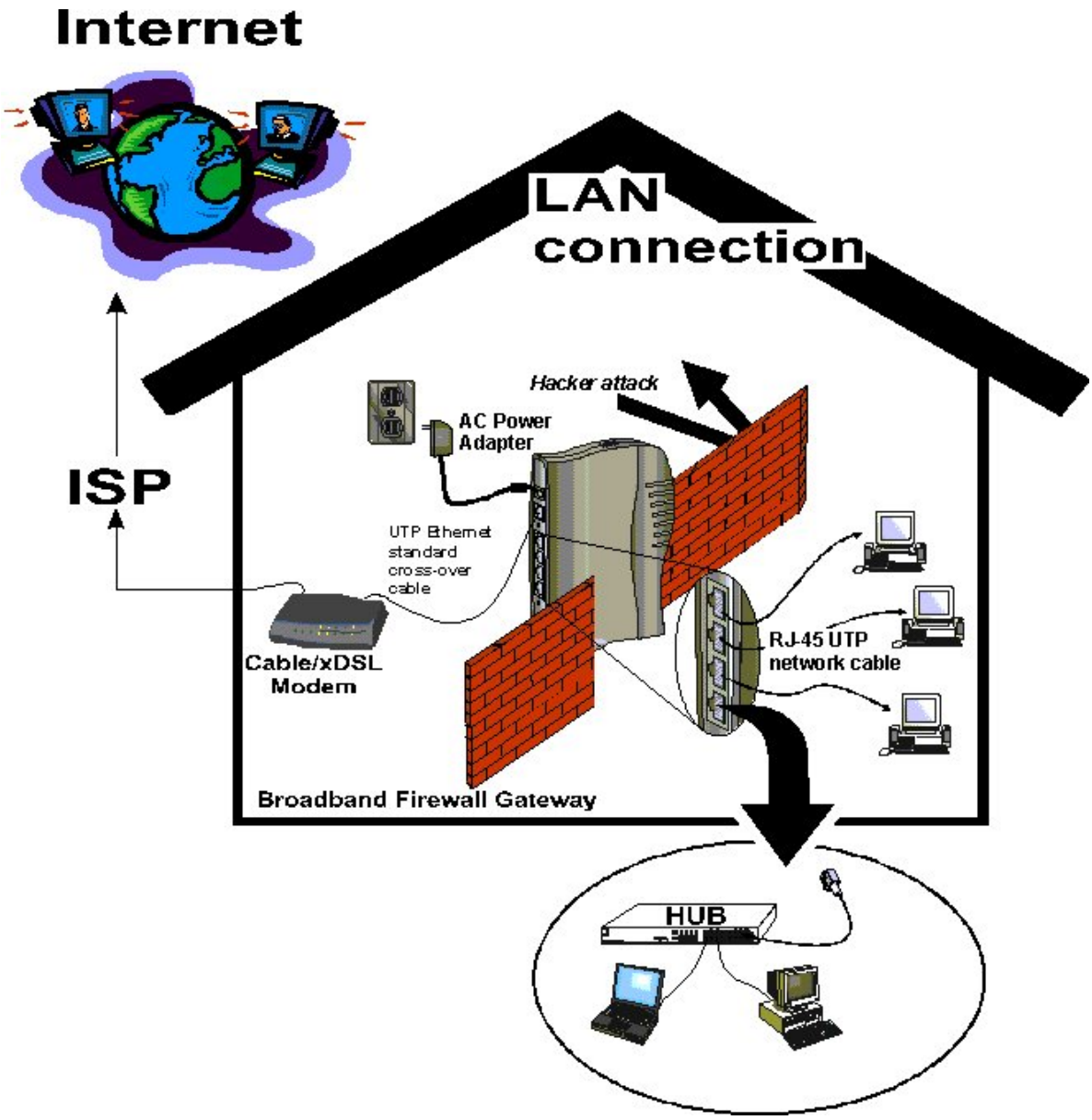
• Embedded L2TP and L2TP over IPSec (future release)

• IKE key management

• DES and 3DES encryption for IPSec

• L2TP/PPTP/IPSec pass through

1.4 BIPAC 6500 Application



Be noted, BIPAC 6500 provides a 10/100Mbps 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 BIPAC 6500

2.1 Cautions for Using BIPAC 6500

Do not place BIPAC 6500 under high humidity and high temperature.

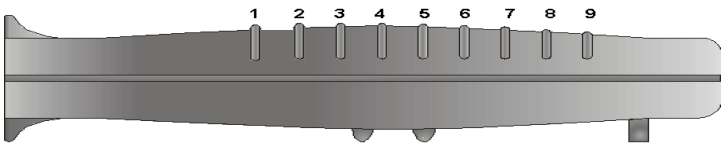
Do not use the same power source for BIPAC 6500 with other equipment.

Do not open or repair the case yourself. If BIPAC 6500 is too hot, turn off the power immediately and have a qualified serviceman repair it.

Place BIPAC 6500 on the stable surface.

Only use the power adapter that comes with the package.

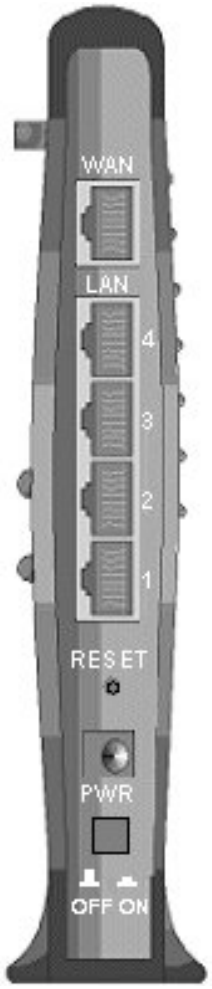
2.2 The Front LEDs



LED		Meaning
1	**Power**	Lit green when power ON.
2	**SYS**	Lit when system is ready.
4	**LAN 1**	Lit green when connected at 100 Mbps. Lit orange when connected at 10 Mbps. Flashes when sending/receiving data.
5	**LAN 2**	
6	**LAN 3**	
7	**LAN 4**	
8	**WAN**	Lit green when connected at 100 Mbps. Lit orange when connected at 10 Mbps. Flashes when sending/receiving data.
9	**PPP/Mail**	Lit green when PPPoE or PPTP connection is established. Lit orange when there is email in the email account Flashes orange when upgrading firmware.

2.3 The Rear Ports

WAN (RJ-45 connector)	Connect an UTP 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.
LAN (RJ-45 connector)	Connect an UTP Ethernet cable to these four ports when connecting to a LAN of 10Mbps or 100Mbps such as an office or home network.
RESET	After the device is powered on, press it to reset the device or restore to factory default settings. **0-3** seconds: reset the device **3-6** seconds: no action **6 seconds or above**: restore to factory default settings (this is used when you can not login to BIPAC 6500, e.g. forgot the password)
PWR (jack)	Connect the supplied power adapter to this jack.
Power Switch	A Power ON/OFF switch



2.4 Cabling

Please refer to **section 1.4** ***"BIPAC 6500 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. If they are not, verify that you are using the proper cables.

Chapter 3
Configuration

BIPAC 6500 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

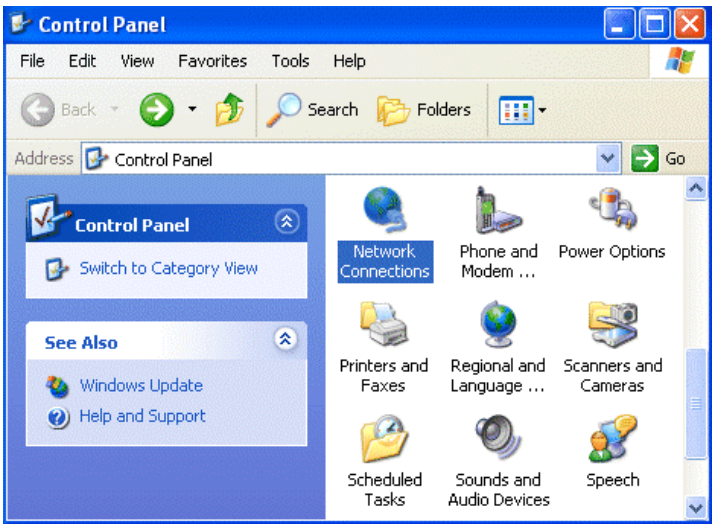
This section describes the configuration required by LAN-attached PCs that communicate with BIPAC 6500, either to configure the device, or for network access. These PCs must have an Ethernet interface installed properly, be connected to BIPAC 6500 either directly or through an external repeater hub, 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 BIPAC 6500. The default IP address of router 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 BIPAC 6500.

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.

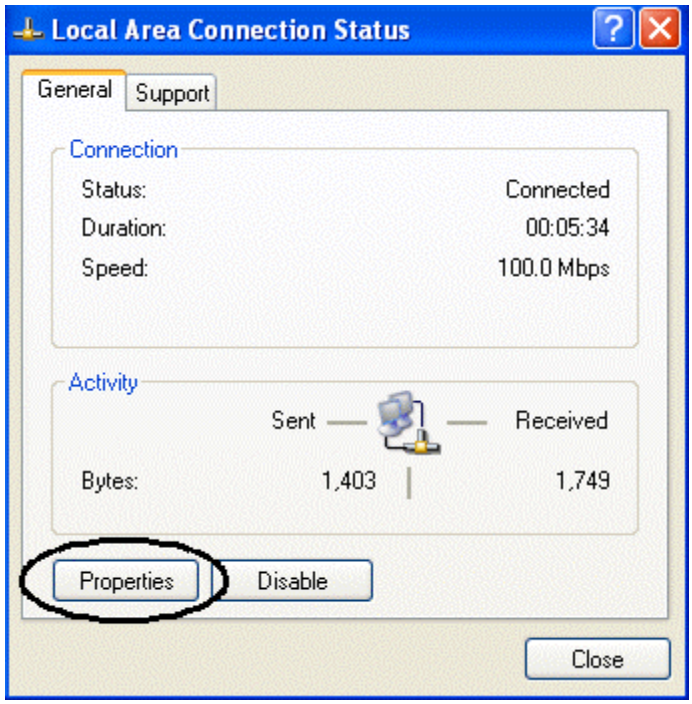
Any TCP/IP capable workstation can be used to communicate with or through BIPAC 6500*. To configure other types of workstations, please consult the manufacturer's documentation.*

Configuring PC in Windows XP

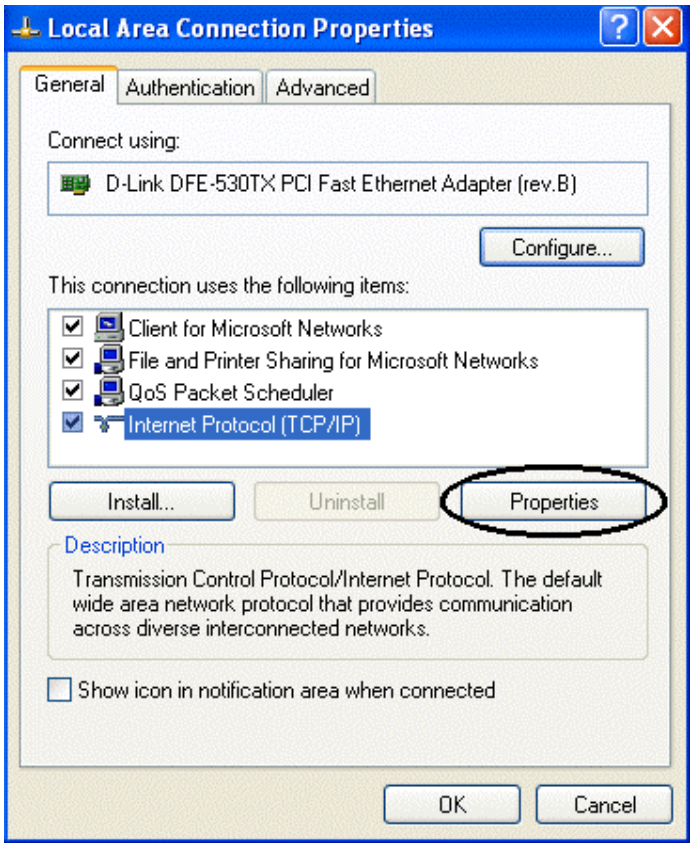
1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections.**
2. Double-click **Local Area Connection**.



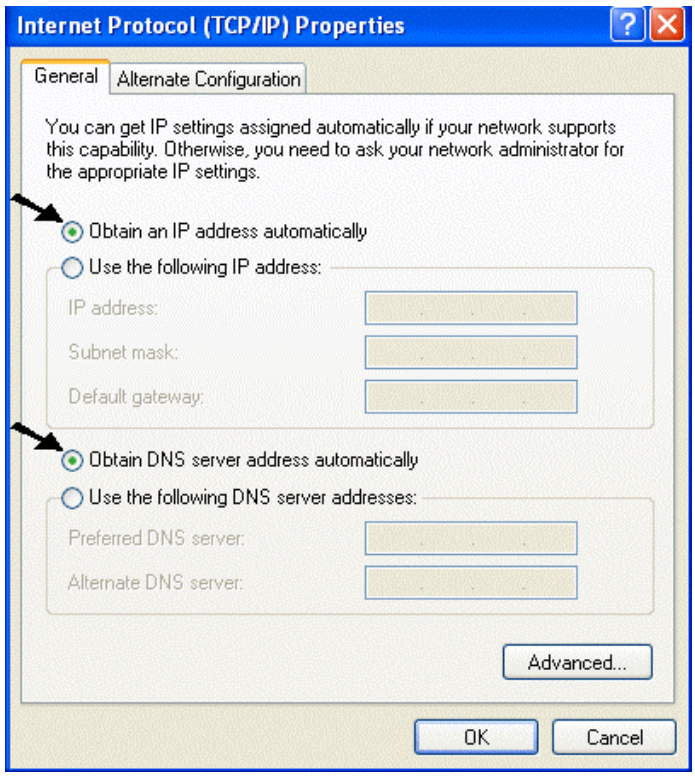
3. In the **Local Area Connection Status** window, click **Properties**.



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



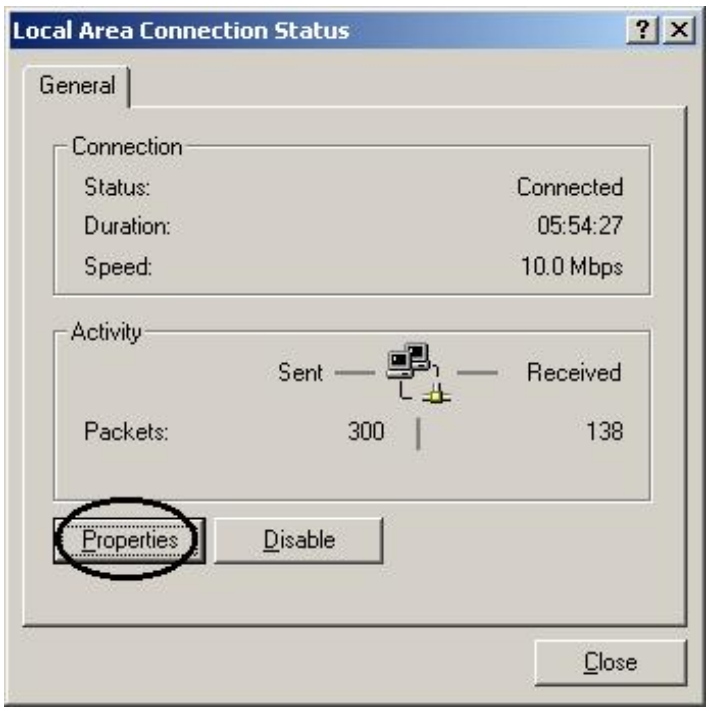
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.



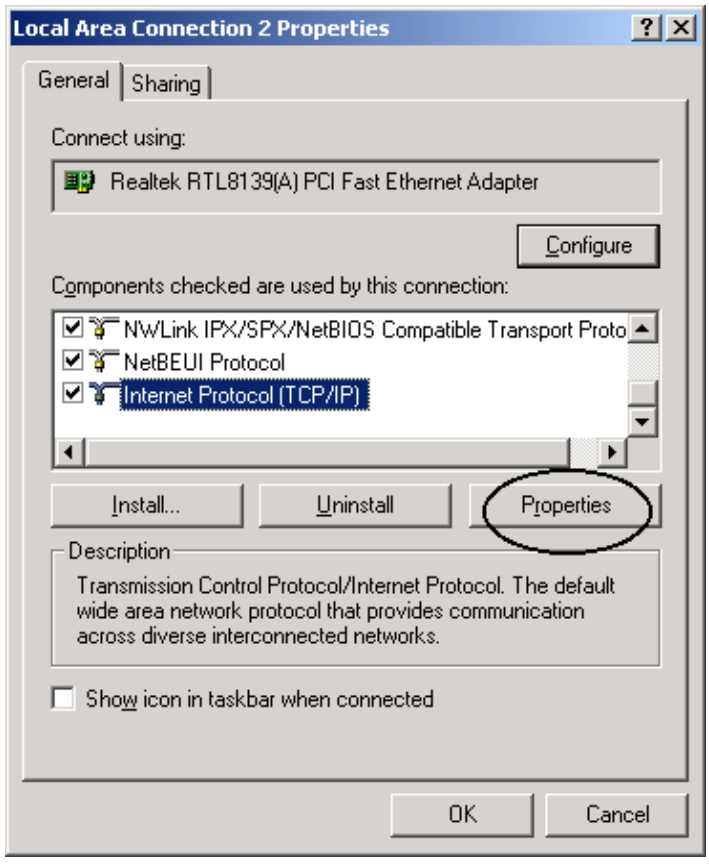
Configuring PC in Windows 2000

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**.

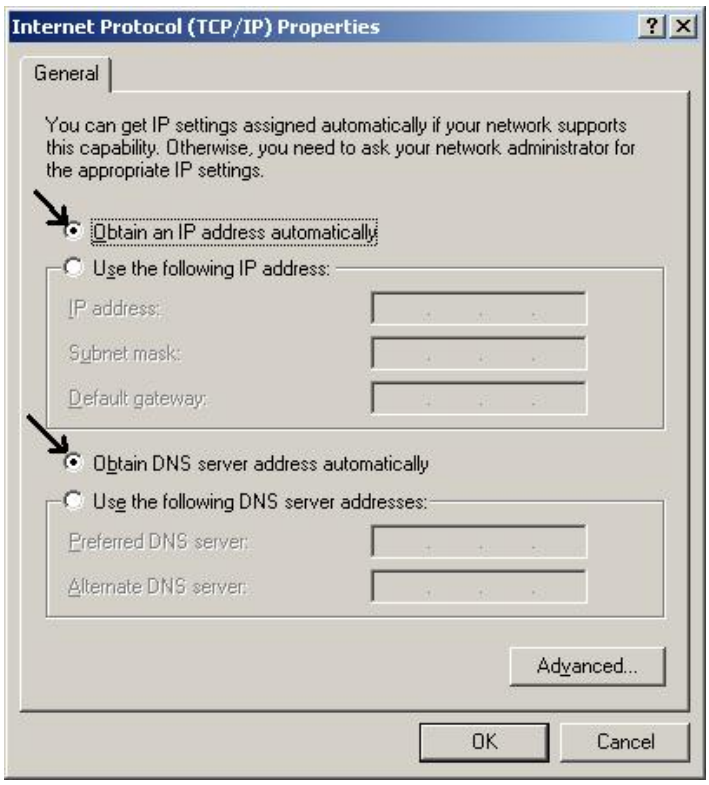
3. In the **Local Area Connection Status** window, click **Properties**.



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

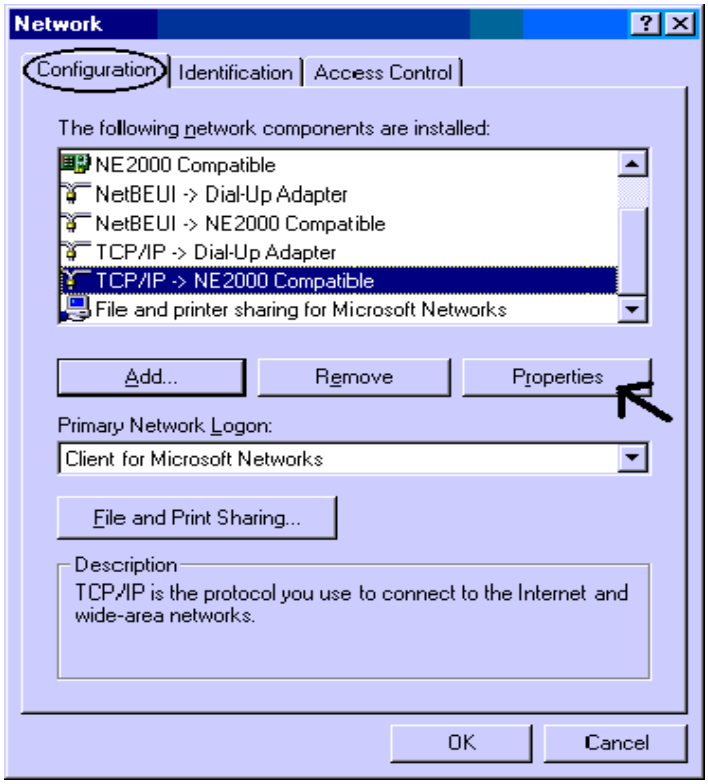


5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.

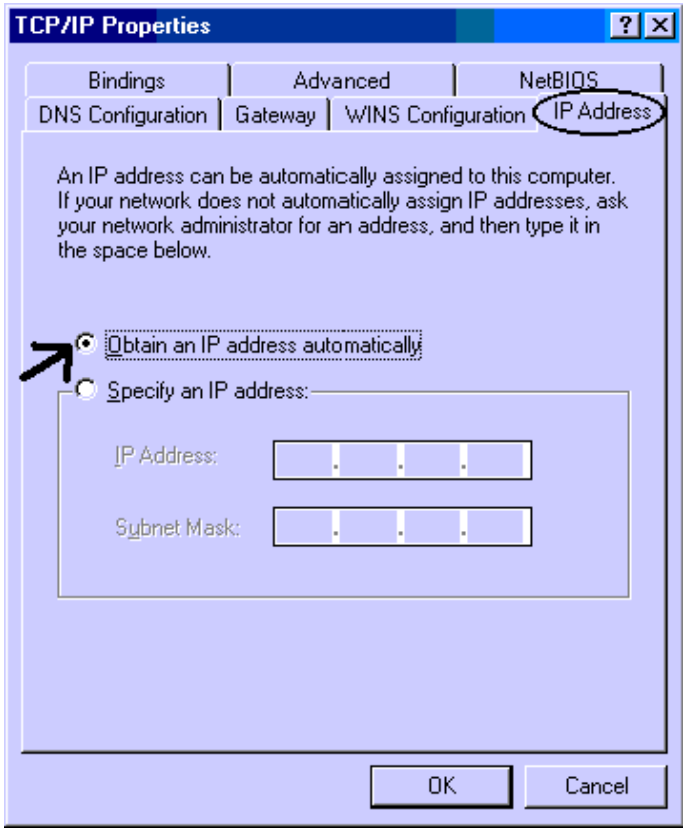


Configuring PC in Windows 95/98/ME

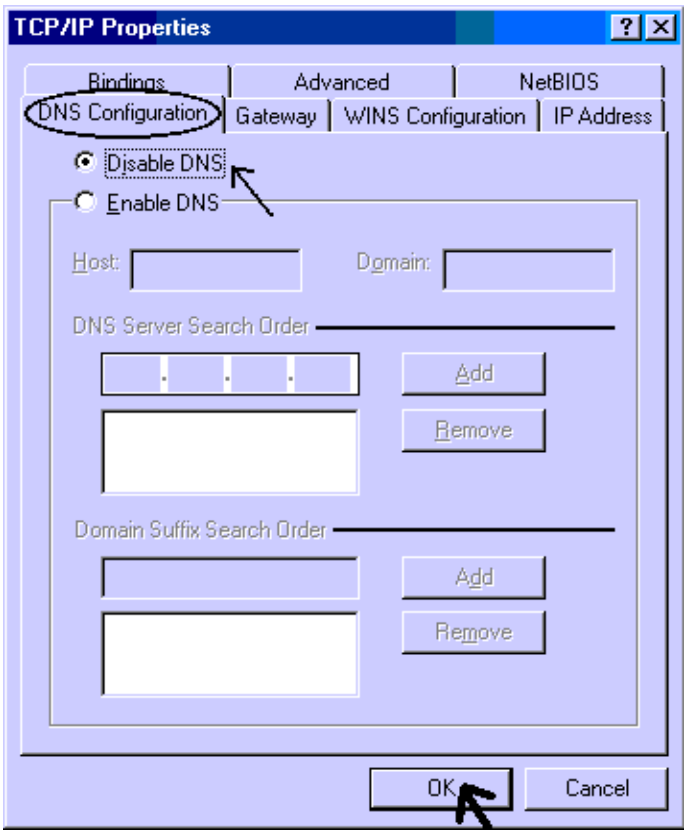
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.
2. Select **TCP / IP -> NE2000 Compatible**, or the name of your Network Interface Card (NIC) in your PC.
3. Click **Properties**.



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

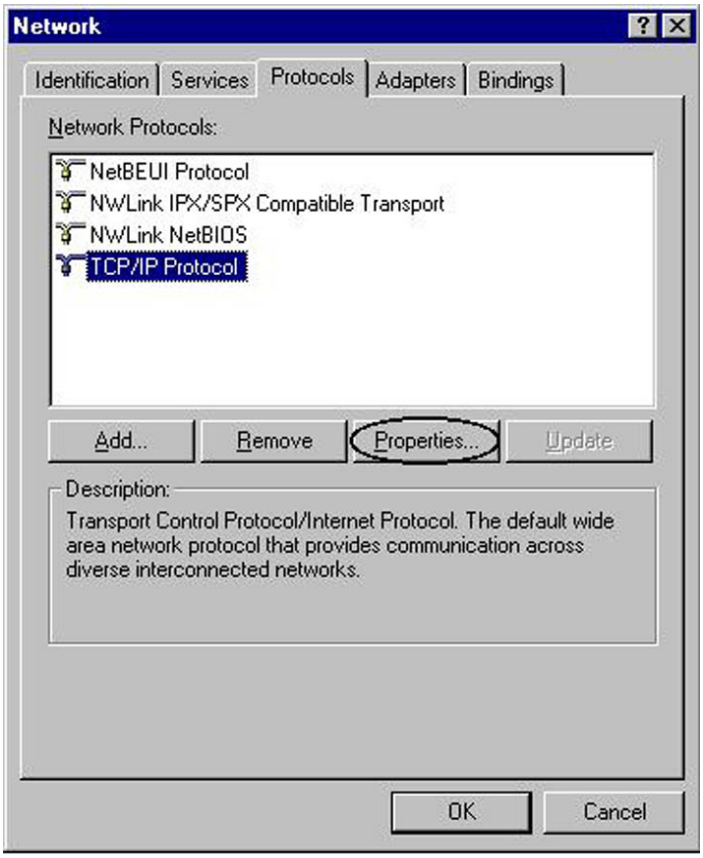


5. Then select the **DNS Configuration** tab.
6. Select the **Disable DNS** radio button and click **OK** to finish the configuration.

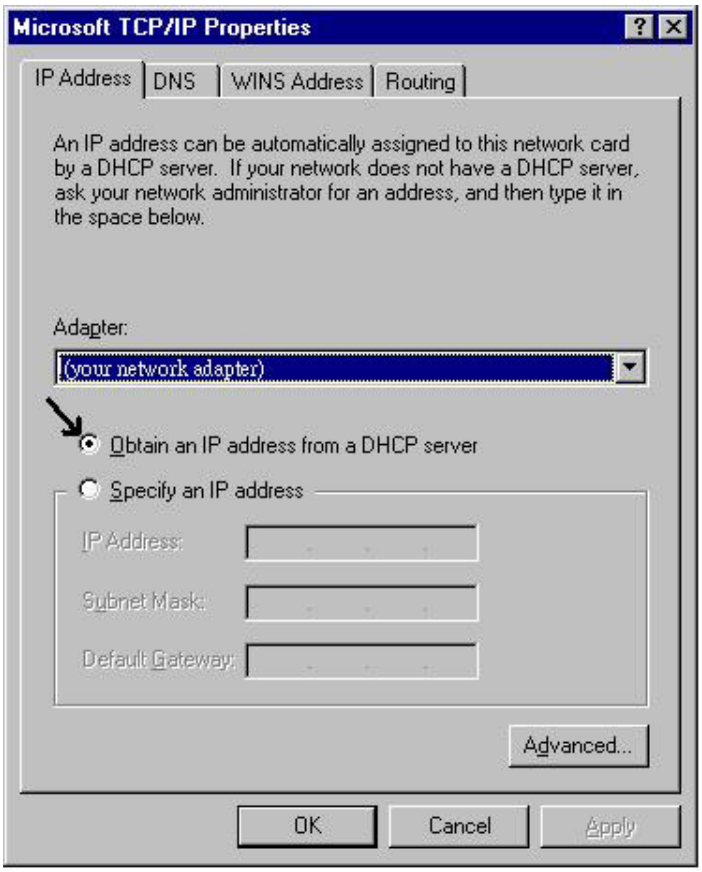


Configuring PC in Windows NT4.0

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 BIPAC 6500, 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 router 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. BIPAC 6500 maintains the password only. It means BIPAC 6500 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

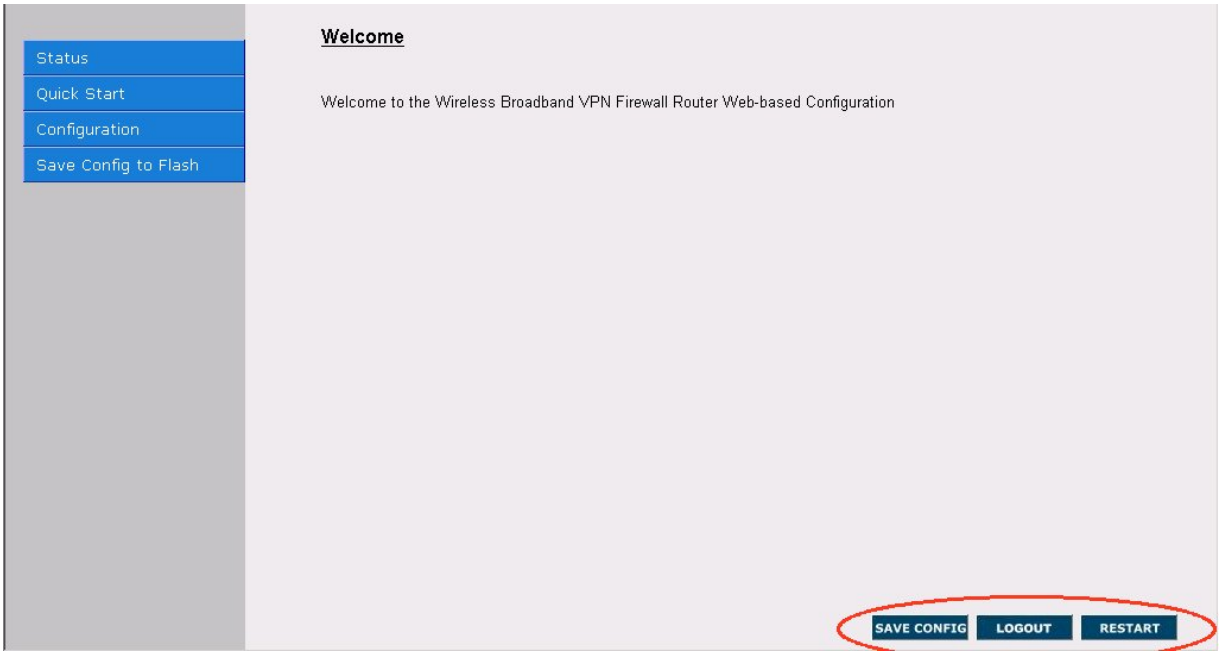
Open the web browser, enter the local port IP address of this router, which default at **192.168.1.254**, and click "**Go**" to get the login page.

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

At the configuration homepage, the left navigation pane where bookmarks are provided links you directly to the desired setup page, including :

- **Quick Start**
- **Configuration** (LAN, WAN, Firewall, System, VPN, Virtual Server, Advanced and Help)
- **Status** (System Status, Device Info, System Logs, Security Logs, ARP Cache Table, DHCP Table, Routing Table and VPN Connect Status)

3.4.1 Main Navigation Pane



Save Config : After configuring this network router, you have to save all of the configuration parameters to FLASH.

Restart : 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 **Restart** button. Each time you reboot your Router, the following figure will appear. Please wait seconds for auto-reconnection.

Logout : Logout the device when you finish configuring the router.

3.4.2 Quick Start

If you use this device to access the Internet through the ISP, this web page is enough for you to configure this router and access the Internet without a problem. Please check Chapter 3.3 (*Information from the ISP)*, then enter the proper values into this web page, click the **Apply** button and then click the **Save Config** button to save all of the configuration parameters to FLASH. After the router reboot, you may check the Status web page to check whether the router is connected to the ISP or not. In most cases, you can access the Internet immediately. If not, please refer to the sections below for more information.

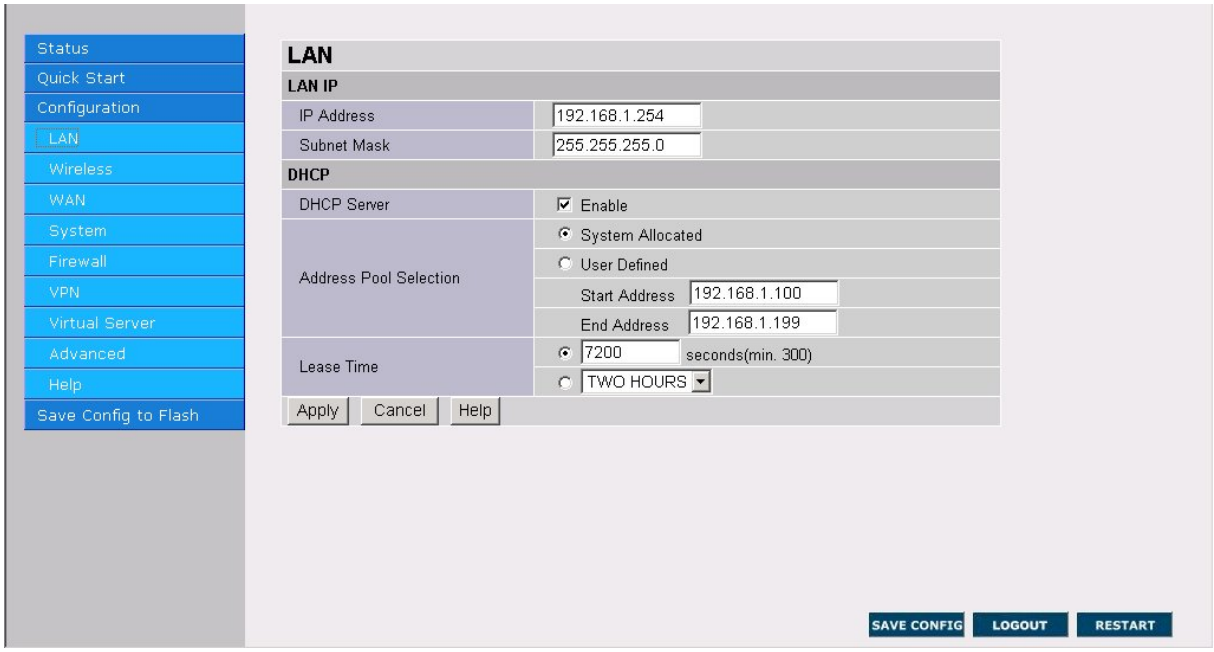
3.4.3 Configuration

When you click this item, you get following sub-items to configure BIPAC 6500.

LAN, WAN, Firewall, System, VPN, Virtual Server, Advanced and Help

3.4.3.1 LAN

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



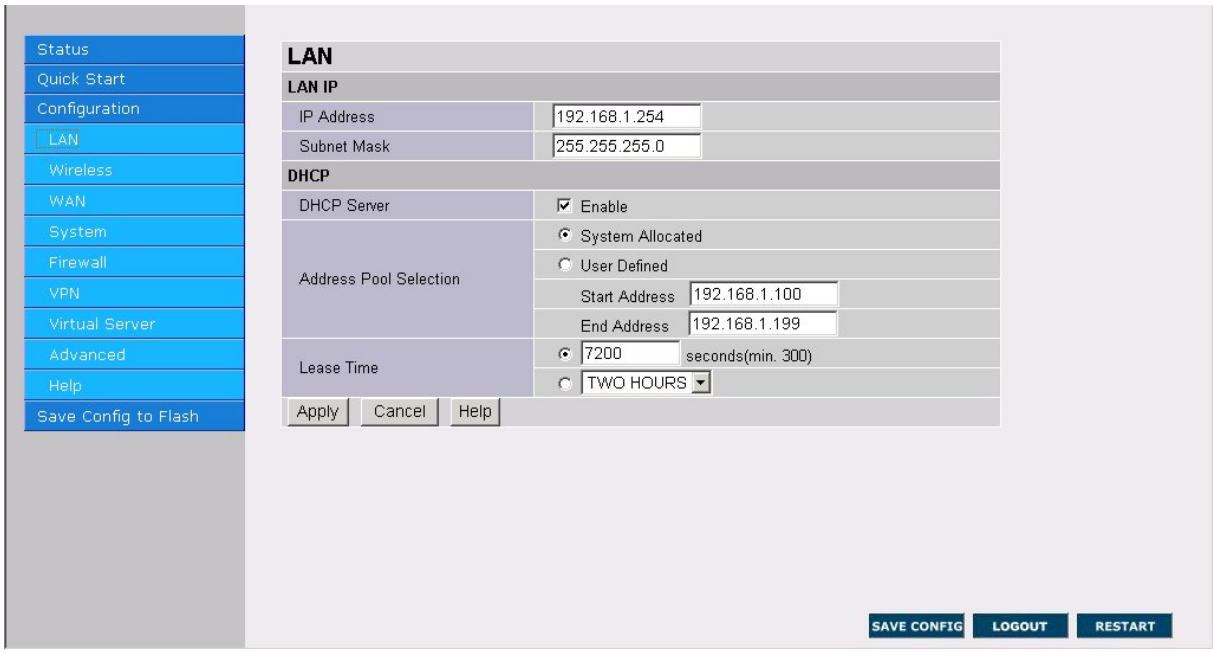
IP Address: Default at 192.168.1.254.

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 router.

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



Check **DHCP Server** to enable the router to distribute IP Addresses, subnet mask and DNS setting to computers. Hence, the following fields will be activated.

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.

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.

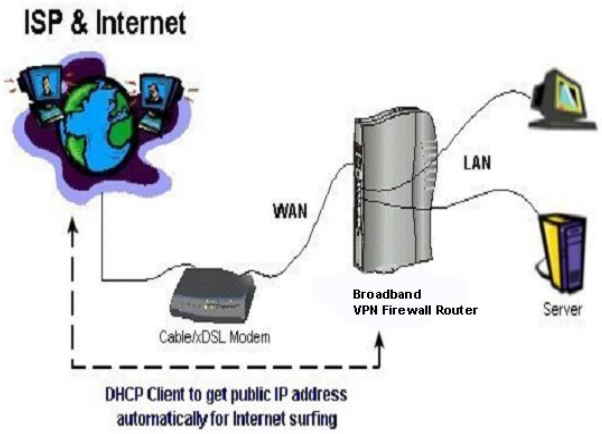
If you disable **DHCP Server**, remember to specify a static IP address, subnet Mask, and DNS setting for each of your local computers. Be careful not to assign the same IP address to different computers.

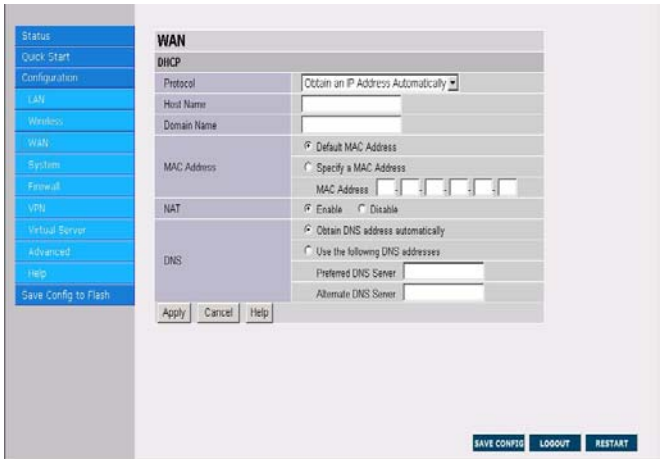
3.4.3.2 WAN

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

There are four ways — 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 router dynamically when logon.

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

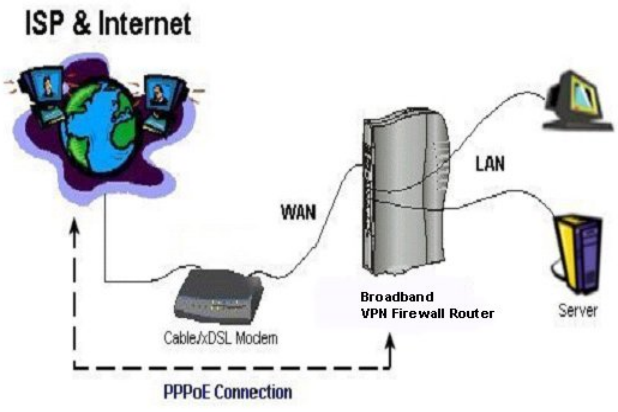
Domain Name: Enter the domain name provided by your ISP. The maximum input is **20** alphanumeric characters (case sensitive).

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**.

Username: 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.

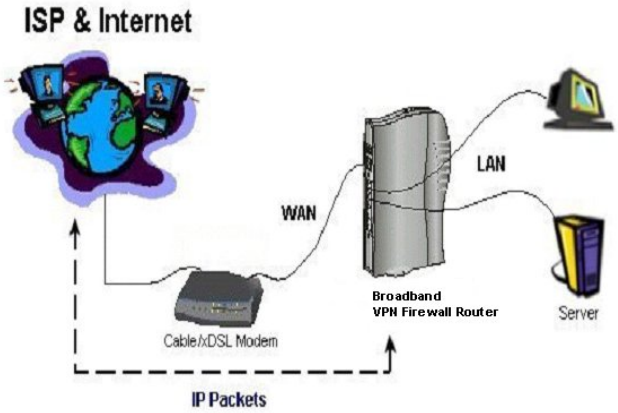
NAT: The NAT feature allows multiple users to access Internet through a single IP account, sharing the single IP address. If users in the LAN site have public IP addresses and can access Internet directly, the NAT function can be disabled.

⊙ **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 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.

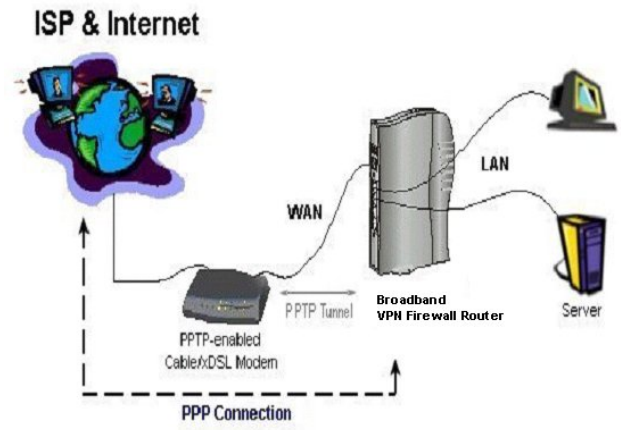
IP Address: Enter the information provided by your ISP.

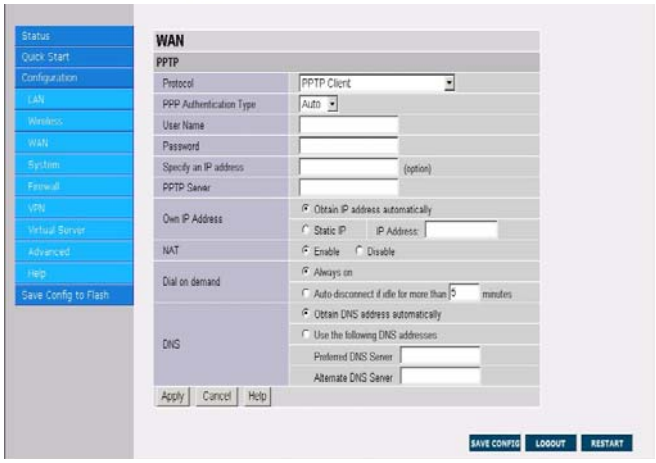
Subnet Mask: Enter the information provided by your ISP.

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. Maximum input is **128** alphanumeric characters (case sensitive).

Password: Enter the password. Maximum input is **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 interface to be PPTP client, you will not see the VPN selection in the left pane after you reboot the router. 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 Server

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 protocol.

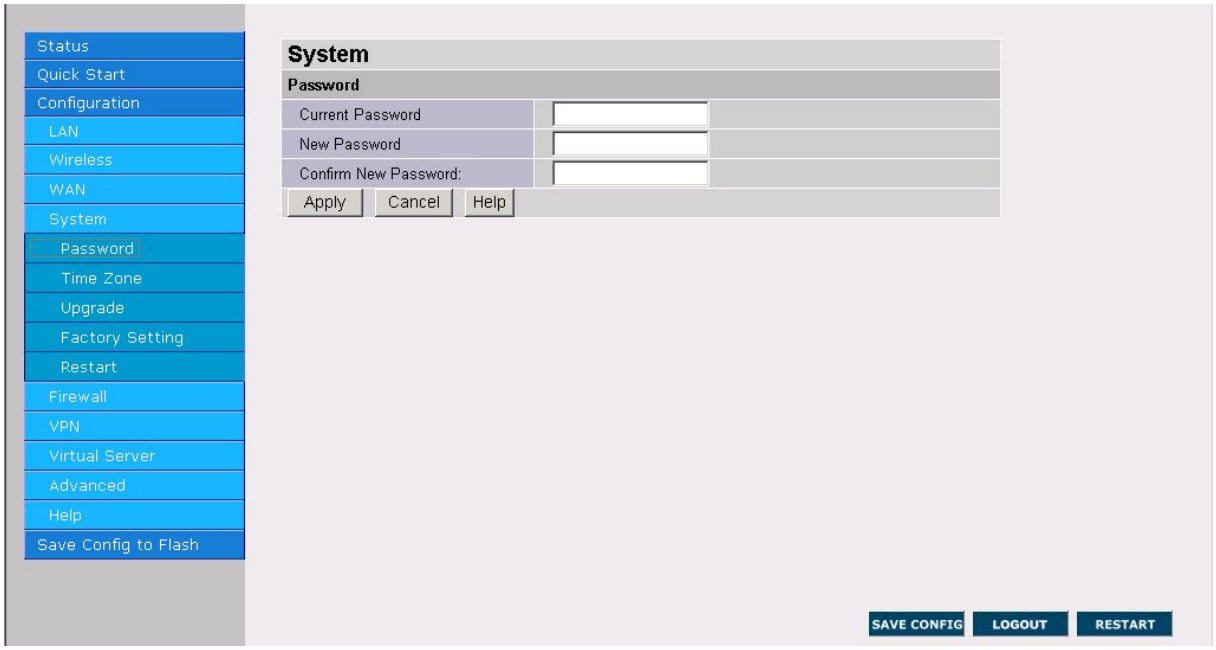
Or your ISP may provide you with an IP address of DNS. If this is the case, you must enter the DNS IP address. Moreover, if you set Fixed IP as your ISP protocol, you can only enter the DNS IP Address instead of obtaining the address automatically.

3.4.3.3 System

There are six items under the **System** section: Password, Time Zone, Upgrade, Factory Setting, Reboot and Logout.

3.4.3.3.1 Password

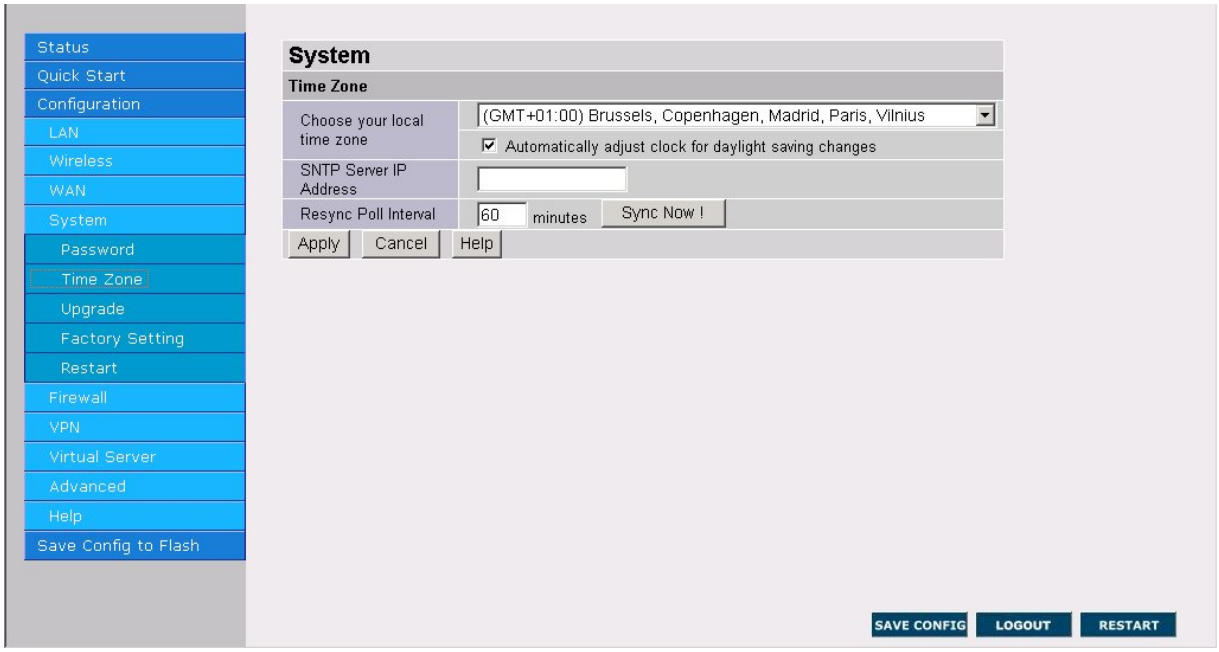
In factory setting, there is no password protection when user accesses BIPAC 6500. It is recommended that you change the default password <BLANK> to ensure that someone cannot adjust your settings without your permission. <BLANK> means there is no password. Every time you change your password, please 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.

3.4.3.3.2 Time Zone

BIPAC 6500 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.

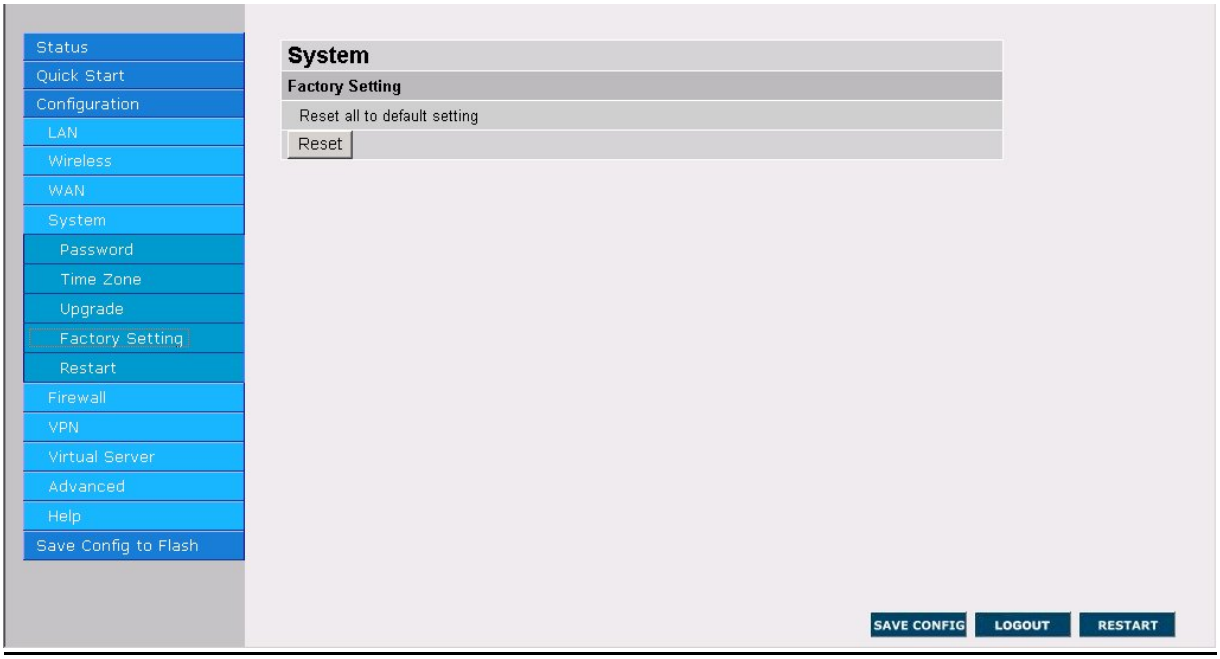
SNTP Server IP Address: Specify the IP address if you want to use your familiar SNTP server.

3.4.3.3.3 Upgrade

To upgrade the firmware of BIPAC 6500, 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, BIPAC 6500 will reset automatically to make the new firmware work.

3.4.3.3.4 Factory Setting

If for any reason, you have to reset this router 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''*.**

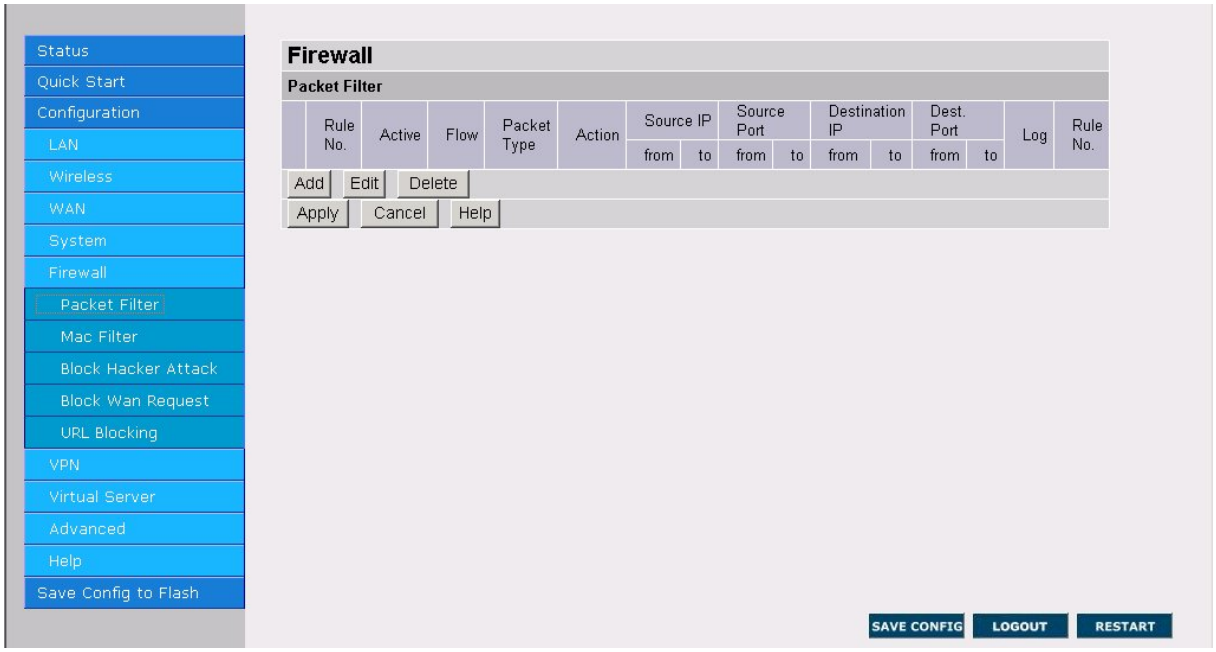


3.4.3.4 Firewall

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.

3.4.3.4.1 Packet Filter

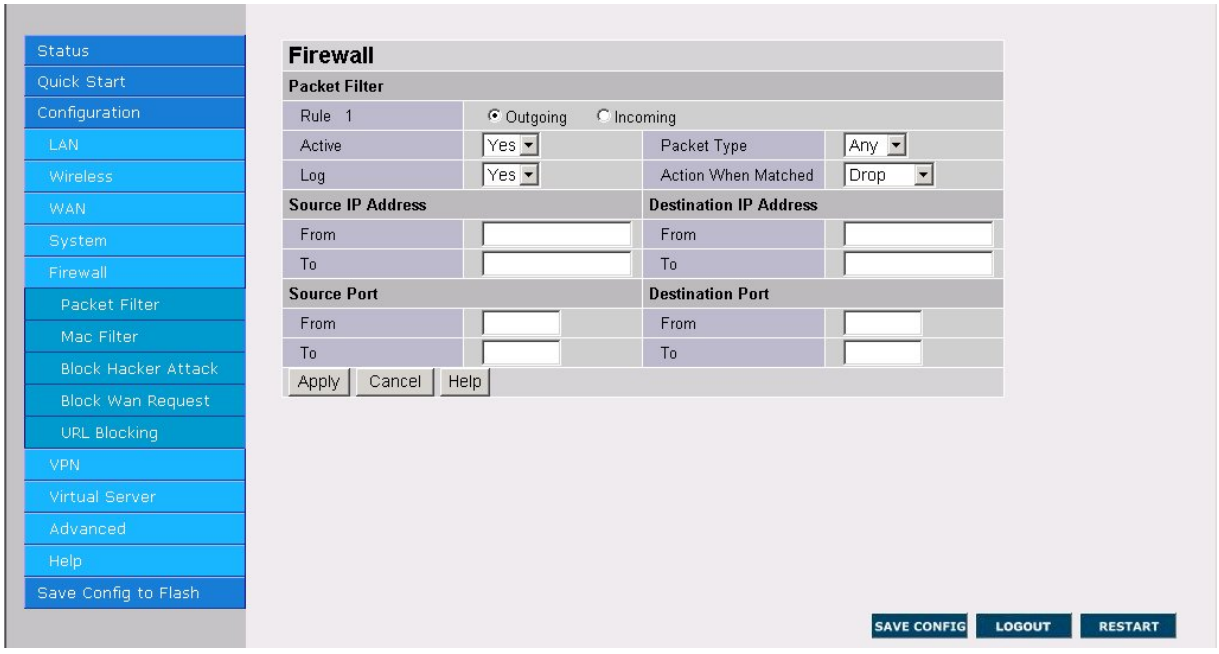
Packet filtering function enables you to configure your router to block specified internal/external user (**IP address**) from Internet access, or you can disable specific service request (**Port number**) to /from Internet. You must check the **"Enable"** radio button to make the following figure appear 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, stating 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.



⊙ **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 filer 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).

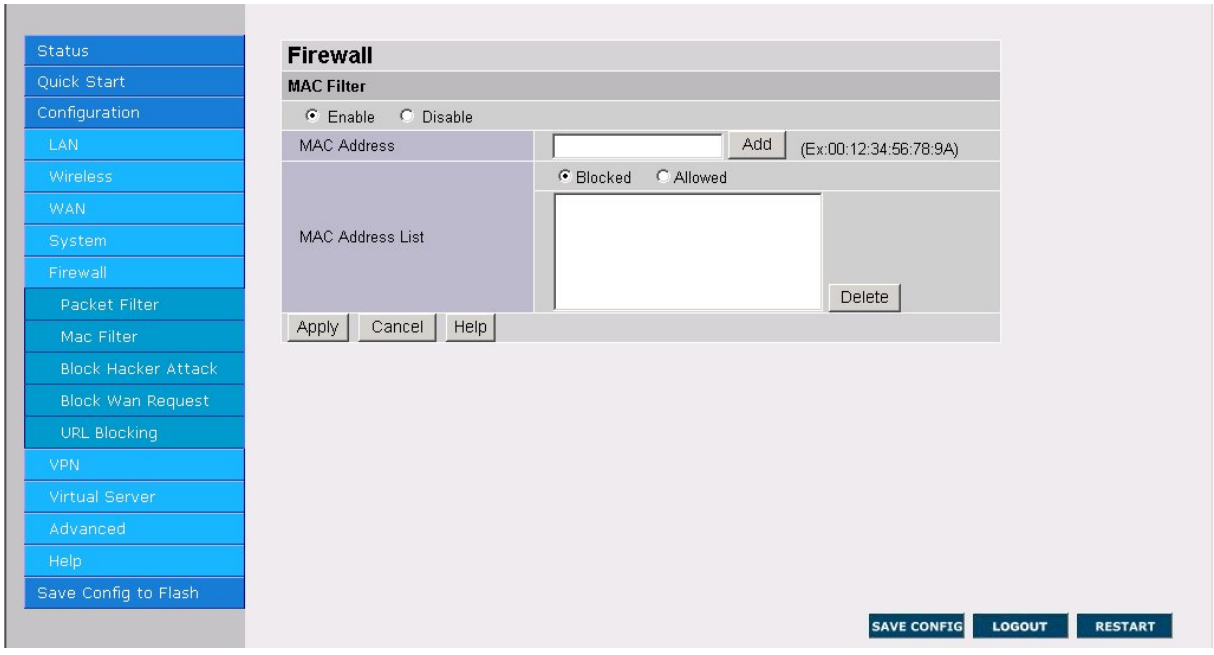
Destination IP Address: Enter the incoming or outgoing packet's destination IP address(es).

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.

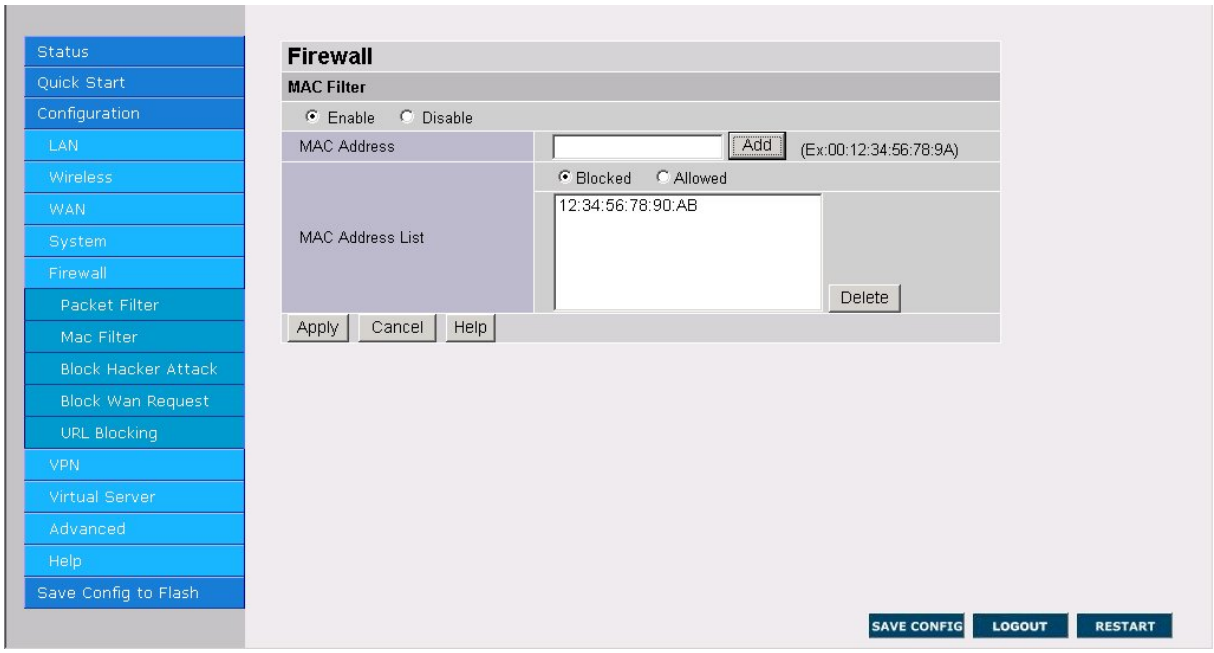
3.4.3.4.2 MAC Filter

MAC filtering function enables you to configure your router to block specified internal user (**MAC address**) from Internet access. You must check the **"Enable"** radio button to make the following figure appear 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

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

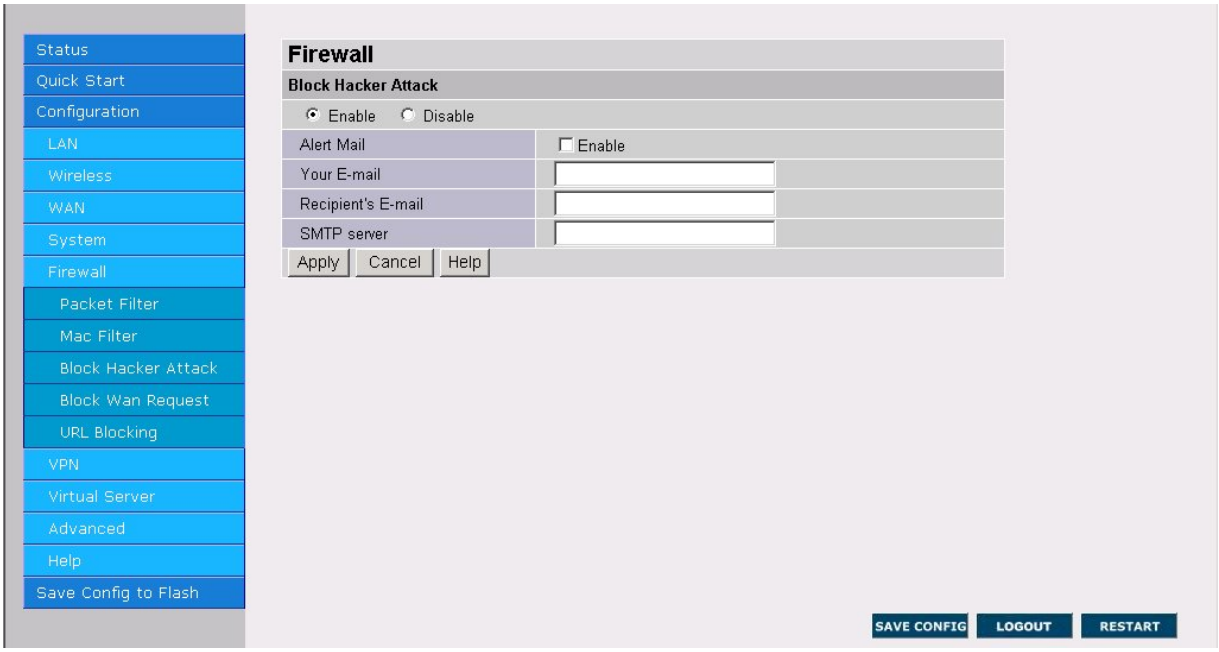
⊙ **Allowed:** Select this radio button if you want to block all the PCs in the LAN from Internet access except for those with MAC address listed in the list.

3.4.3.4.3 Block Hacker Attack

BIPAC 6500 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**



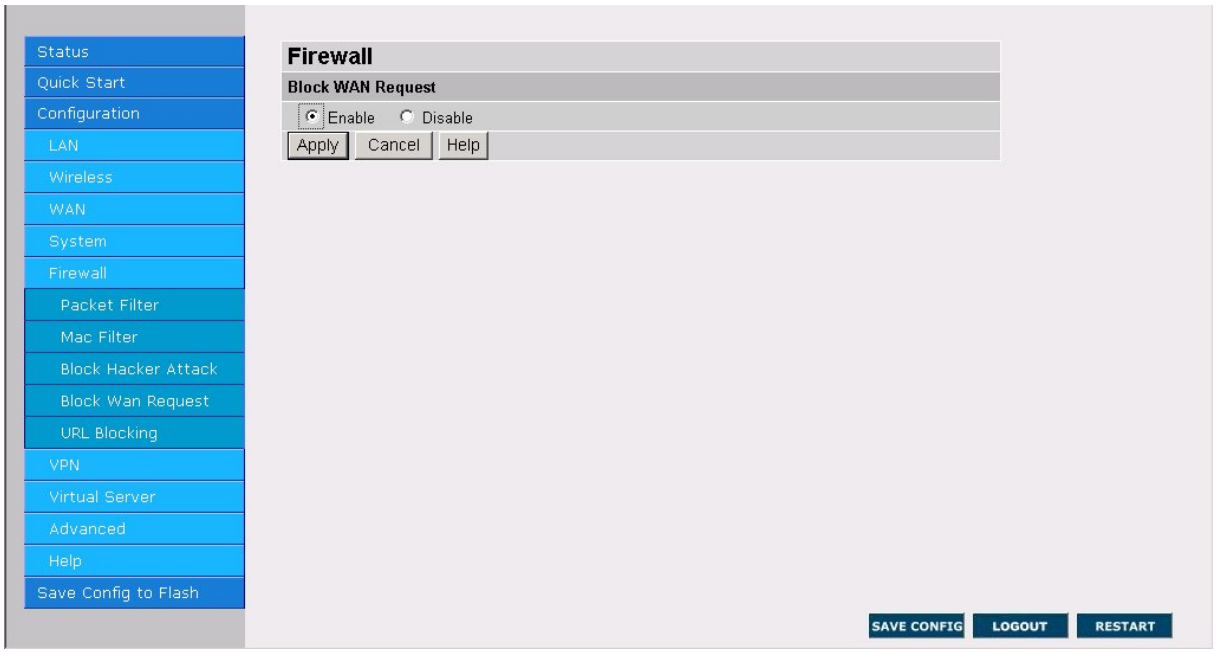
☐ **Alert Mail:** Check if you want to be informed by emails when hackers attack the router.

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

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

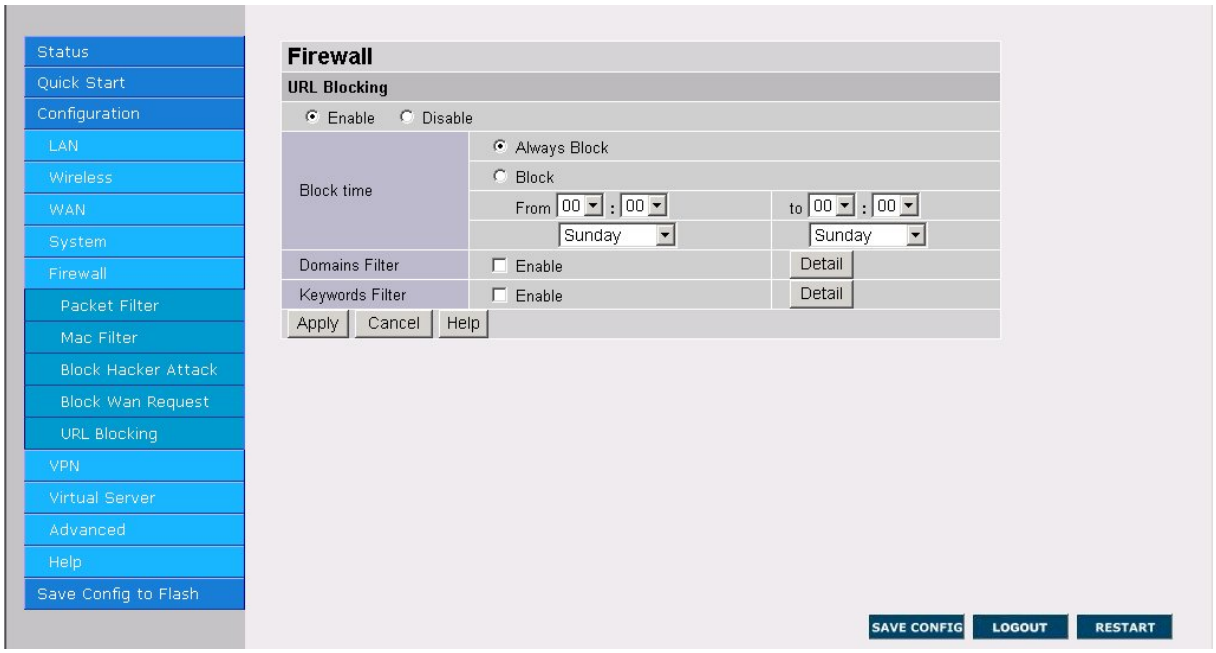
3.4.3.4.4 Block WAN Request

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



3.4.3.4.5 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

Check this button, if you wish not to access this website through out the entire time.

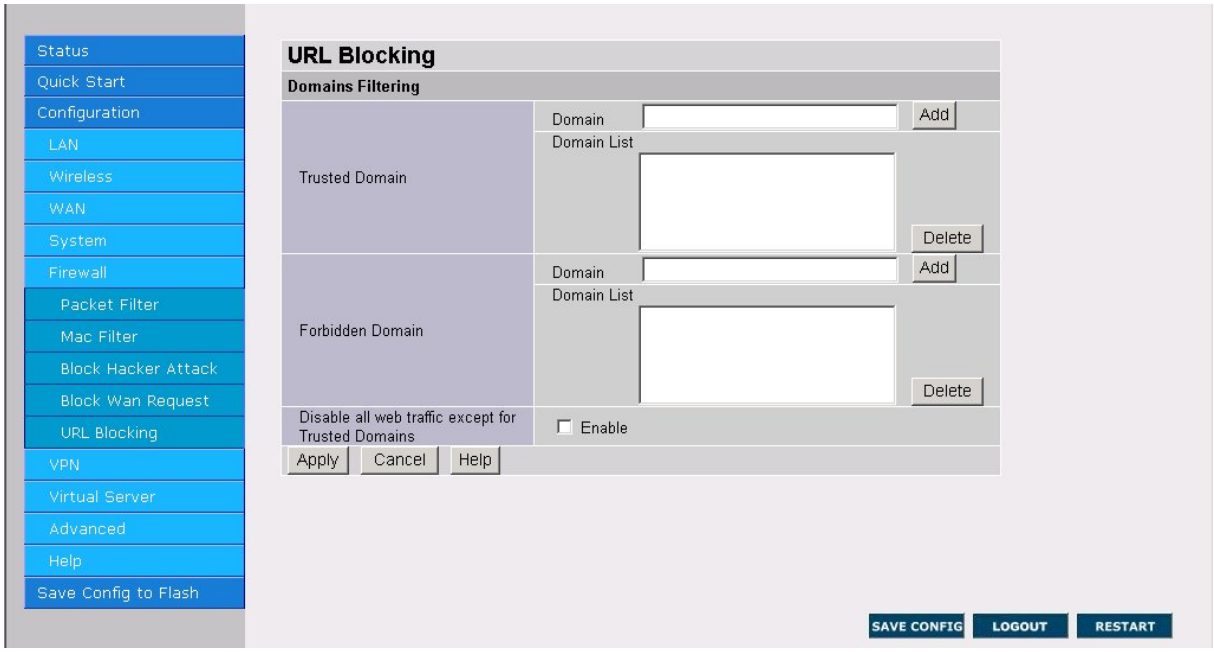
⊙ Block (From ☐ to ☐)

Check this button, if you only wish to block a URL in a specific time interval. For example, if you wish to temporarily block a URL from Monday 8:00am until Wednesday night at 7:40pm, in the space provided above, you should select **08:00, Monday** to **19:40, Wednesday.**

☐ **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

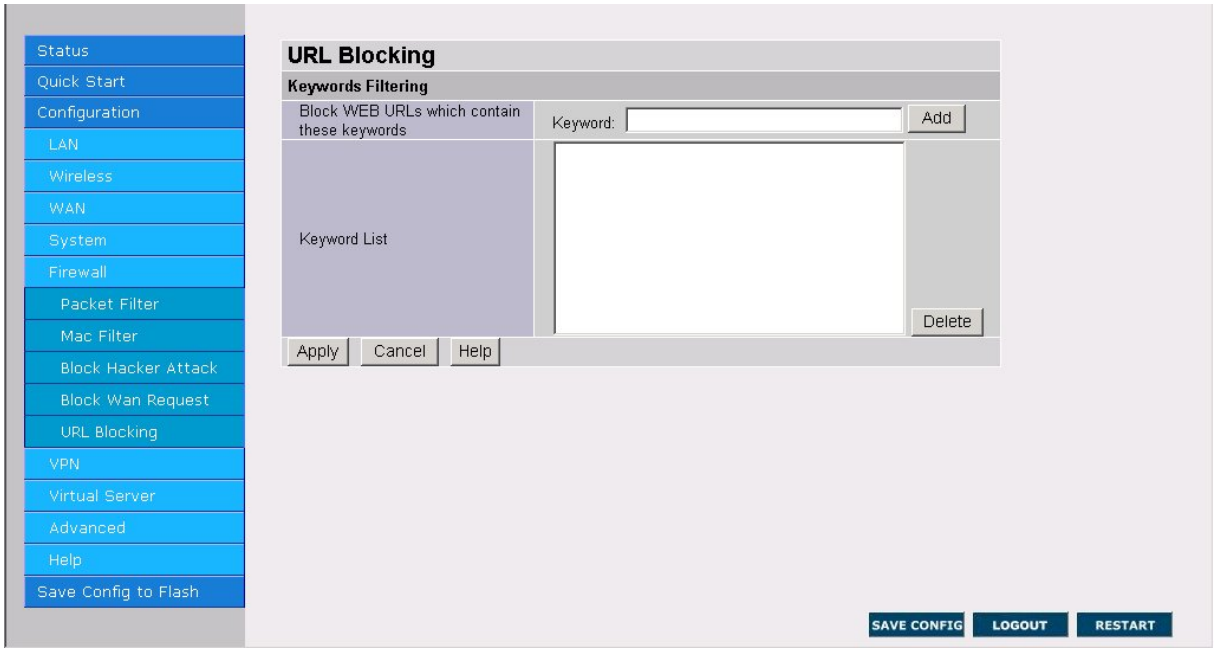


If the router is configured to allow internal users to access only certain specified domains, check the **Disable all web traffic except for Trusted Domains** and add domain name into the domain list. If the router is configured to allow internal users to access all websites except for some forbidden 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



BIPAC 6500 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 can not 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.

3.4.3.5 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.

There is three items under **VPN** section: PPTP, IPSec and L2TP.

- ***The reference of VPN, please refer to VPN Configuration document of CD.***

3.4.3.6 Virtual Server

Being a natural Internet firewall, BIPAC 6500 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 router, then passed to the DMZ host when packet is not sent from hacker and not matched by virtual server list.

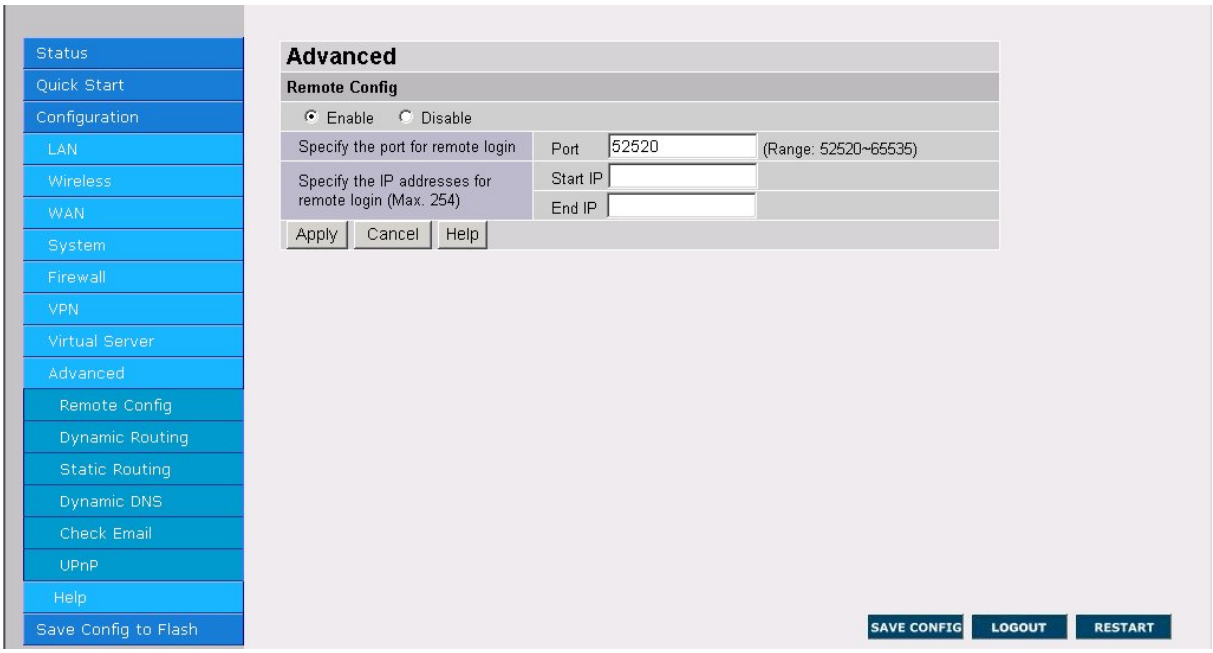
If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easy way is that the IP address assigned to each virtual server should not fall into the range of IP addresses that are to be issued by the DHCP server.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

3.4.3.7 Advanced

There are six items under the **Advanced** section: Remote Config, Dynamic Routing, Static Routing, Dynamic DNS, Check Email and UPnP .

3.4.3.7.1 Remote Config

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



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.

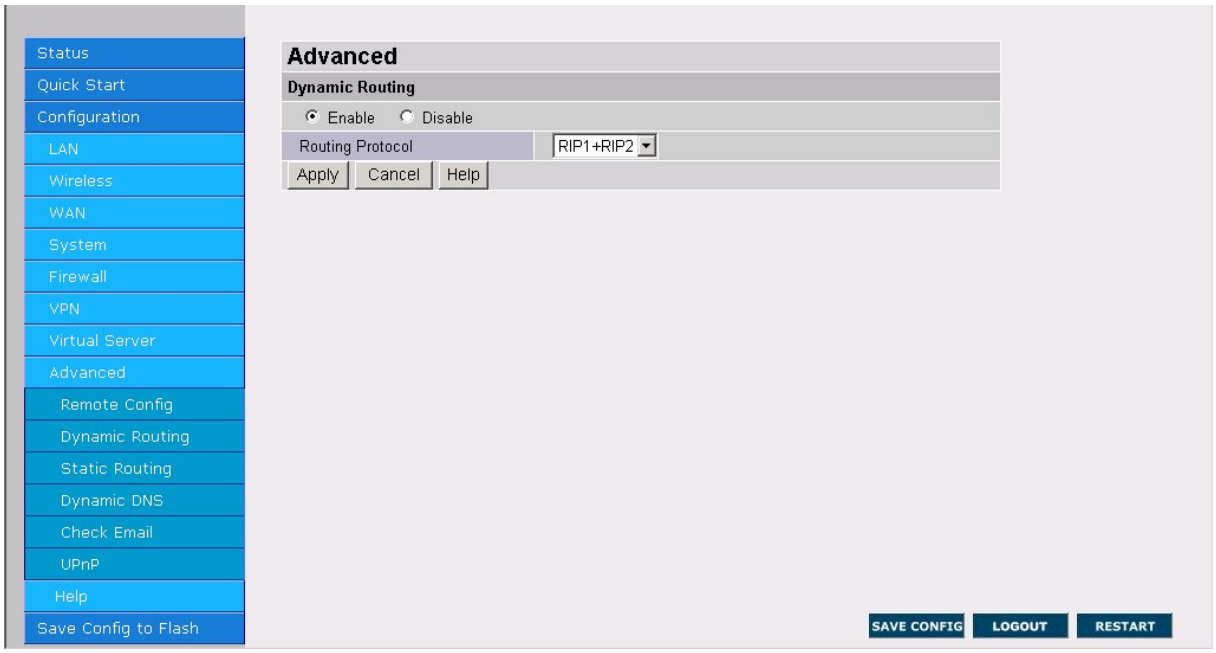
If for any reason you want to limit the IP addresses for remote login, please enter the **Start IP** and the **End IP** address. But be noted that the range is not allowed to exceed 254.

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.

3.4.3.7.2 Dynamic Routing

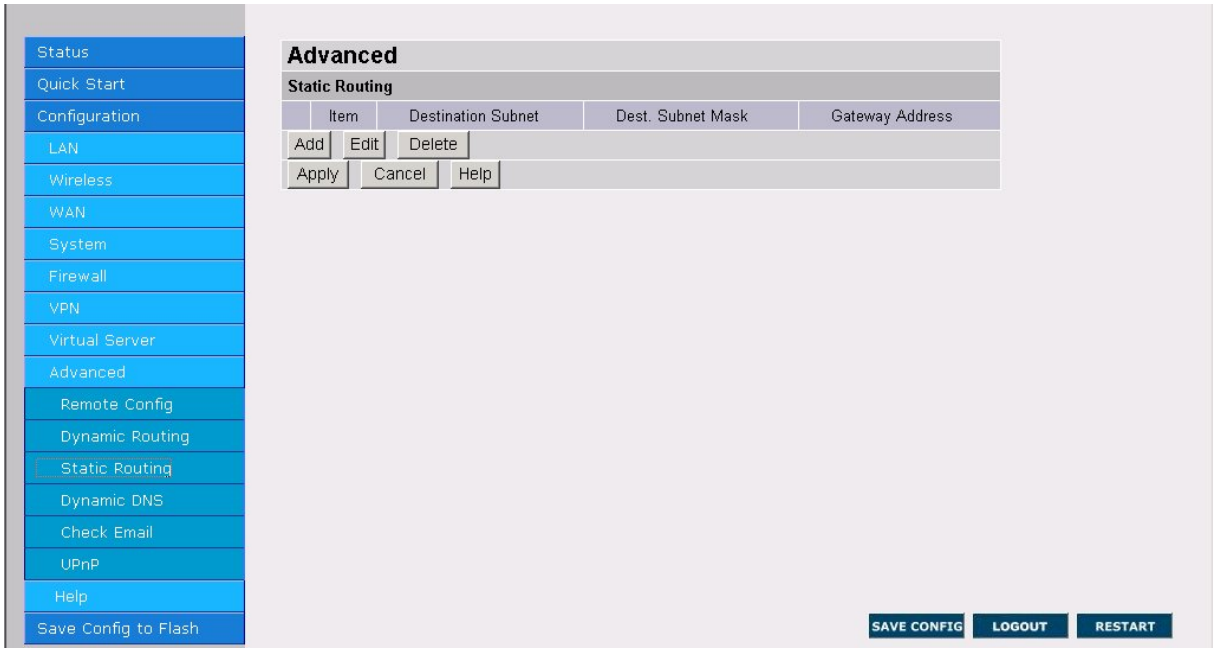
The dynamic routing function of BIPAC 6500 can be used to allow the router to automatically adjust to physical changes in the network’s layout. BIPAC 6500 uses the dynamic RIP protocol. It regularly broadcasts routing information to other routers on the network. Choose the protocol

— RIP1 or RIP1+RIP2 — you want the router to use to transmit / receive data on / from the network.



3.4.3.7.3 Static Routing

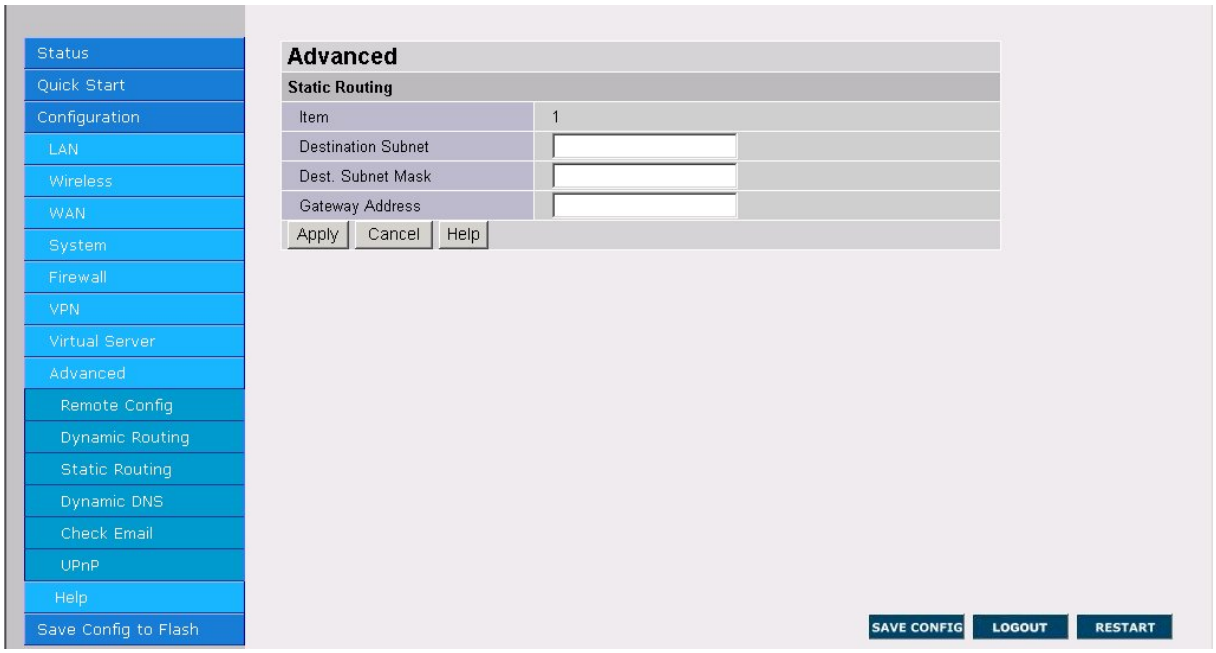
If you have another router with a LAN-to-LAN connection, you may create a static routing on the router that is the gateway to Internet.



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.



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

3.4.3.7.4 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.

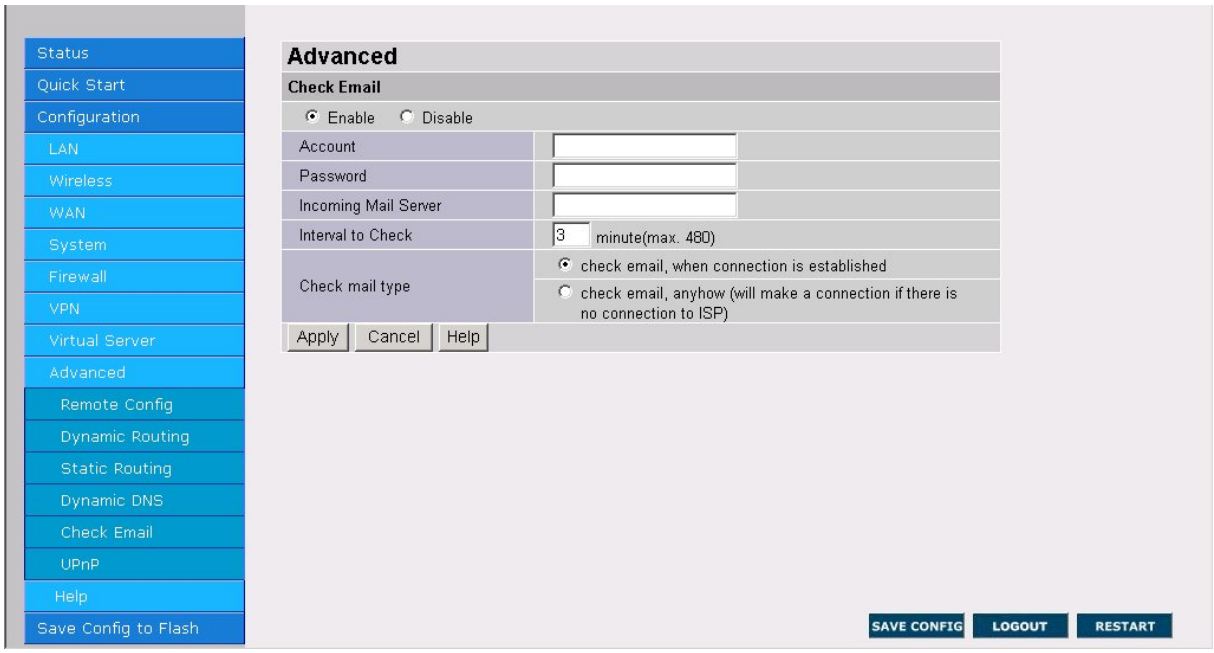
User Name: Enter the username used for sign-up.

Password: Enter the password used for sign-up.

Period: Set the time period for the Router to exchange information with the DDNS server. In addition to update periodically according to this period setting, BIPAC 6500 will take the same action automatically whenever the assigned IP changes.

3.4.3.7.5 Check Email

BIPAC 6500 may set a Email account to periodically check up incoming mail, LED flashes green when there is Email.



Account : Enter your Email account in the field.

Password : Enter your Email password in the field.

Incoming Mail Server : Specify your incoming mail server name or IP address.

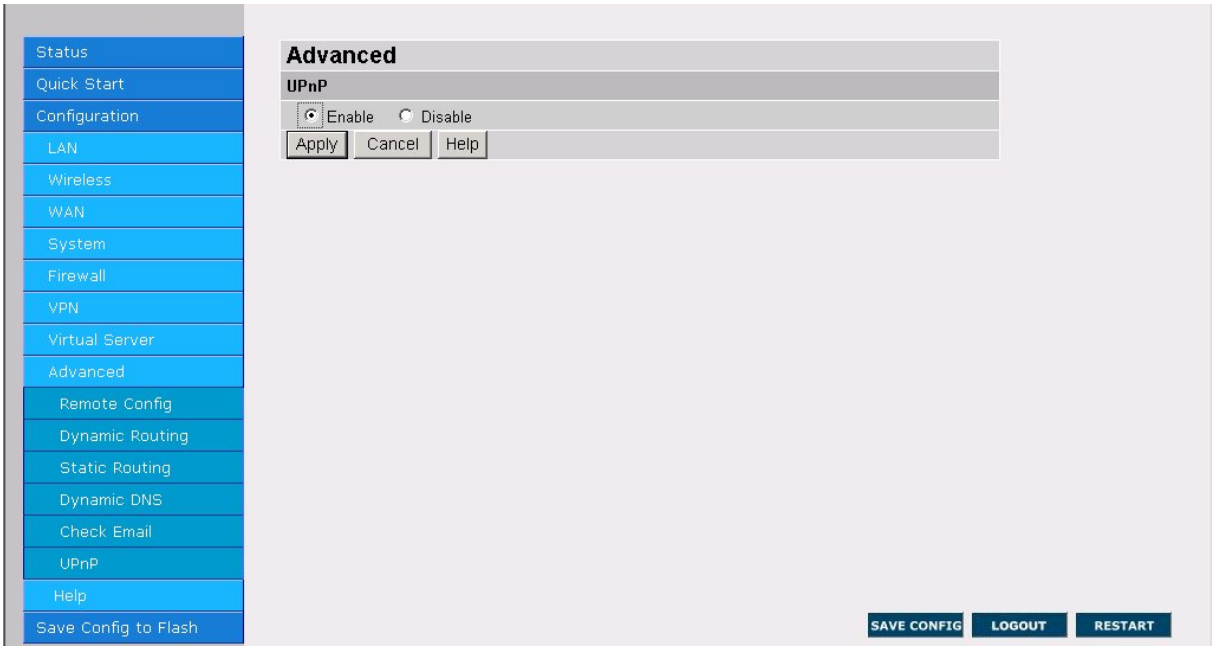
Interval to Check : Periodical timer checks up incoming Emails.

3.4.3.7.6 UPnP

Universal Plug and Play (UPnP) is an architecture for pervasive peer-to-peer network connectivity of PCs and intelligent devices or appliances, particularly within the home. UPnP builds on Internet standards and technologies, such as TCP/IP, HTTP, and XML, to enable these

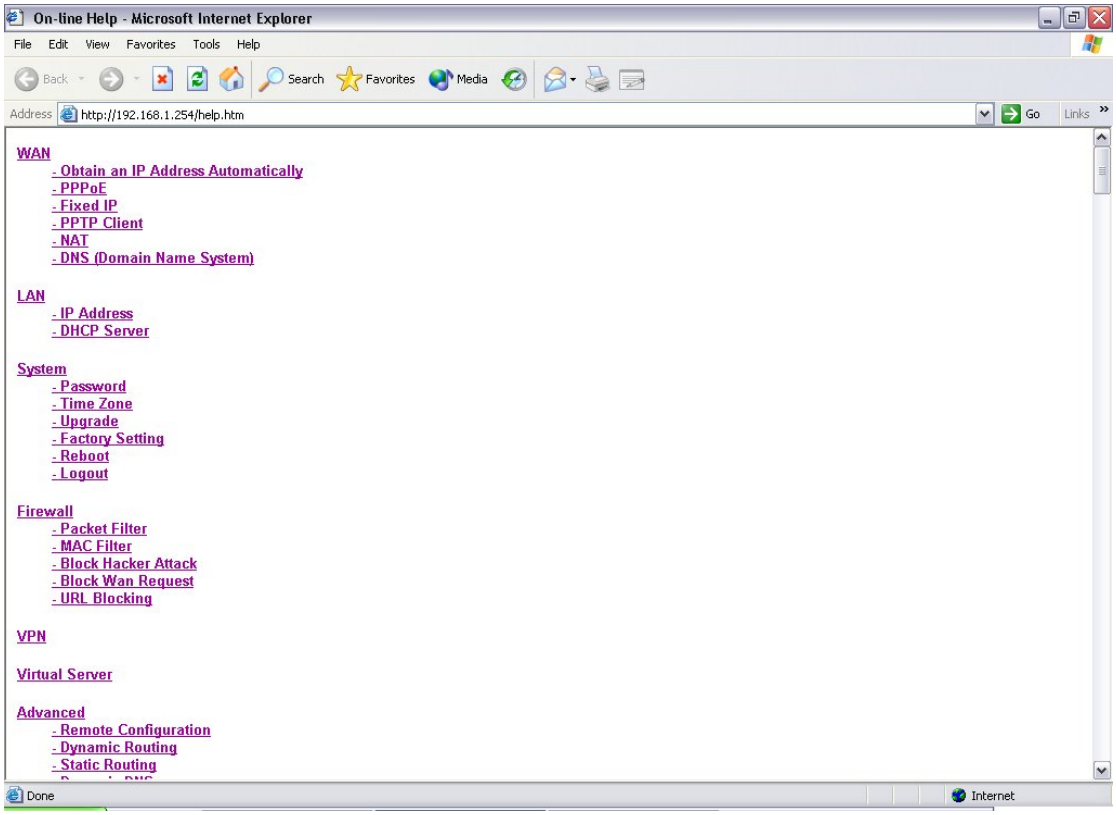
devices to automatically connect with one another and work together to make networking - particularly home networking - possible for more people.

The UPnP aware applications such as MSN Messenger will discover that they are behind a NAT router, learn the external IP address and configure port mappings on the router to forward packets from the external ports of the router to the internal ports used by the application.



3.4.3.8 Help

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 proceed the configuration.



3.4.4 Status

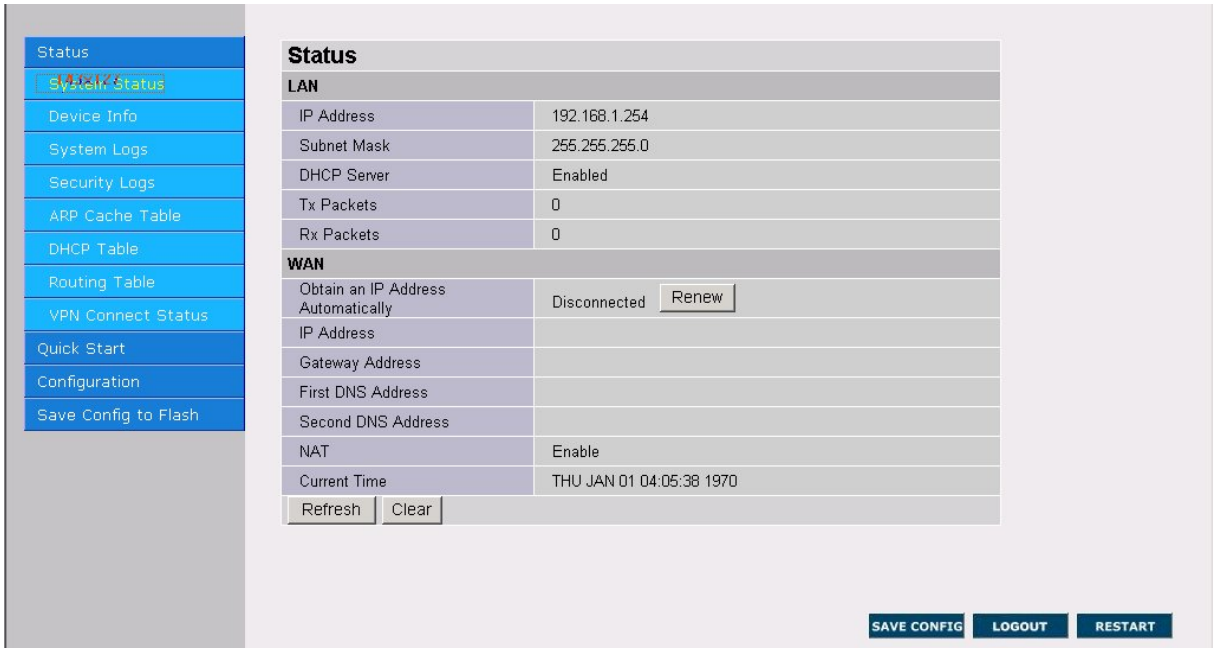
The **Status** section provides and contains many items including device H/W and S/W information, LAN, WAN, Port status and all defined interfaces. It also provides useful information for users to review the status of the device.

3.4.4.1 System Status

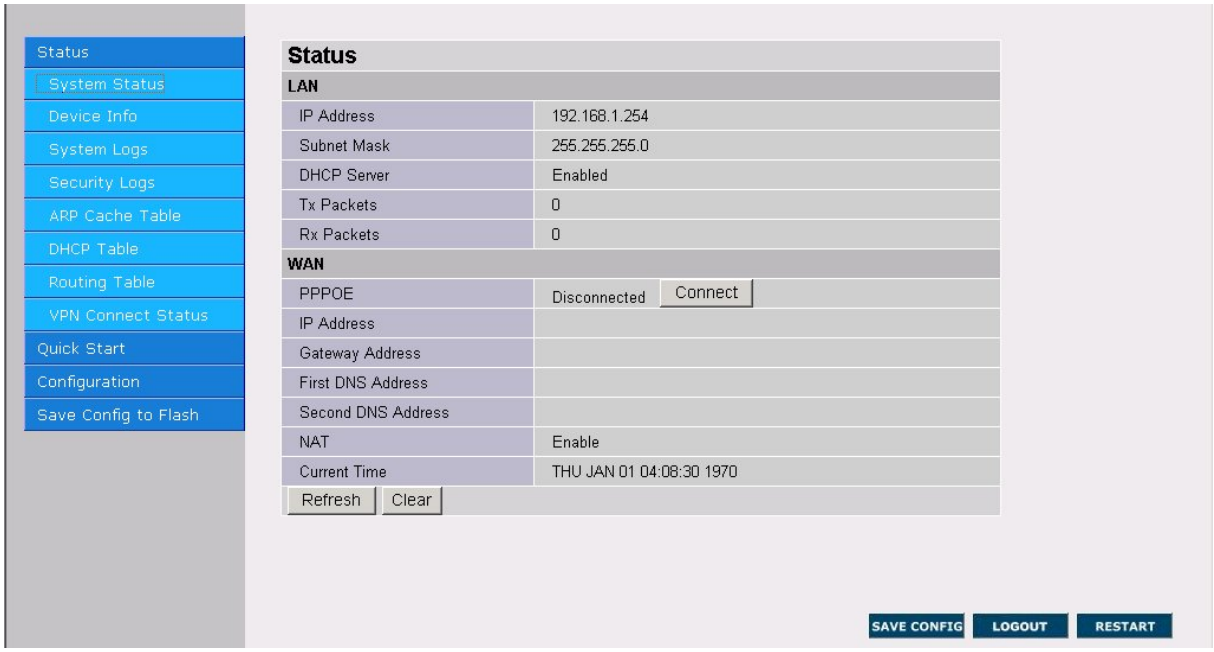
Display the current LAN and WAN connection status.

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.

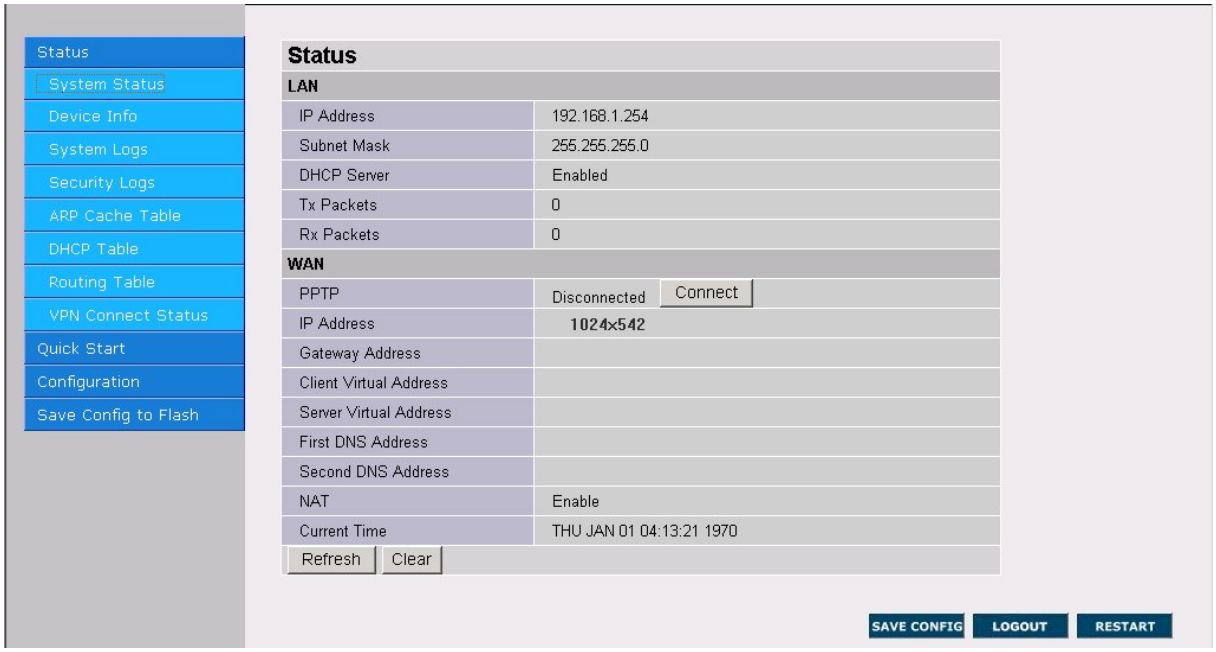
If you choose “Obtain an IP Address Automatically” as your protocol, there will be a **“Renew”** button beside the connection status description. Click this **“Renew”** button whenever you want to get a new IP Address rather than the existent one. There are three connection statuses in total under this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



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.



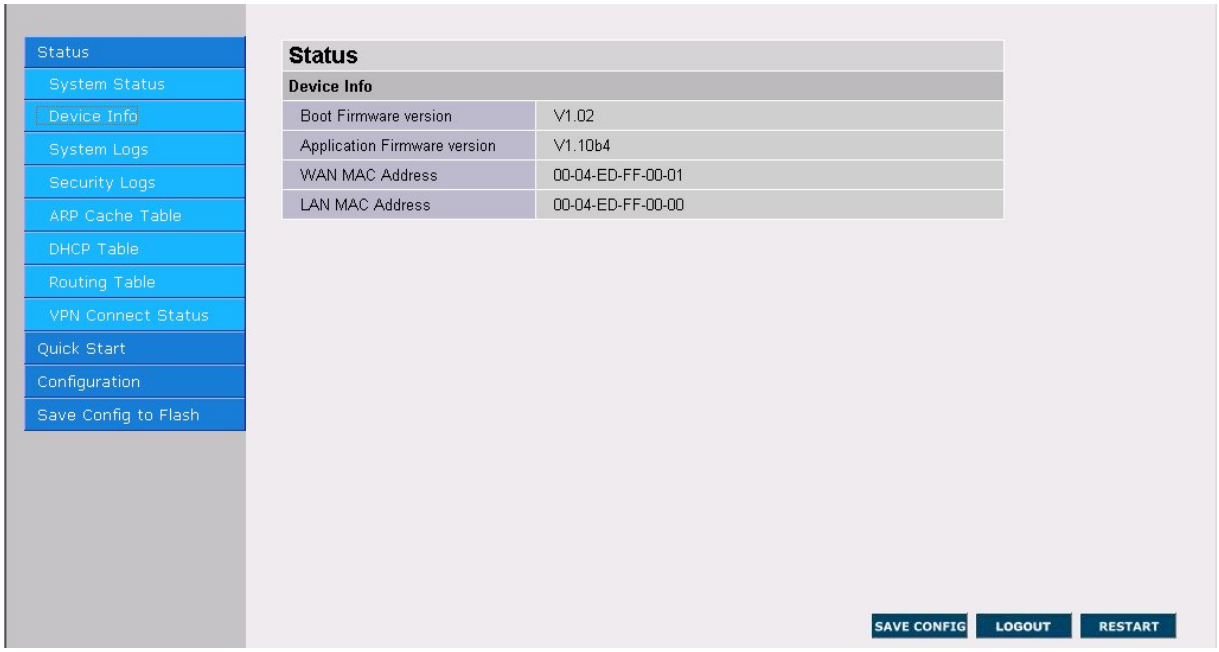
In the “PPTP Client” protocol, you can press the “Connect” button when the line is disconnected or press the “Disconnect” button when the line is connected.



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.

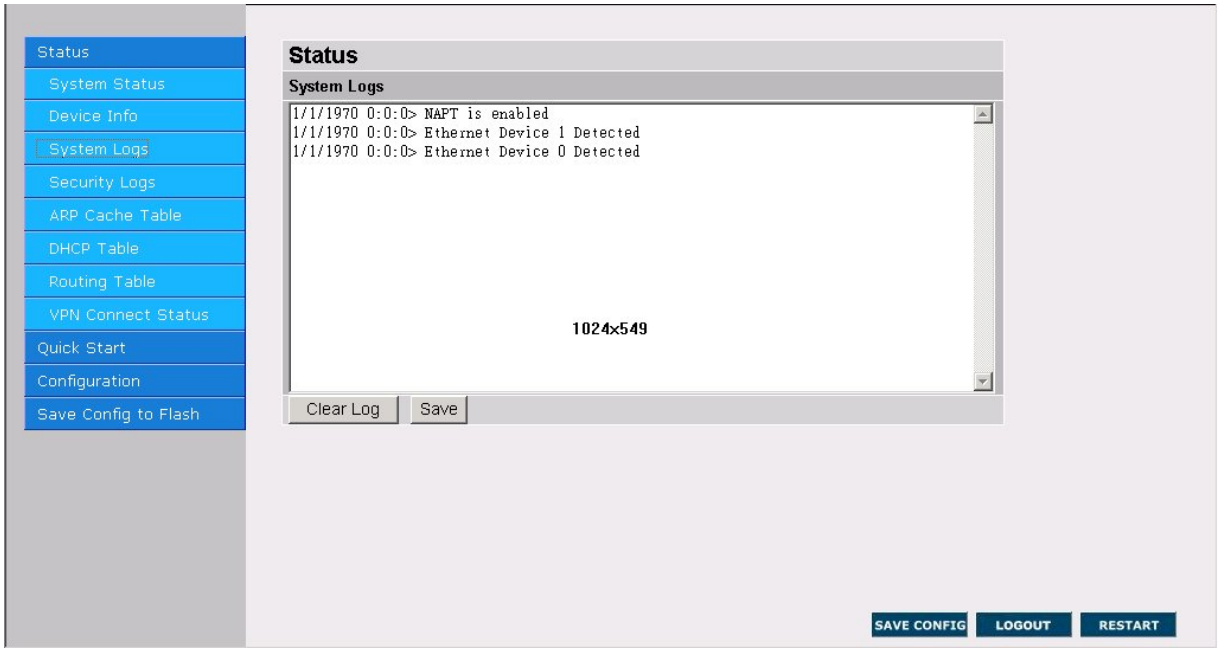
3.4.4.2 Device Info

Display the current Firmware version and MAC addresses of your router.



3.4.4.3 System Logs

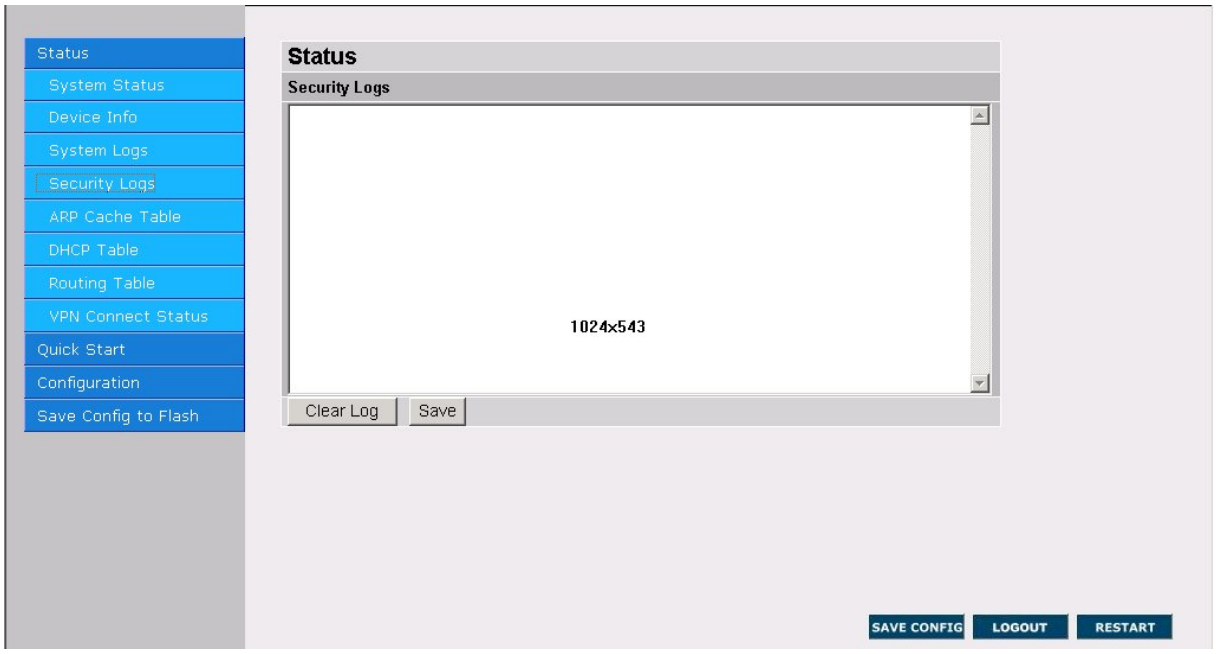
Display the system logs cumulated till the present time. You can trace the historical information through this function.



Refresh: Click **"Refresh"** to get the latest information of system logs.

3.4.4.4 Security Logs

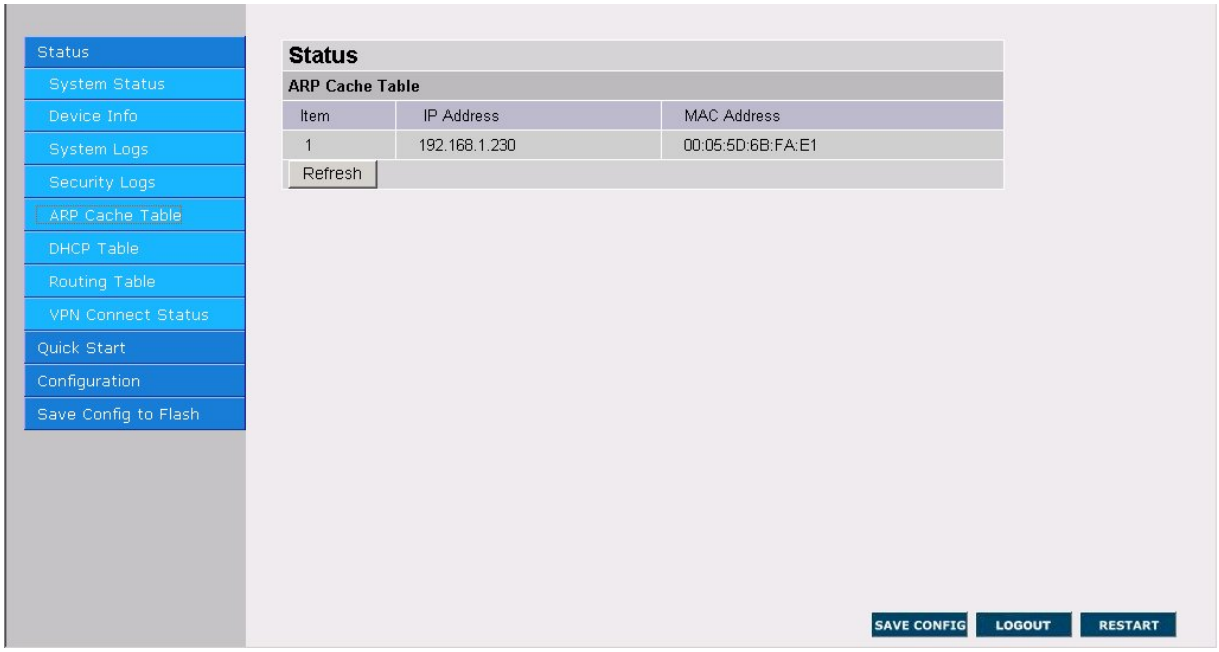
Display the information of security logs. If hacker attacks your sever, he will be isolated by the firewall function and the router will record related information. Hence, you know where the hacker comes from.



Refresh: Click **"Refresh"** to get the latest information of system logs.

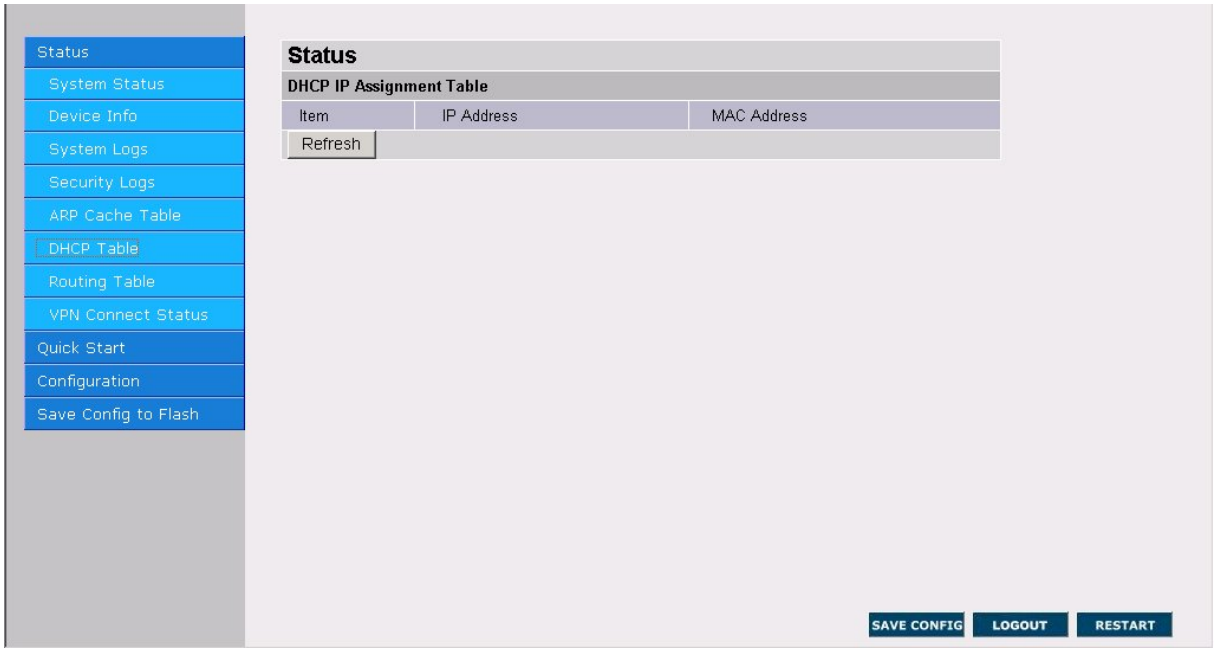
3.4.4.5 ARP Cache Table

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



3.4.4.6 DHCP Table

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.

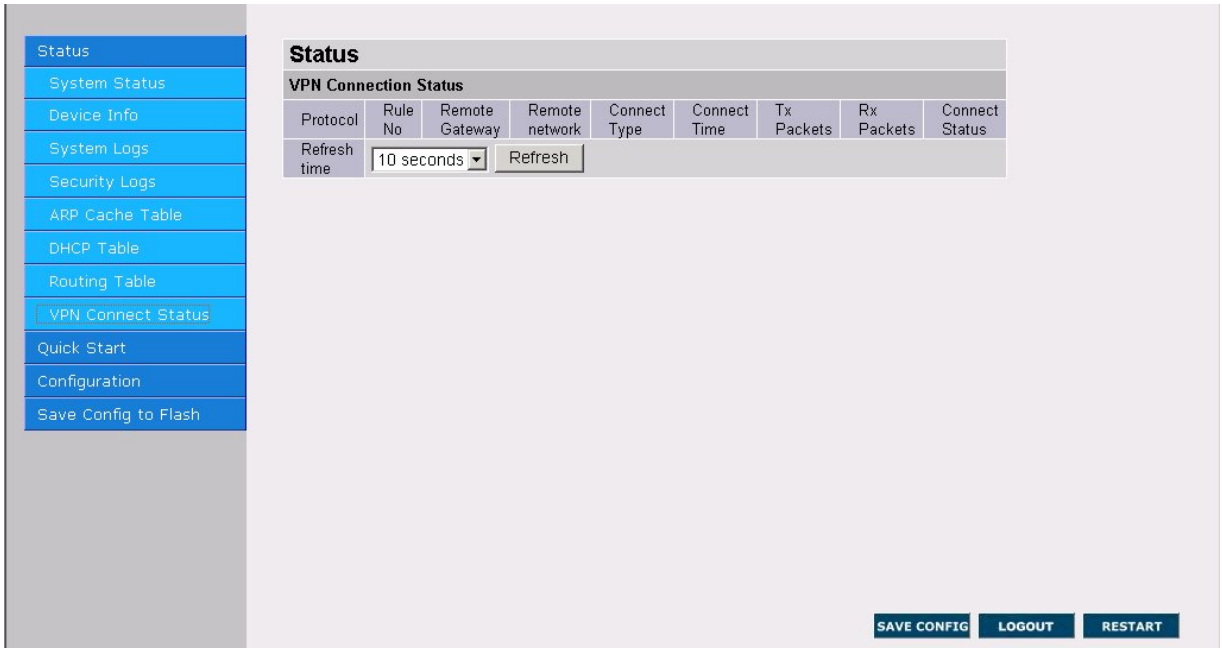


3.4.4.7 Routing Table

Display the current routing paths of BIPAC 6500.

3.4.4.8 VPN Connect Status

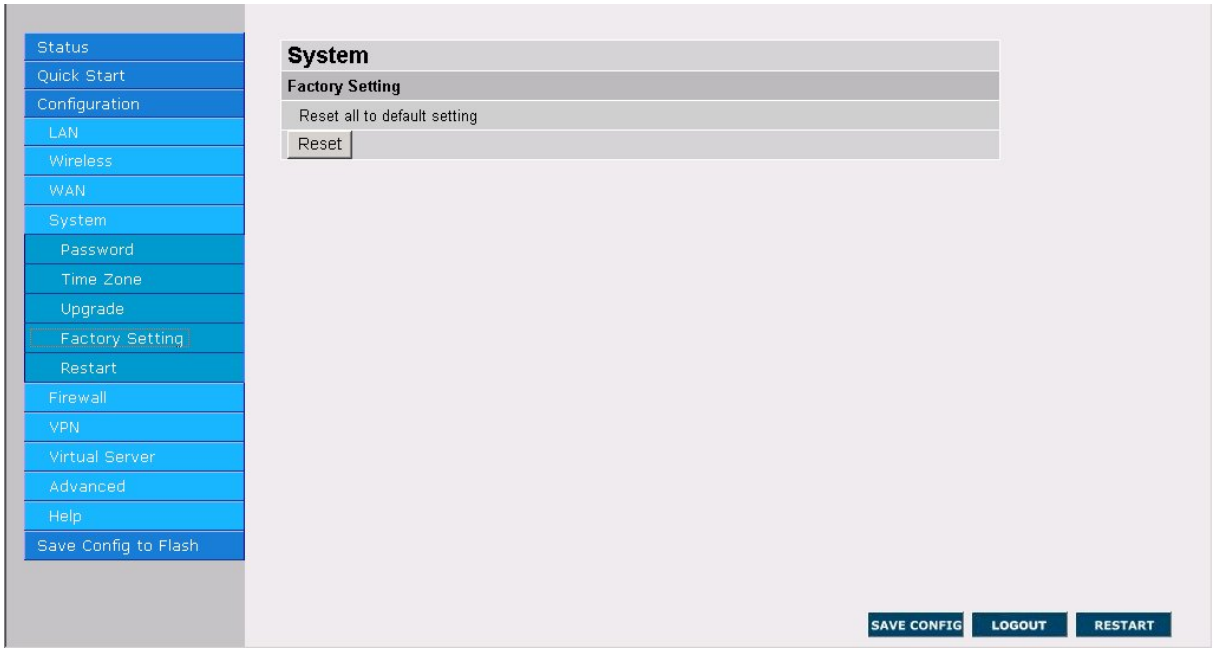
Display the current VPN connection status.


Status
System Status
Device Info
System Logs
Security Logs
ARP Cache Table
DHCP Table
Routing Table
VPN Connect Status
Quick Start
Configuration
Save Config to Flash
Status
VPN Connection Status
Protocol
Rule No
Remote Gateway
Remote network
Connect Type
Connect Time
Tx Packets
Rx Packets
Connect Status
Refresh time
10 seconds
Refresh
SAVE CONFIG
LOGOUT
RESTART

Chapter 4
Troubleshooting

If BIPAC 6500 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 it's default state. The factory default values is 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 BIPAC 6500 or by two or more workstations occupying the same IP address. Please run the "**winipcfg**" utility to release all current configuration first, and then renew all if your computer is set to get an IP address automatically. BIPAC 6500 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.

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 router 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 router 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 router's IP address (192.168.1.254). BIPAC 6500 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 router's IP address (192.168.1.254) in this field and click Add button.

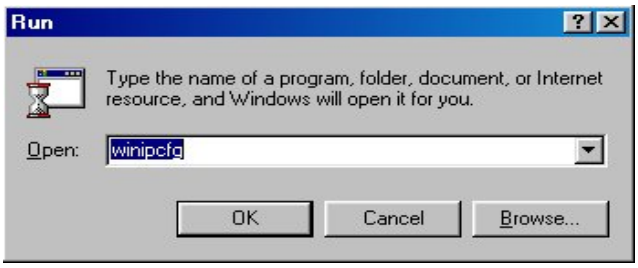
Is there a tool to check my PC's TCP/IP settings in MS Windows?

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

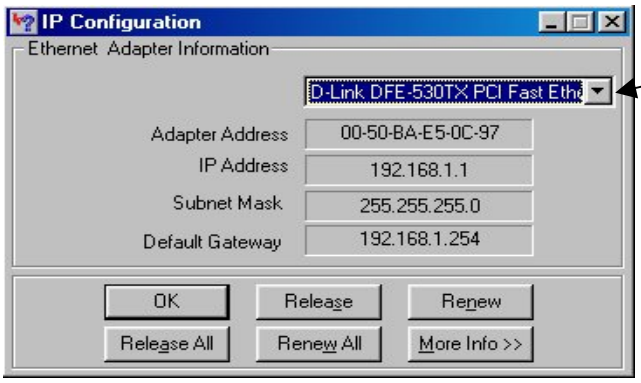
WINIPCFG.EXE

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.

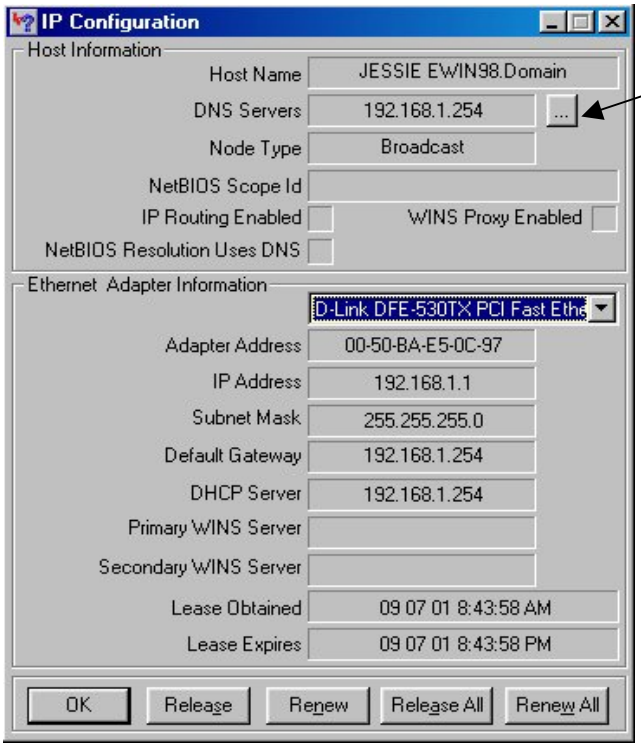
1. From Windows, go to **Start → Run**, enter **WINIPCFG,** and click **"OK"**.



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".



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. BIPAC 6500) 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

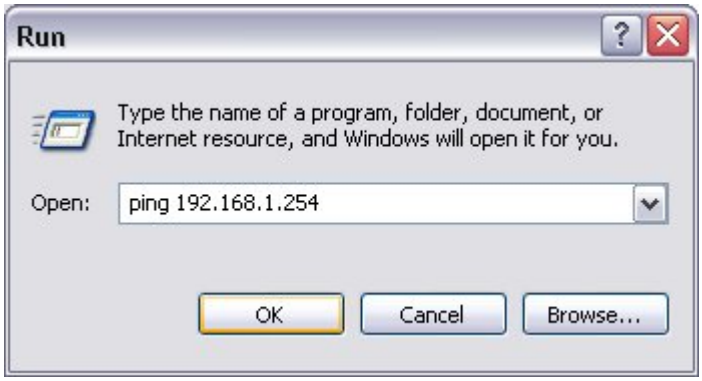
For WinNT, Win2000 and WinXP, go to **Start → Programs → Accessories → Command Prompt** to open the Command Prompt. Type in **IPCONFIG /ALL** and hit "Enter" to see the adapter's information. Type in **IPCONFIG /RELEASE** to release all adapters' IP address and **IPCONFIG /RENEW** to renew IP addresses.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

How can I test the whole path (PC←→Router←→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 router, please verify the PC, cables, HUB/Switch and router.

- **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 router, 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 router.

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 router 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 Info** or **WAN -> Obtain an IP address automatically**, then you will see the MAC address for WAN port. Usually, some cable operators need this information for registration.

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

When being a natural Internet firewall (NAT + Advanced Firewall), BIPAC 6500 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 3.4.3.6 "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 router, 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 BIPAC 6500?

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

We will suggest that the router 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 Router?

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 router 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 BIPAC 6500 simultaneously?

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

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

The broadband firewall router 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 **3.4.3.2** "WAN" to configure broadband firewall router and enjoy surfing the Internet.

APPENDIX A
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)

APPENDIX B
Product Support

Most problems can be solved by using the *Troubleshooting* in Chapter 4.

If you continue to have problems, you should contact the dealer where you bought this product.

For further assistances with the product, please feel free to contact and visit us at: http://www.billion.com/T