Michelangelo Office Pro V
Michelangelo Office Wave Pro V

User's Guide
rev. 1.0 10/2003

digicom
http://www.digicom.it

User's Manual

Table of Contents

Chapter 1
Introduction

1.1 An Overview of the MICHELANGELO OFFICE PRO-V

The MICHELANGELO OFFICE PRO-V ADSL Firewall Router provides office and residential users the ideal solution for sharing a high-speed ADSL broadband Internet connection between an 11Mbps wireless* network and a 10/100Mbps Fast Ethernet backbone. It can support downstream transmission rates of up to 8Mbps and upstream transmission rates of up to 1024Kbps. It also supports rate management that allows ADSL subscribers to select an Internet access speed suiting their needs and budgets. It is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G992.2).

The product supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1577) to establish a connection with ISP. Besides, an embedded PPTP client and PPTP server are supported to establish a VPN tunnel with a remote PPTP device. The product also supports VC-based and LLC-based multiplexing.

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.

This product also serves as an Internet firewall, protecting your network from being accessed by outside users. Not only provides the natural firewall function (Network Address Translation, NAT), it also provides rich firewall features to secure a 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, a user can open some specific ports for outside users to access internal services in the network. Finally it can also detect and block many Hacker Patterns and not allow hackers into your network.

Integrated DHCP services, client and server, allows 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 a 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

*Wireless only on Michelangelo Office Wave Pro-V model

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 Multi-player 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. One Digicom ADSL Firewall Router
2. One CD-ROM containing the on-line manual
3. One RJ-11 ADSL/telephone cable
4. One straight-through CAT-5 Ethernet cable
5. One AC-DC power adapter (output: 12V DC, 1A)
6. One Quick Start Guide

1.3 MICHELANGELO OFFICE PRO-V Features

MICHELANGELO OFFICE PRO-V provides the following features:

ADSL Multi-Mode Standard: Supports downstream transmission rates of up to 8Mbps and upstream transmission rates of up to 1024Kbps. It also supports rate management that allows ADSL subscribers to select an Internet access speed suiting their needs and budgets. It is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G992.2).

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 MDI-X for 10Base-T and 100Base-TX ports is supported. An Ethernet straight or crossover cable can be used directly, this fast Ethernet switch will detect it automatically.

Multi-Protocol to Establish A Connection: Supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1577) to establish a connection with the ISP. The product also supports VC-based and LLC-based multiplexing.

Quick Installation Wizard: Supports a WEB GUI page to install this device quickly. With this wizard, an end user can enter the information easily which they from the ISP, then surf the Internet immediately.

Universal Plug and Play (UPnP) and UPnP NAT Traversal: This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors. It makes network simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices.

*Wireless only on Michelangelo Office Wave Pro-V model

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 and others.

Firewall: Supports SOHO firewall with NAT technology. Automatically detects and blocks the Denial of Service (DoS) attack. The packet filtering and SPI are also supported. The hacker's attack will be recorded associated with timestamp in the security logging area. More firewall features will be added continually, please visit our web site to download latest firmware.

Domain Name System (DNS) relay: provides an easy way to map the domain name (a friendly name for users such as www.yahoo.com) and IP address. When a local machine sets its DNS server with this router's IP address, then every DNS conversion requests packet from the PC to this router will be forwarded to the real DNS in the 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. For example, to use the service, you must first apply an account from this free Web server http://www.dyndns.org/. There are more than 5 DDNS servers supported.

Virtual Private Network (VPN): Allows a user to make a tunnel with a remote site directly to secure the data transmission among the connection. Users can use **embedded PPTP client/server and IPSec** supported by this router to make a VPN tunnel or the 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 the 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 the local computer. The Always ON, Dial On Demand and auto disconnection (Idle Timer) functions are provided too.

Virtual Server: Users 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, users can assign a PC in a LAN acting as a WEB server inside and expose it to the outside network. Outside users can browse an 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 filters the packet based on IP address, but also based on Port numbers.

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.

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

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

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

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

Rich management interfaces: Supports flexible management interfaces with local console port, LAN port, and WAN port. Users can use terminal application through console port to configure and manage the device, or Telnet, WEB GUI, and SNMP through LAN or WAN ports to configure and manage a device.

Chapter 2
Using MICHELANGELO OFFICE PRO-V

2.1 Cautions for using the MICHELANGELO OFFICE PRO-V

Do not place the MICHELANGELO OFFICE PRO-V under high humidity and high temperature.

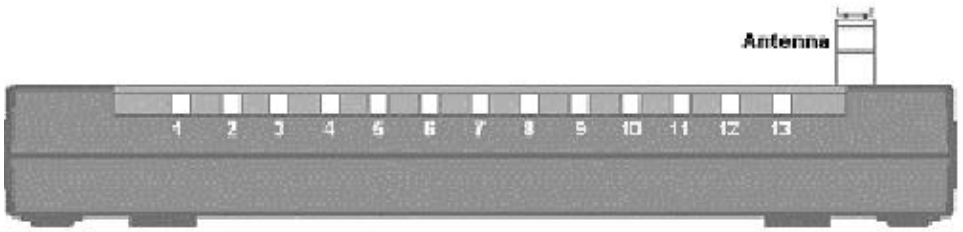
Do not use the same power source for MICHELANGELO OFFICE PRO-V with other equipment.

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

Place the MICHELANGELO OFFICE PRO-V on a stable surface.

Only use the power adapter that comes with the package.

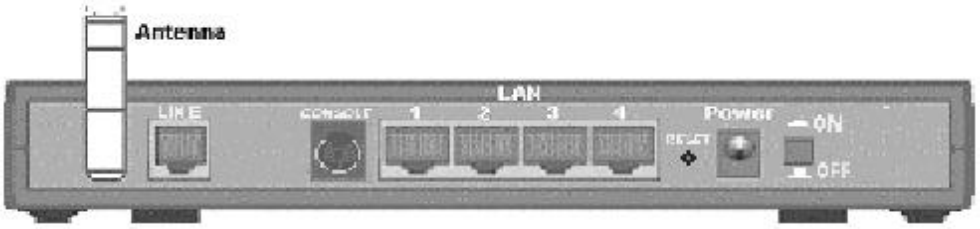
2.2 The Front LEDs



LED		Meaning
1	**PWR**	Lit when power ON
2	**SYS**	Lit when system is ready
3	**LAN port 1**	Lit when connected to Ethernet device Green for 100Mbps; Orange for 10Mbps Blinking when data transmit/received
4	**LAN port 2**	Lit when connected to Ethernet device Green for 100Mbps; Orange for 10Mbps Blinking when data transmit/received

5	**LAN port 3**	Lit when connected to Ethernet device Green for 100Mbps; Orange for 10Mbps Blinking when data transmit/received
6	**LAN port 4**	Lit when connected to Ethernet device Green for 100Mbps; Orange for 10Mbps Blinking when data transmit/received
7	**WLAN***	Lit green when the wireless connection is established. Flashes when sending/receiving data.
10	**MAIL**	Lit when there is email in the email account
11	**PPP**	Lit when there is a PPPoA/PPPoE connection
13	**ADSL**	Lit when successfully connected to an ADSL DSLAM

2.3 The Rear Ports



Port		Meaning
1	**LINE**	Connect the supplied RJ-11 cable to this port when connecting to the ADSL/telephone network.
2	**CONSOLE**	Connect a PS2/RS-232 cable to this port when connecting to a PC's RS-232 port (9-pin serial port).
3	**LAN** **1X — 4X (RJ-45 connector)**	Connect an UTP Ethernet cable to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
4	**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 the router, e.g. forgot the password)
5	**PWR**	Connect the supplied power adapter to this jack.

*Wireless only on Michelangelo Office Wave Pro-V model

6	**Power Switch**	A Power ON/OFF switch

2.4 Cabling

The most common problem is bad cabling or ADSL line. Make sure that all connected devices are turned on. On the front of the product is a bank of LEDs. As a first check, verify that the LAN Link and ADSL line LEDs are lit. If they are not, verify that you are using the proper cables.

Chapter 3
Configuration

The MICHELANGELO OFFICE PRO-V can be configured with your Web browser. The web browser is included as a standard application in the following operation systems, UNIX, Linux, Mac OS, Windows 98/NT/2000/Me, 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 MICHELANGELO OFFICE PRO-V, either to configure the device, or for network access. These PCs must have an Ethernet interface installed properly, be connected to the MICHELANGELO OFFICE PRO-V 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 that must be in the same subnet of the MICHELANGELO OFFICE PRO-V. The default IP address of the MICHELANGELO OFFICE PRO-V 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 MICHELANGELO OFFICE PRO-V. Also make sure you have UNINSTALLED any kind of software firewall that can cause problems accessing the 192.168.1.254 IP address of the router.

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 related manuals.

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

3.2 Connecting the MICHELANGELO OFFICE PRO-V

1. Connect the Router to a LAN (Local Area Network) and the ADSL/telephone network.
2. Power on the device
3. Make sure the PWR and SYS LEDs are lit steady & LAN LED is lit.
4. Before proceeding to the next step, make sure you have **uninstalled** any software firewall.

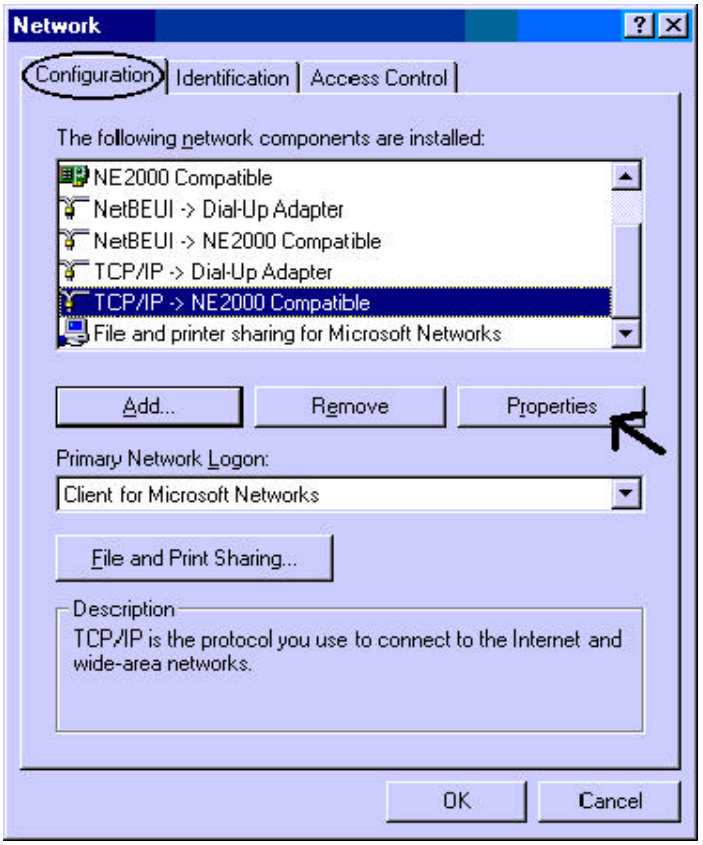
3.3 Configuring PC in Windows

3.3.1 For Windows 98/ME

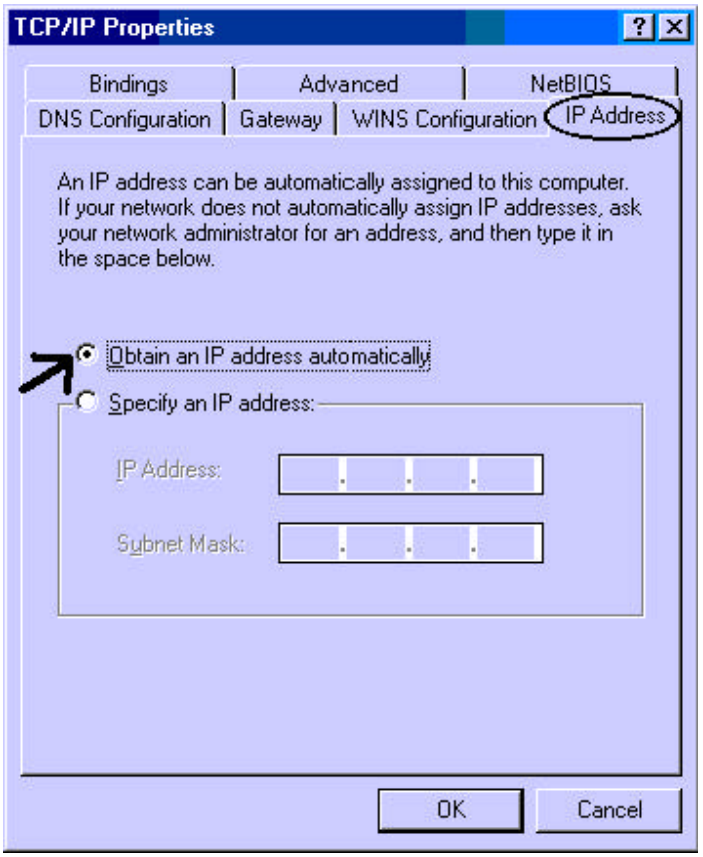
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.

2. Select **TCP / IP -> NE2000 Compatible**, or the name of any Network Interface Card (NIC) in your PC.

3. Click **Properties**.

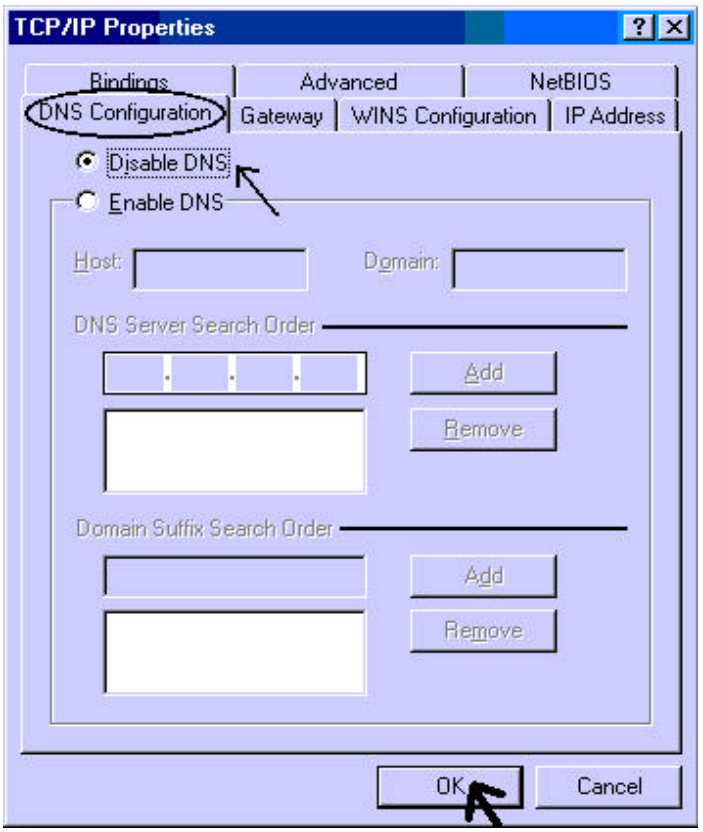


4. Select the **IP Address** tab. In this page, click the **Obtain an IP address automatically** radio button.



5. Then select the **DNS Configuration** tab.

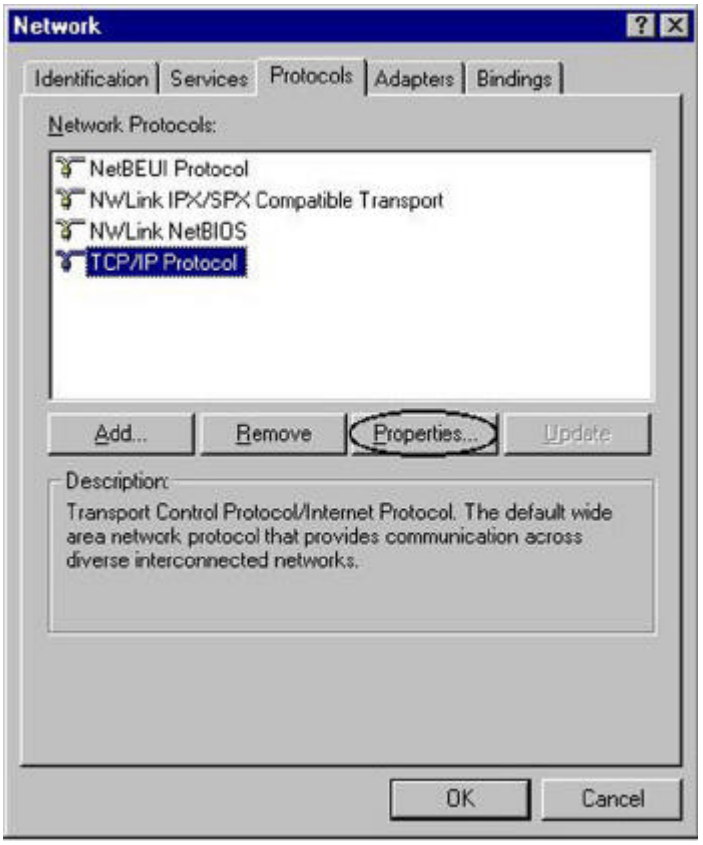
6. Select the **Disable DNS** radio button and click **"OK"** to finish the configuration.



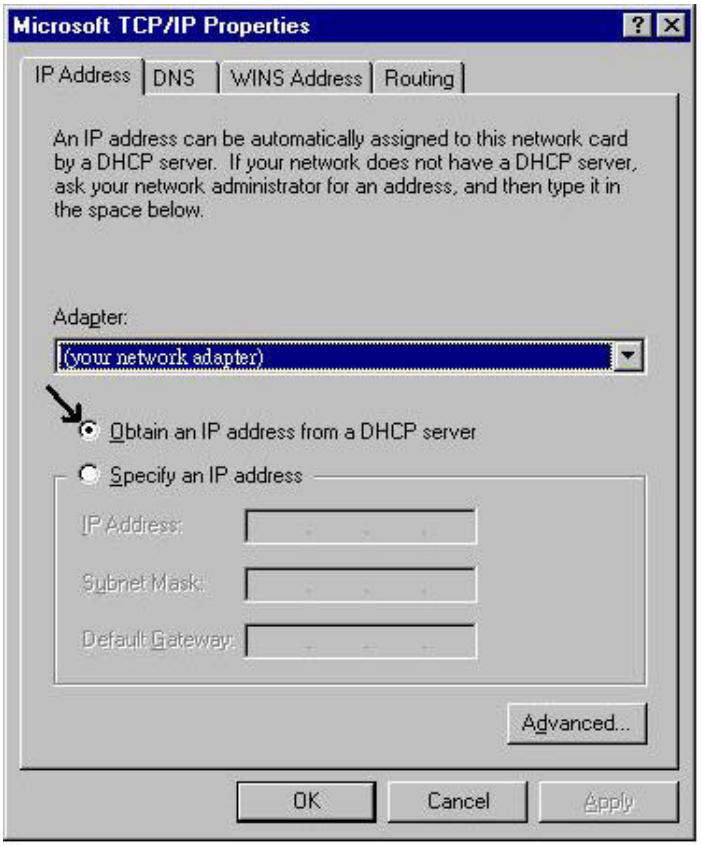
3.3.2 For Windows NT4.0

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**.



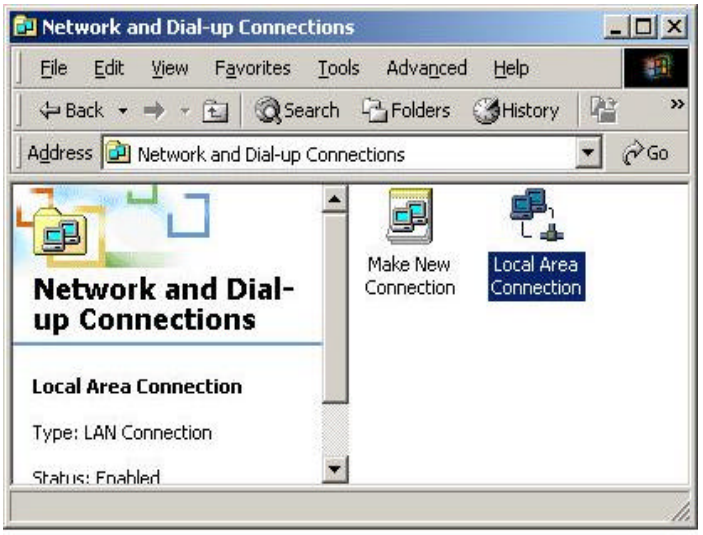
3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**.



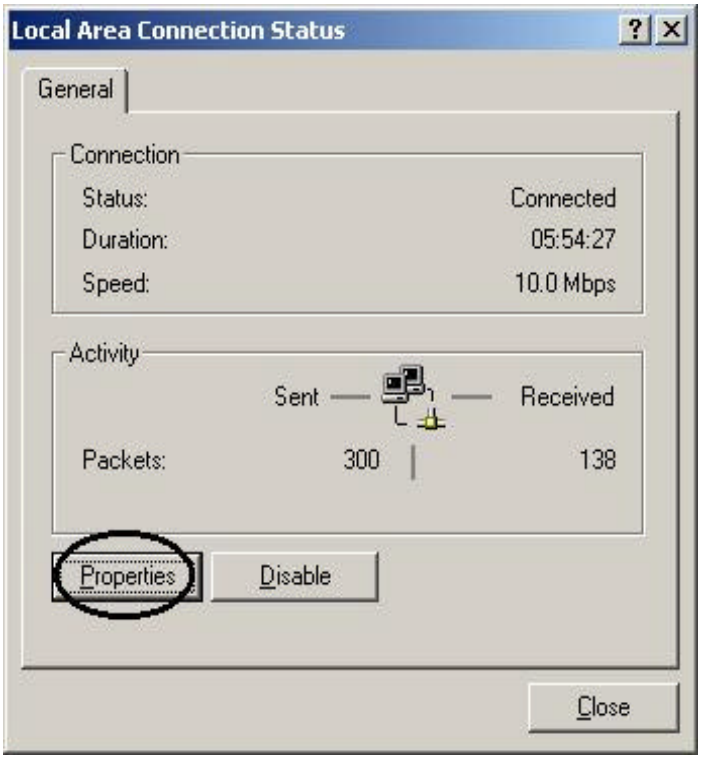
3.3.3 For Windows 2000

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

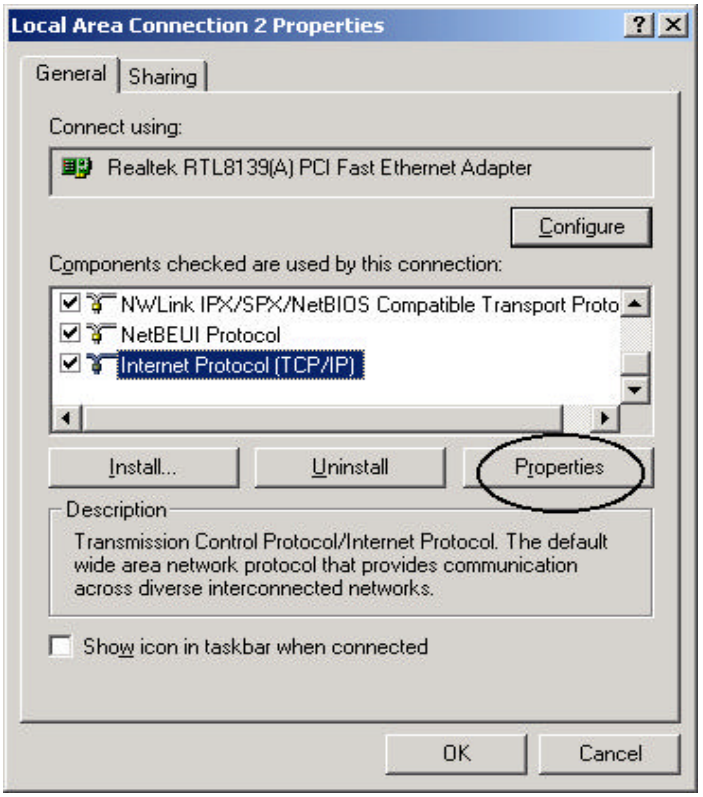
2. Double-click **LAN Area Connection**.



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

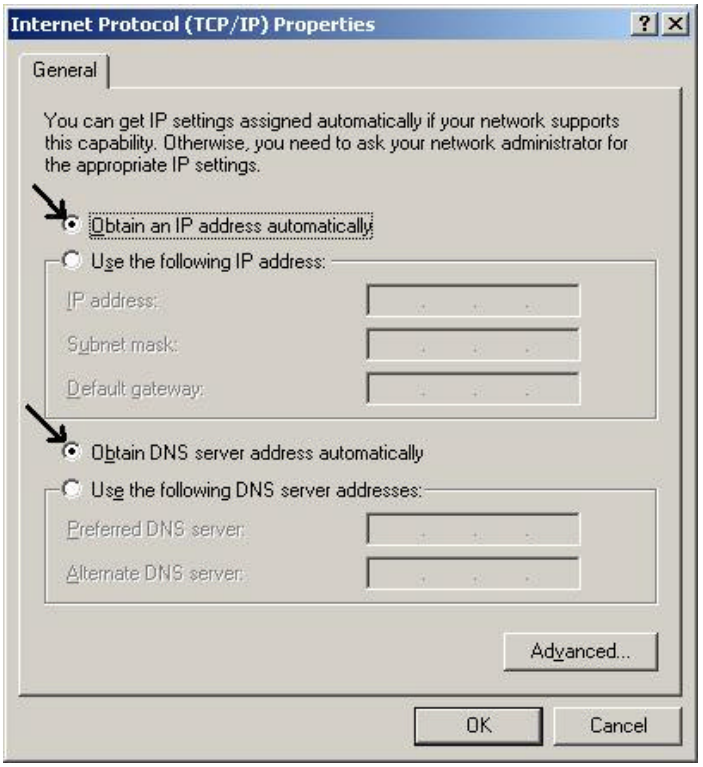


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.

6. Click OK to finish the configuration.

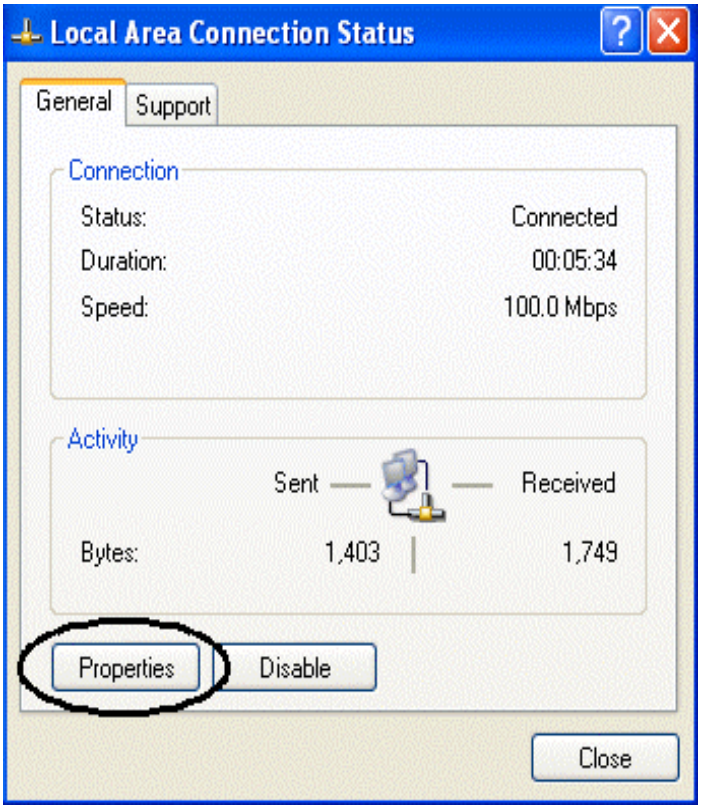


3.3.4 For Windows XP

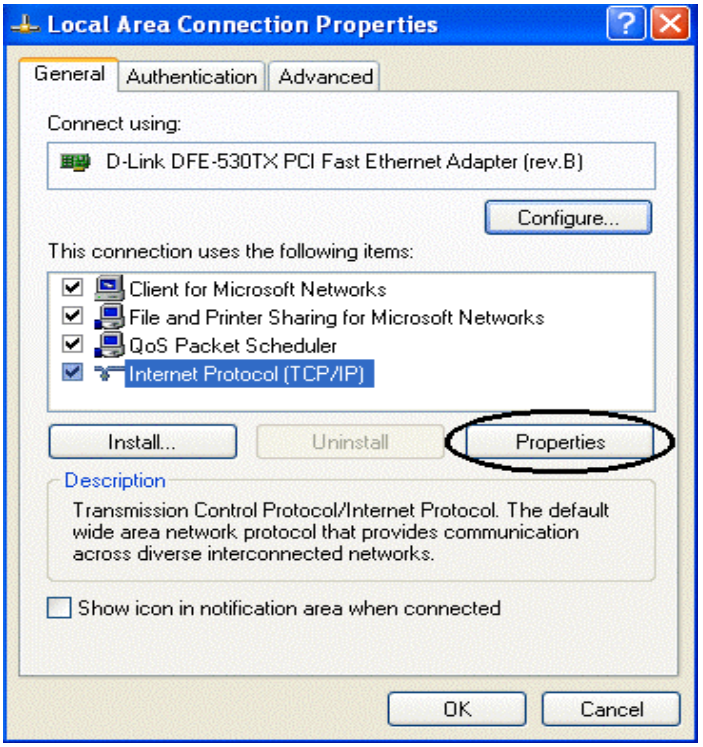
1. Go to Start / Control Panel (in Classic View). In the Control Panel, double-click on Network Connections.

2. Double-click Local Area Connection

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

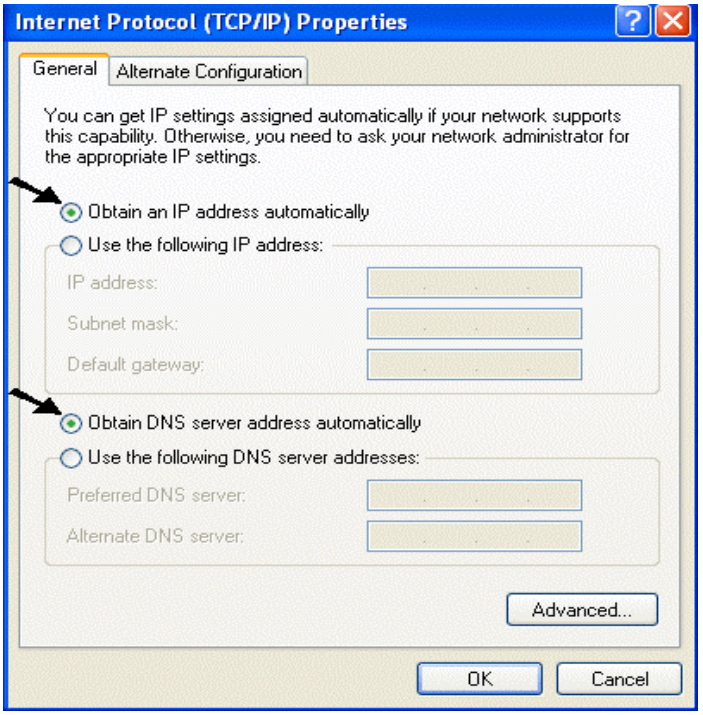


4. Select Internet Protocol (TCP/IP) and click Properties.



5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons

6. Click OK to finish the configuration.



3.4 Factory Default Settings

Before configurating this MICHELANGELO OFFICE PRO-V, you need to know the following default settings.

1. **Web Configurator**

   Username: admin

   Password : admin

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**

   PPPoE

4. **DHCP server**

   DHCP server is enabled.

   Start IP Address : 192.168.1.100

   IP pool counts : 100

3.4.1 Username and Password

The default username and password are admin and admin respectively.

If you ever forget the password to log in, you may press the RESET button to restore the factory default settings..

3.4.2 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	The PPPoE function is *enabled* to automatically get the WAN port configuration from the ISP, but you have to set the username and password first.
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 support up to 253 users.)	

3.5 Information from the ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) what kind of service is provided such as PPPoE, PPPoA, RFC1483, IPoA, or PPTP-to-PPPoA Relaying.

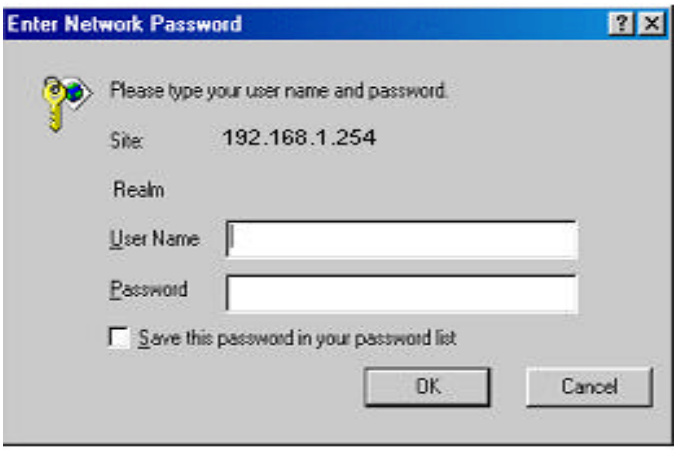
Gather the information as illustrated in the following table and keep it for reference.

PPPoE	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed).
PPPoA	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, and Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed).
RFC1483 Bridged	VPI/VCI, VC-based/LLC-based multiplexing and configure this product into BRIDGE Mode.
RFC1483 Routed	VPI/VCI, VC-based/LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).

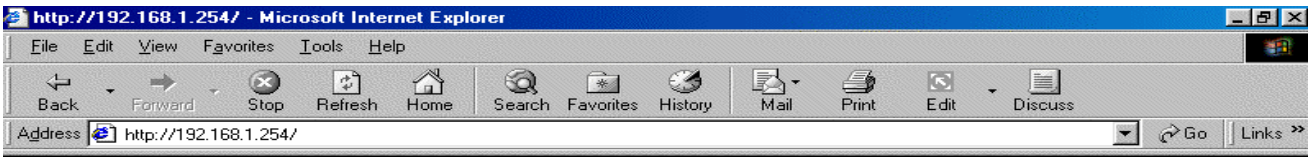
IPoA	VPI/VCI, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).

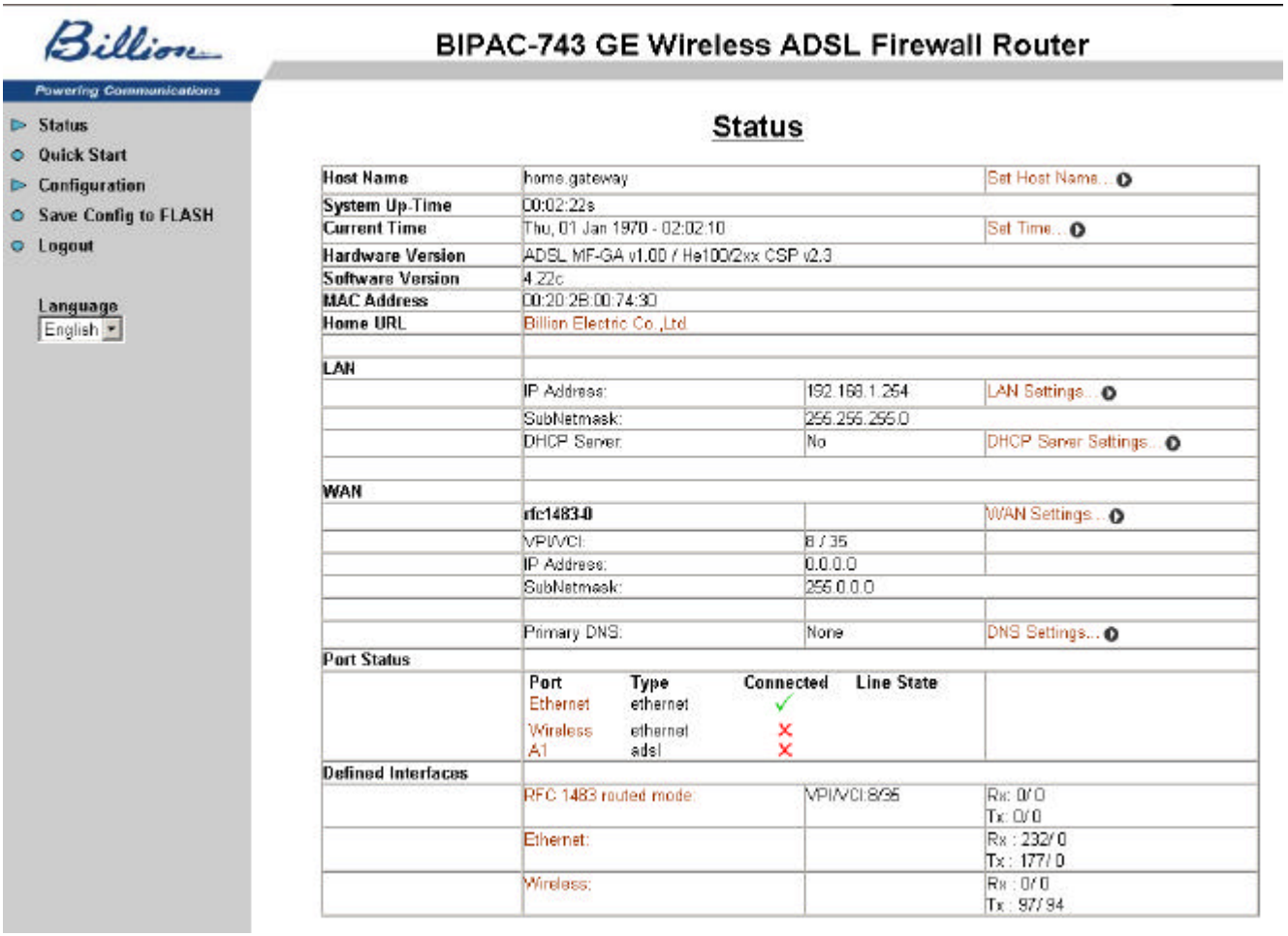
3.6 Configuring with the Web Browser

Open the web browser, enter the local port IP address of this MICHELANGELO OFFICE PRO-V , which defaults at **192.168.1.254**, and click "**Go**", a user name and password window prompt will appear. **The default username and password are admin and admin.**



You will get a status report web page when login successfully.





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

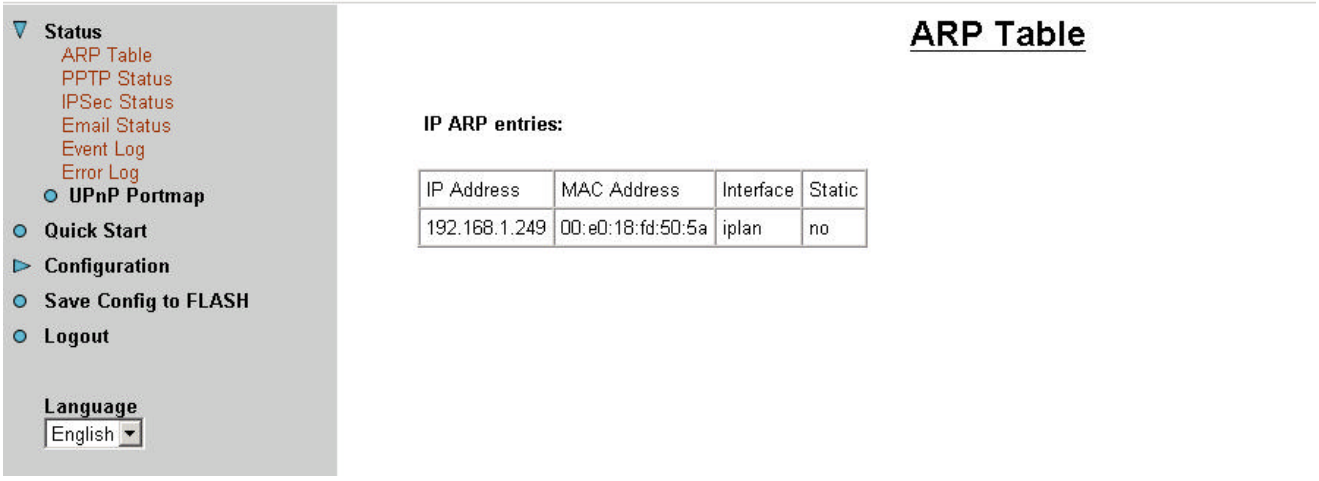
- **Status** (ARP Table, PPTP Status, IPSec Status, Email Status, Event Log, Error Log and UPnP Portmap)
- **Quick Start**
- **Configuration** (LAN, WAN, System, Firewall, VPN, Virtual Server & Advanced)
- **Save Config to FLASH**
- **Logout**
- **Language (**provides user interface in English language)

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

3.6.1 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.

When you click the **ARP Table,** you will see the data of the IP address of each PC in your LAN as well as its associated MAC address.



When you click the **PPTP Status**, it gives you a quick overview of the PPTP connection status.

When you click the **IPSec Status**, it gives you a quick overview of the IPSec connection status.

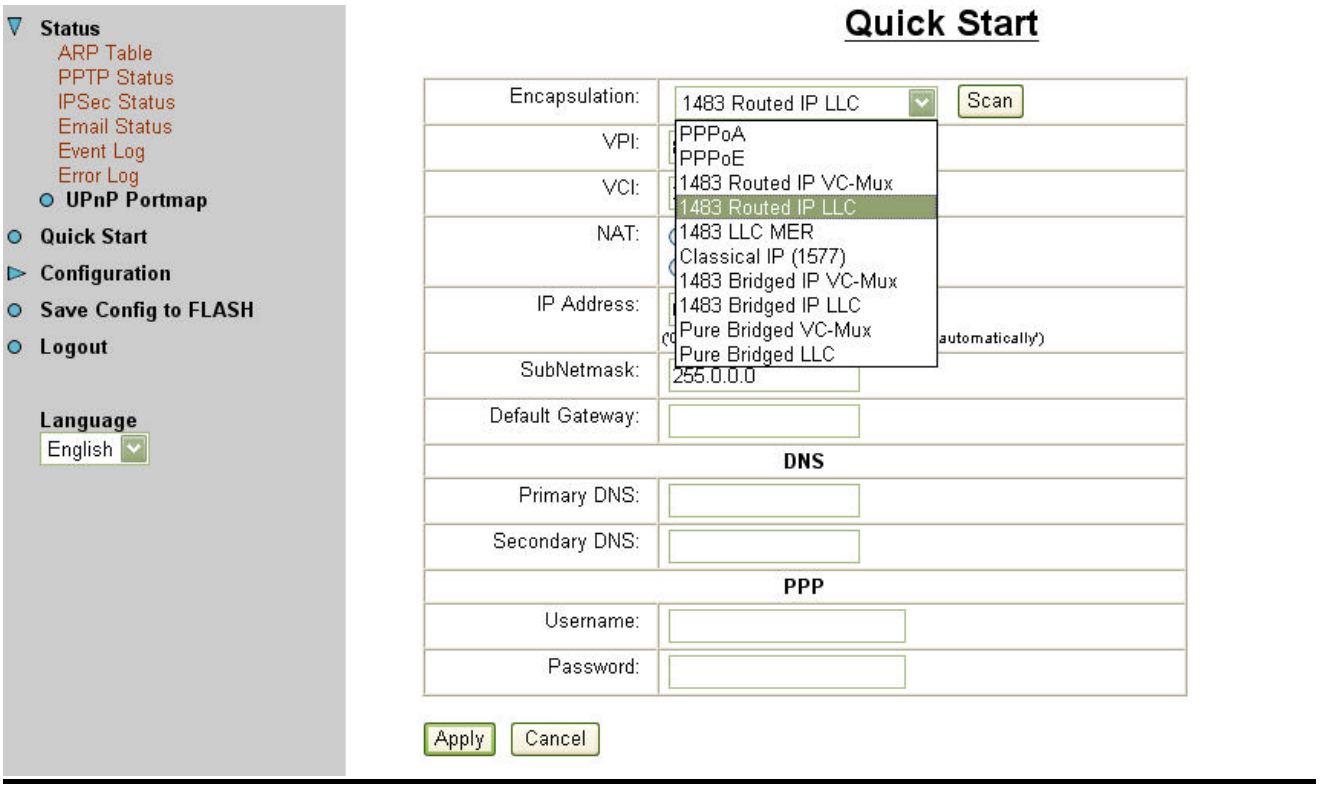
When you click the **Email Status**, it gives you a quick view to know if there is email in your pre-defined email account. You will see the unread emails in the email server once you have successfully configured the "Check Emails" in **Configuration → Advance.**

When you click the **Event Log**, it displays valuable system event logging information and status after the power is turned on, such as ADSL line, WAN port, SNTP, Firewall, and etc.

When you click the **Error Log**, it shows the error message log. When you face a problem, please send this error log to support for quick feedback.

When you click the **UPnP Portmap**, it displays the Virtual Servers (or Port Mappings) that created by UPnP protocol implemented in Windows.

3.6.2 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 3.5 (*Information from the ISP)*, then enter the proper values into this web page, click the **Apply** button and then **Save Config to FLASH** in the left panel. 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.

3.6.3 Configuration

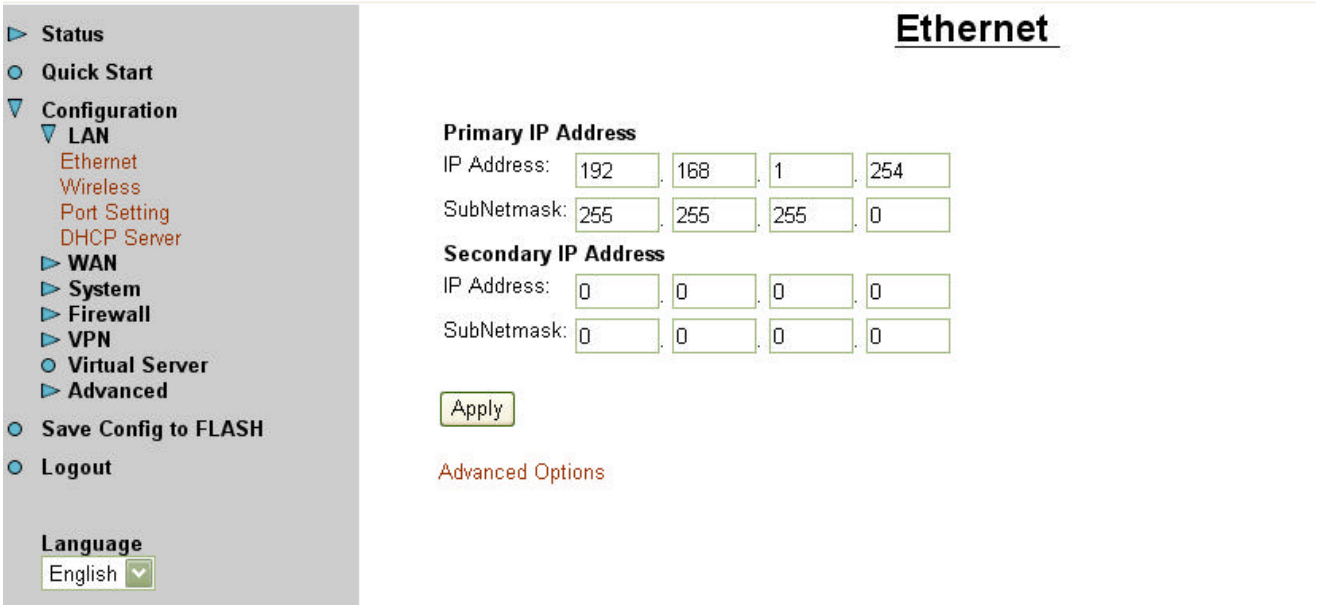
When you click this item, you get following sub-items to configure the ADSL router.

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

These functions are described below in the following sections.

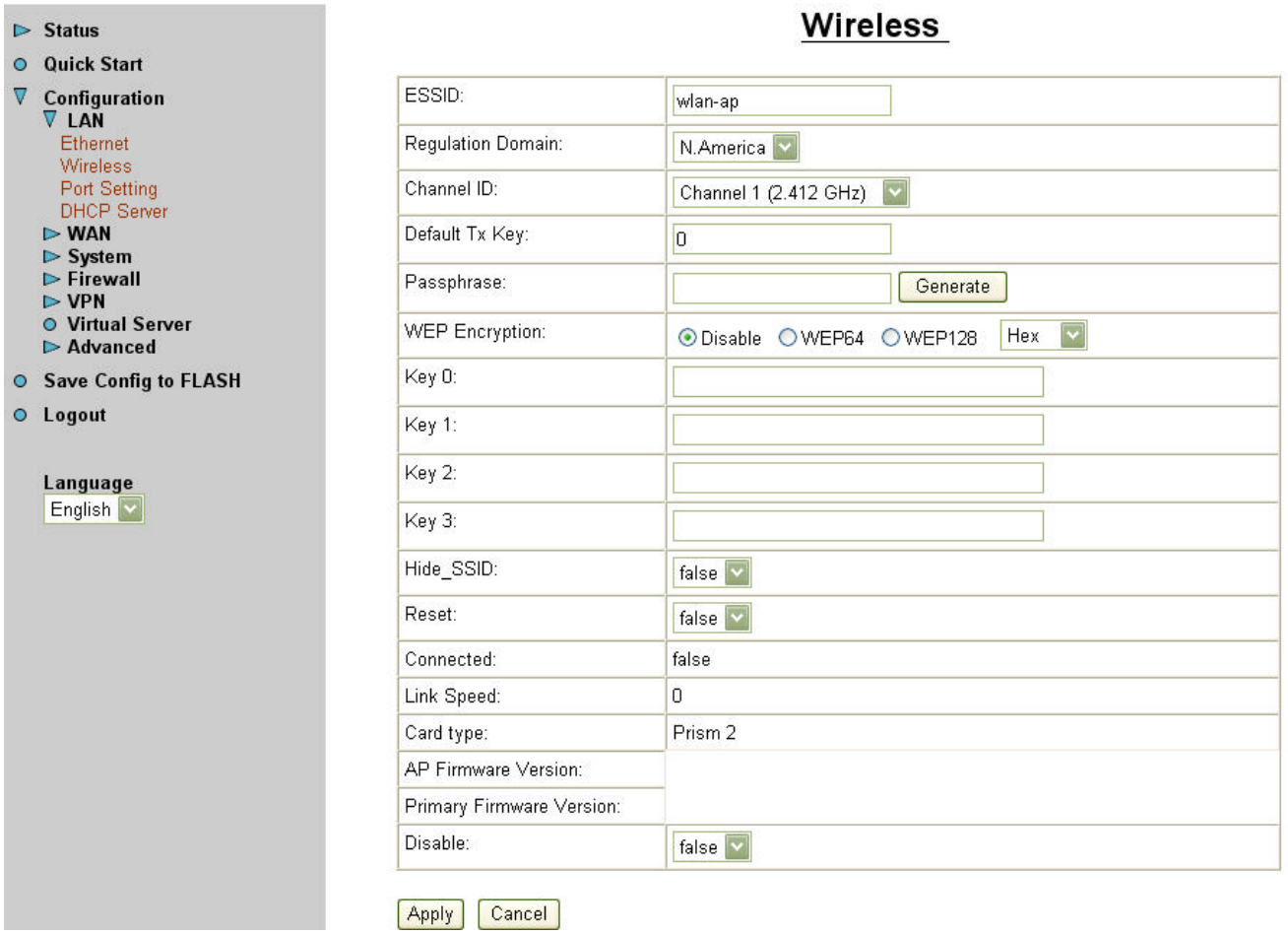
3.6.3.1 LAN

There are four items under the **LAN** section: **Ethernet, Wireless*, Port Setting** and **DHCP Server.** When you click **Ethernet**, you get the following figure.



It supports two Ethernet IP addresses in the LAN. With this function, the ADSL router can support two different LAN subnets to access the Internet at the same time. Usually, there is only one subnet in LAN, there is no need to configure a Secondary IP address. The 192.168.1.254 is the default IP address for this ADSL router. The **Advanced Options** will allow you to configure the routing protocol version1 or version 2 in receiving and sending direction.

When you click **Wireless***, you will get the following figure.



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

Regulation_ Domain: There are five Regulation Domains for you to choose from, including **North America (N.America)**, **Europe**, **France**, and **Spain**. The Channel ID will be different based on this setting.

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

Default Tx Key: Select the encryption key ID, please refer to **Key (0-3)** below.

Passphrase: This is used to generate WEP keys automatically by an input string and pre-defined algorithm in WEP64 or WEP128. You can input the same string in both AP and Client card to generate same WEP keys. Please note that you do not have to key in **Key (0-3)** as below when the **Passphrase** is enabled.

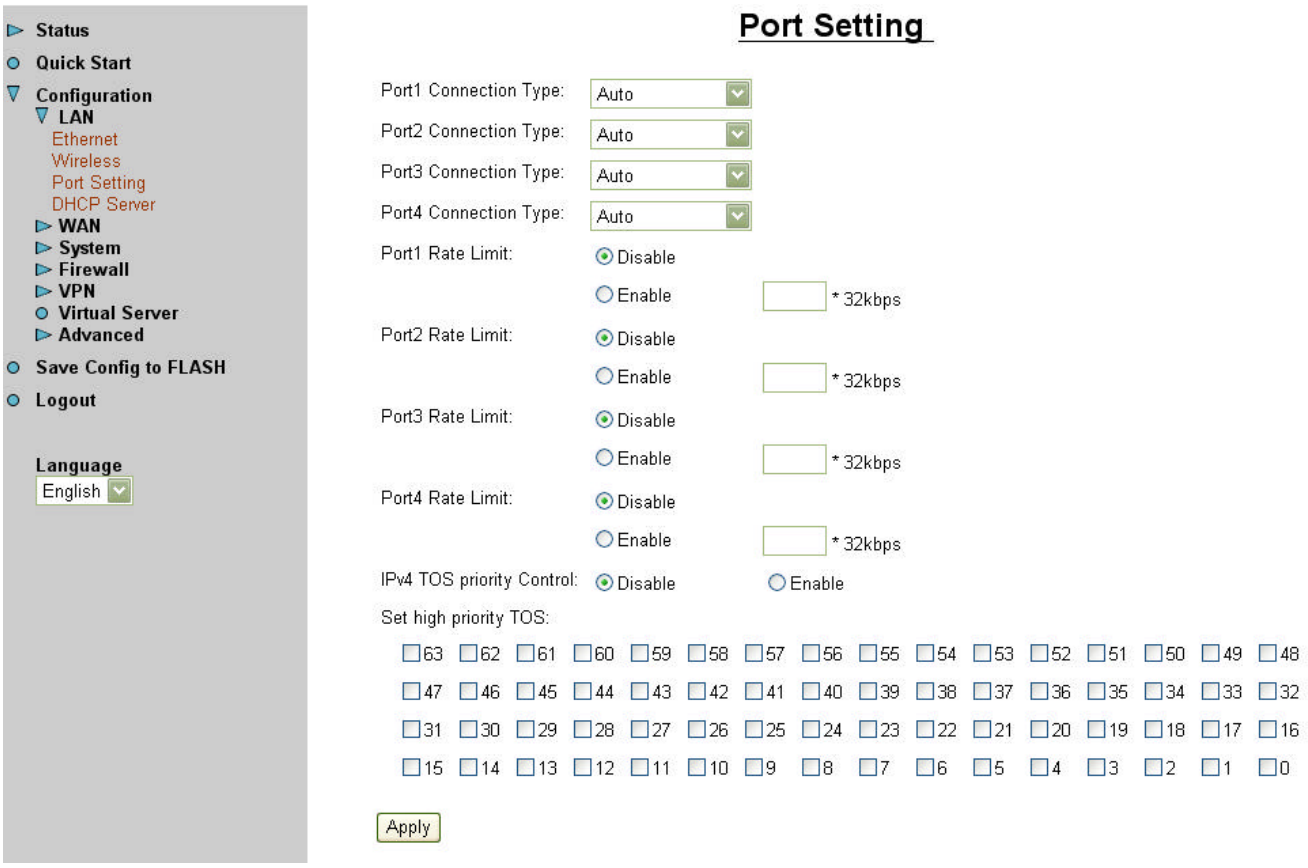
WEP Encryption: To prevent unauthorized wireless stations from accessing data transmitted over the network, the wireless broadband firewall gateway offers highly secure data encryption, known as WEP. If you require high security in transmission, there are two alternatives to select from, WEP 40 and WEP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

Key (0-3): 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 the device. There are four keys for your selection. The input format is in HEX style, 5 and 13 HEX codes are required for WEP64 and WEP128 respectively, the separator is "-". Take WEP64 case for example, 11-22-33-44-55 is a valid key, 1122334455 is invalid instead.

Hide_SSID: When enabled, the Wireless AP is invisible from the site-surveying by Wireless clients. The wireless clients still can associate with this Wireless AP if entered with the same ESSID value.

Reset: Reset the Wireless AP function

When you click **Port Setting**, you get the following figure. This allows you to configure the port setting to solve some of the compatibility problems while connecting to the Internet.



Port # Connection Type: Five options to choose from: auto, 10M half-duplex, 10M full-duplex, 100M half-duplex or 100M full-duplex. Sometimes, there are Ethernet compatibility problems with legacy Ethernet devices. You can configure different types to solve the compatibility issues.

Port # Rate Limit: When it is enabled, enter a rate value that is configured as multiple of 32kbps. This function limits the inbound and outbound Ethernet throughput around the value that you specified.

TOS, Type of Services, is the 2nd octet of IP packet. The bits 6-7 of this octet are reserved and bit 0-5 are used to specify the priority of the packet. The definition of these bits is listed blow:

Two bits: reserved

One bit: high reliability

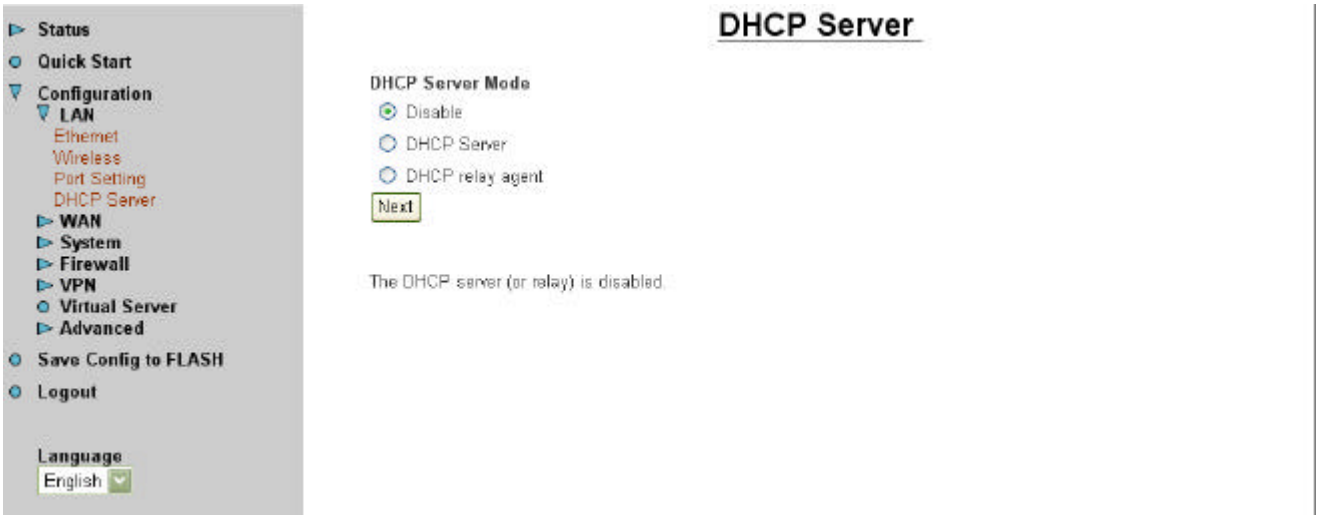
One bit: high throughput

One bit: No delay

Three bits: IP priority (0 to 7)

IPv4 TOS priority Control: This feature uses bits 0-5 to classify the packets' priority. If the packet is in high priority, it will flow first and will not be constrained by the Rate Limit. Therefore, when this feature is enabled, the embedded Ethernet switch IC will check the 2nd octet of each IP packet. If the value in the TOS field matches in the checked values in the table (0 to 63), this packet will treat it as high priority.

When you click **DHCP Server**, you get the following figure. You can disable or enable the DHCP server or enable the DHCP relay functions.



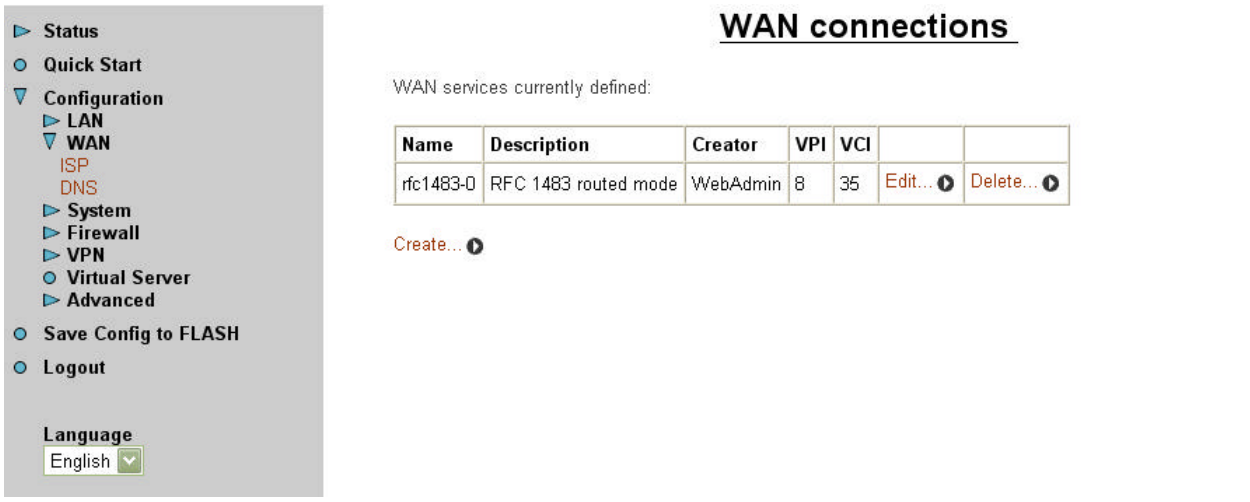
If you check **Disabled** and click **Next,** then click **Apply.** The DHCP server function is disabled. Each PC in the LAN should assign a fixed IP address and set the PC's gateway to the ADSL router.

If you check **DHCP Server** and click **Next**, you can configure parameters of the DHCP server including the IP pool (starting IP address and ending IP address), leased time for each assigned IP address, DNS IP address, Gateway IP address. Those messages are sent to the DHCP client when it requests an IP address from the DHCP server. Click **Apply** to enable this function. If you check "**Use Router as a DNS Server**", the ADSL Router will find the IP address from the outside network automatically and forward it back to requesting PC in the LAN.

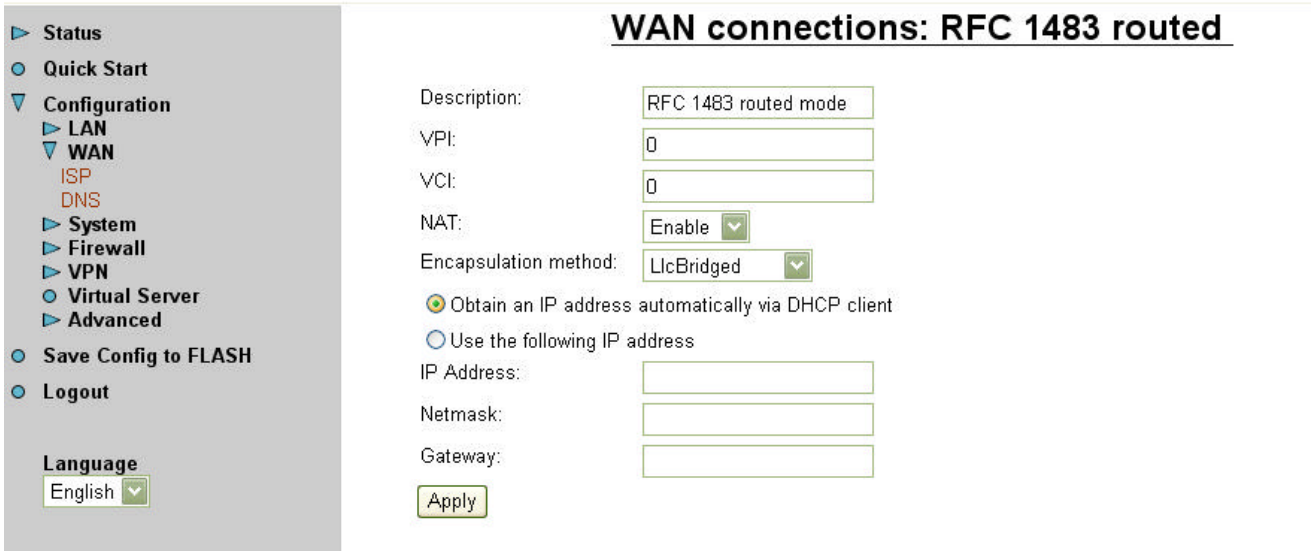
If you check **DHCP Relay Agent** and click **Next**, then you will have to enter the IP address of the DHCP server which will assign an IP address back to the DHCP client in the LAN. Click **Apply** to enable this function.

3.6.3.2 WAN

There are items under the **WAN** section: **ISP** and **DNS.** When you click **ISP**, you will get the following screen.



The factory default is **rfc 1483-0**. If your ISP uses the same access protocol, please click **Edit** to input other parameters as below. If your ISP does not use rfc 1483-0, you can delete it, click **Delete**. Then you may click **Create** to create a connection to your ISP to surf the Internet. Refer to the figure after the **RFC 1483 routed** and **PPPoE** description below.



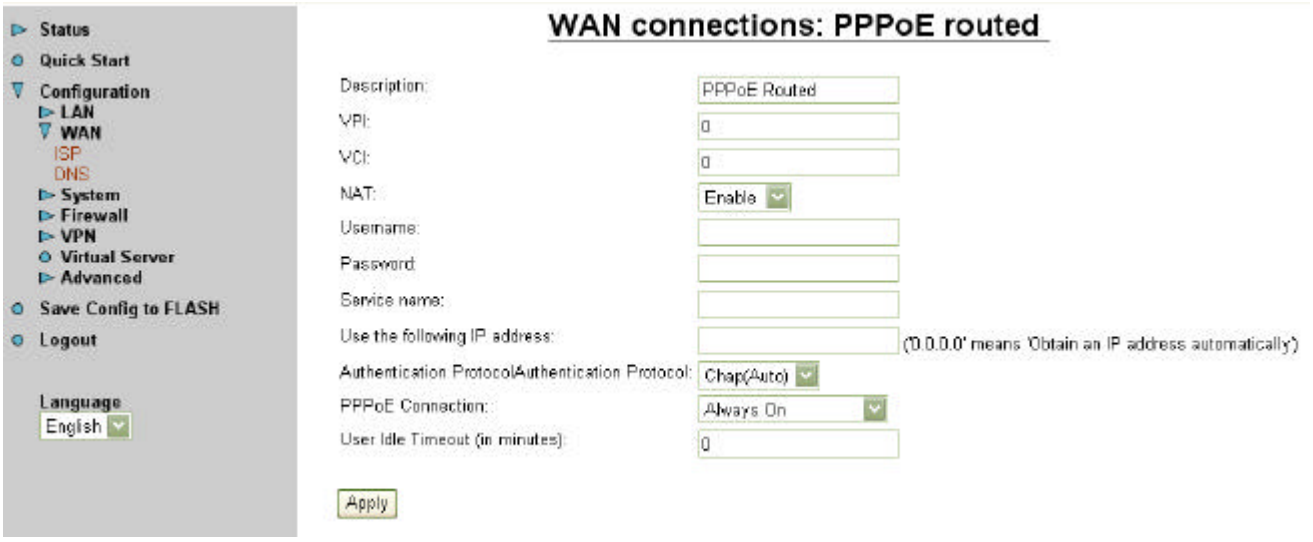
Description: Give a name for this connection.

VPI and VCI: Enter the information provided by your ISP.

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

Encapsulation method: Select the protocol format, the default is LlcBridged. Select the one provided by your ISP.

DHCP client: Enable or disable the DHCP client, specify if the Router can get an IP address from the Internet Server Provider (ISP) automatically or not. Please click Obtain an IP address automatically via DHCP client to enable the DHCP client function or click Specify an IP address to disable the DHCP client function, and specify the IP address manually. The setting of this item is specified by your ISP.



Description: Give a name for this connection.

VPI/VCI: Enter the information provided by your ISP.

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

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).

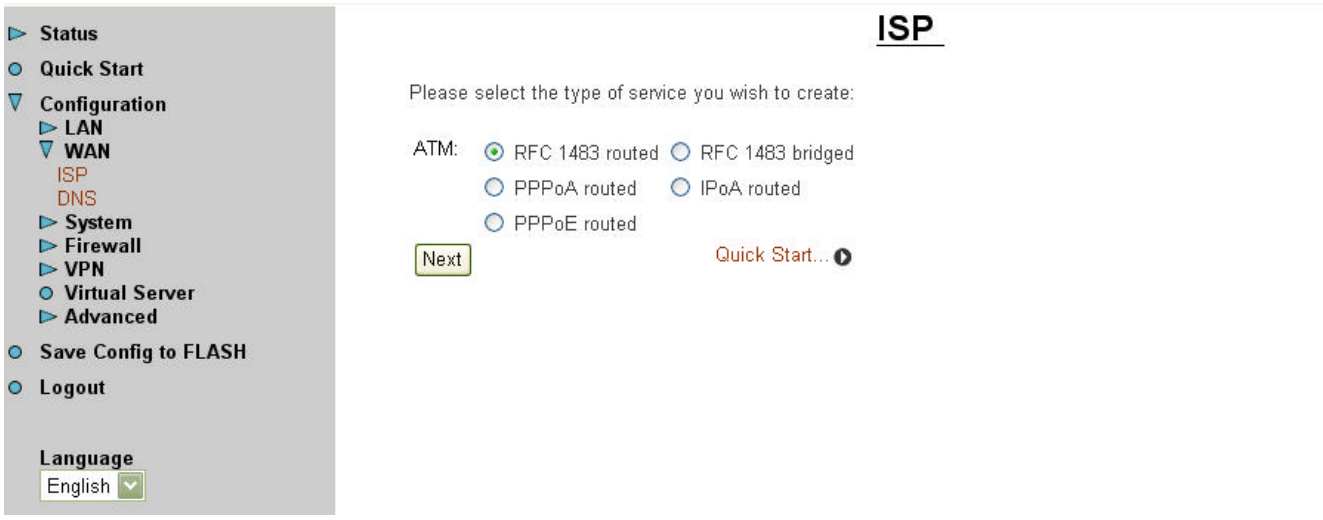
Service Name: This item is for identification purpose. If it is required, your ISP will provide you the information. Maximum input is **20** alphanumeric characters.

PPP Authentication Protocol Type: Default is **Auto**.

⊙ **Always on:** if you want to establish a PPPoE session when starting up. It will also automatically re-establish the PPPoE session when disconnected by the ISP.

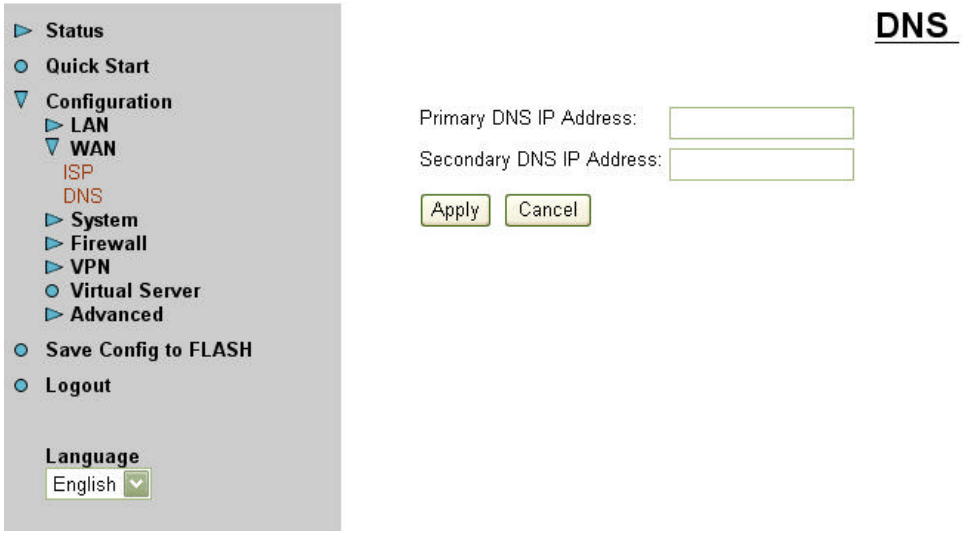
⊙ **Connect to Demand:** if you want to establish a PPPoE session only when there is a packet requesting access to the Internet.

User Idle Timeout (in minutes): Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.



Select one of the access methods among the 5 listed items and click **Next** to configure the right connection method. Please refer to the above description and Section 3.5 Information from ISP.
Quick Start... is a short cut to the Quick Start page.

The WAN-DNS is shown as below.



A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. In the Internet, every host has a unique and friendly name such as www.yahoo.com and an IP address. As the IP Address is hard to remember, the DNS converts the friendly name into its equivalent IP Address.

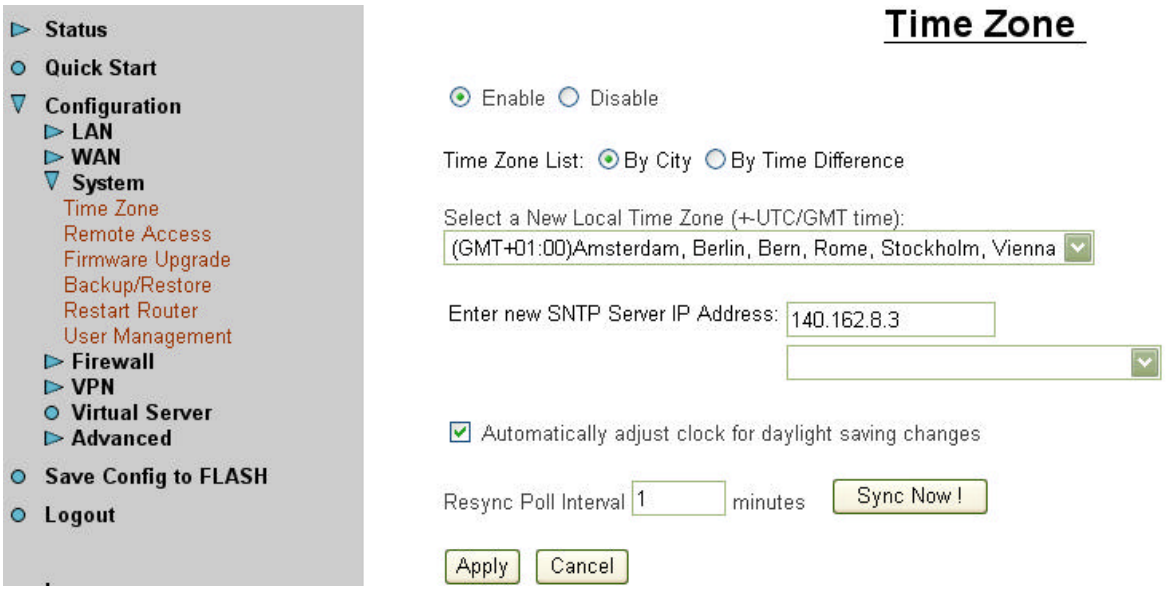
You can obtain a Domain Name System (DNS) IP address automatically if your ISP has provided it when you logon. Usually when you choose PPPoE or PPPoA as your WAN - ISP protocol, the ISP will provide the DNS IP address automatically. You may leave it as blank. Or your ISP may provide you with an IP address of their DNS. If this is the case, you must enter the DNS IP address.

If you choose one of the other three protocols - RFC1483 routed /bridged and IPoA. Check with your ISP, it may provide you with an IP address of DNS. You must enter the DNS IP address if you set the DNS of your PC to the LAN IP address of this router.

3.6.3.3 System

There are six items under the **System** section: **Time Zone, Remote Access, Firmware Upgrade, Backup/Restore, Restart Router** and **User Management.**

When you click **Time Zone**, you get the following figure.



The router 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 from the outside network. Please choose your local time zone, click **Enable** and click the **Apply** button. You will get the correct time information after you ready establish a connection to the Internet. If you prefer to enter your own SNTP server, please enter and use it as the first choice.

Resync Poll Interval (in minutes) is the periodical interval of router's SNTP client to update (or re-synchronize) the current time with SNTP server after it synchronized with SNTP server.

When you click **Remote Access** and then click **Enable**, you may temporarily permit remote administration of the MICHELANGELO OFFICE PRO-V .

When you click **Firmware Upgrade**, it allows you to input the location of firmware stored on your PC and click the Upgrade button to upgrade to the new firmware.

When you click **Backup/Restore,** it allows you to save your current settings into a file on your PC. If you like to restore it back (input the location of this configuration file in the PC and click the **Restore** button to save it back).

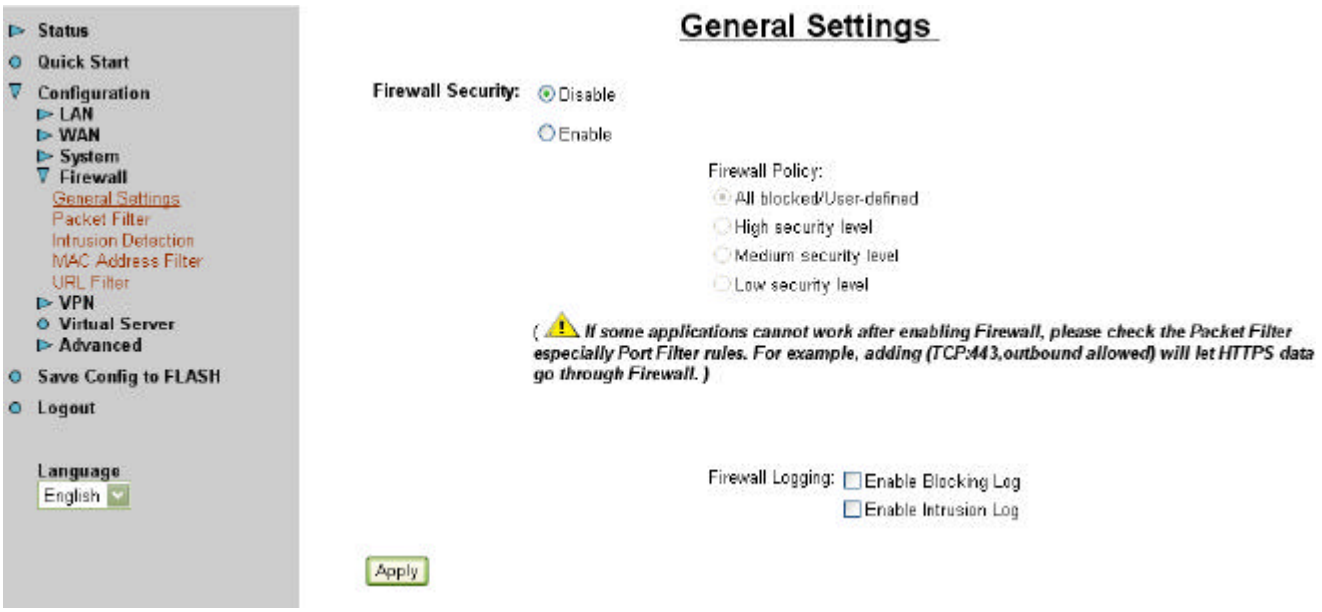
When you click **Restart Router**, you have two functions. One is to restart it with current settings and the other is to restart it with factory default settings if you check **Reset to factory default settings**.

When you click **User Management**, you are able to edit existing user's database or to create other user accessing this device.

3.6.3.4 Firewall

There are five items under the **Firewall** section: **General Settings, Packet Filter, Intrusion Detection, MAC Address Filter** and **URL Filter**.

When you click **General Settings**, you get the following figure.



Firewall: When you enable the Firewall function, you can select one of the firewall security policies. By default the firewall is set to disabled.

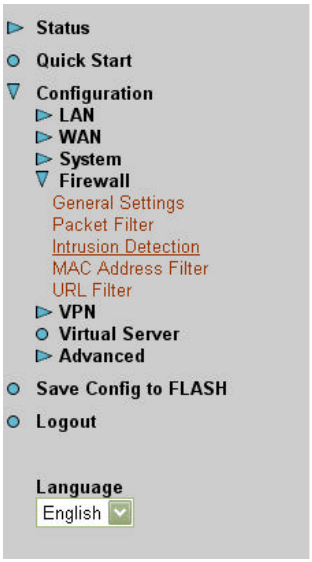
All blocked/User-defined: By default, all traffic between WAN and LAN are blocked. You have to configure the type of traffic passed between WAN and LAN, please refer to Packet Filter below.

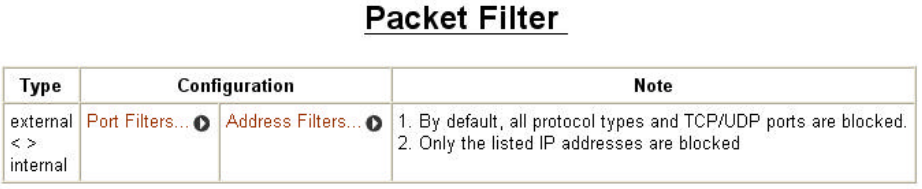
High, Medium and Low security level: By default, your system uses High, Medium and Low firewall security levels between the WAN and LAN. For example, when you select High, the Port Filters of the Packet Filter screen will be set automatically according to High security level settings.

Firewall Logging: When both the Firewall Security and Firewall Logging are enabled, the device will detect the blocked and/or intrusion packets, once the setting has been configured. Then the router will log the corresponding (blocking or intrusion detection) logs into the Event Log under Status.

Select the **Apply** button to save the setting.

When you click **Packet Filter**, you get the following figure.





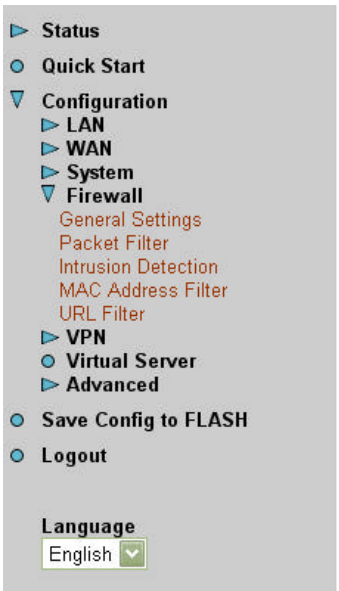
You may configure to filter inbound (incoming) and outbound (outgoing) packets based on PORT or IP address.

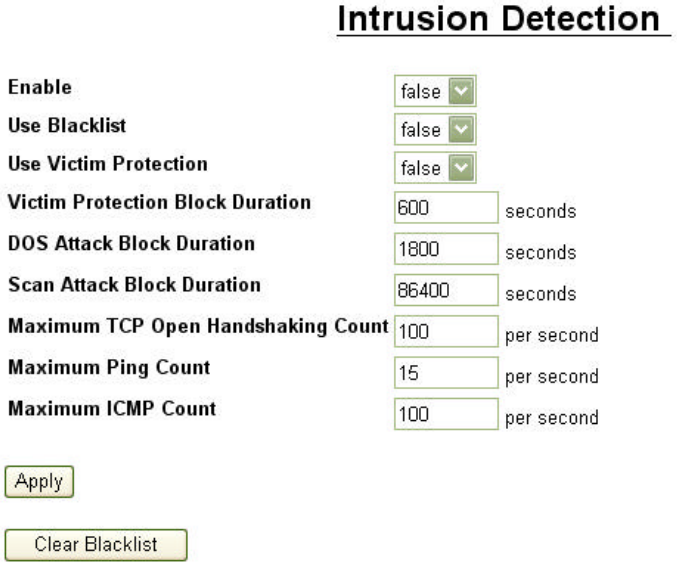
If it is based on PORT, click Port Filters for more options. You may filter the packets based on PORT and packet type (TCP or UDP or any). For example, the protocol number 1 means ICMP. You may enter 1 to protocol number of Raw IP Filtering web page. Port ranges are supported.

If it is based on IP address, click Address Filters for more options. You may enter the IP address and again to select the inbound or outbound packets.

For example, to allow TCP packet, port 0 to 1000 passing router between WAN and LAN and blocks host IP address, 192.168.1.100. Then you have to configure the port filter → add TCP filter > 0 to 1000 and ALLOW in both direction. Then click address filter → add address filter → enter host IP 192.168.1.100, subnet mask 255.255.255.255 (for this single host) and both direction.

When you click **Intrusion Detection**, you get the following figure.





Enable: Set True to enable this Intrusion detection.

Use BlackList: Set True to use router's default backlist to protect router.

Use Victim Protection: Set True to enable Victim protection.

Victim Protection Duration: Input numbers.

DoS Block Duration: Input numbers.

Scan Block Duration: Input number.

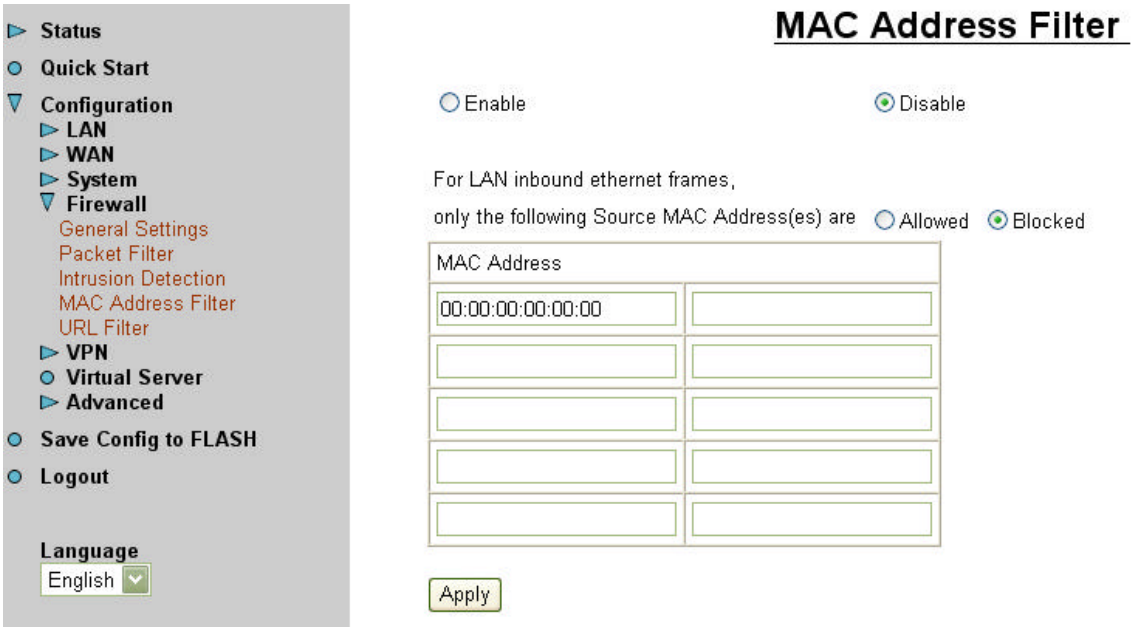
Maximum TCP Open Handshaking Count: Input numbers.

Maximum Ping Count: Input numbers

Maximum ICMP Count: Input numbers

Select the **Apply** button to save the setting.

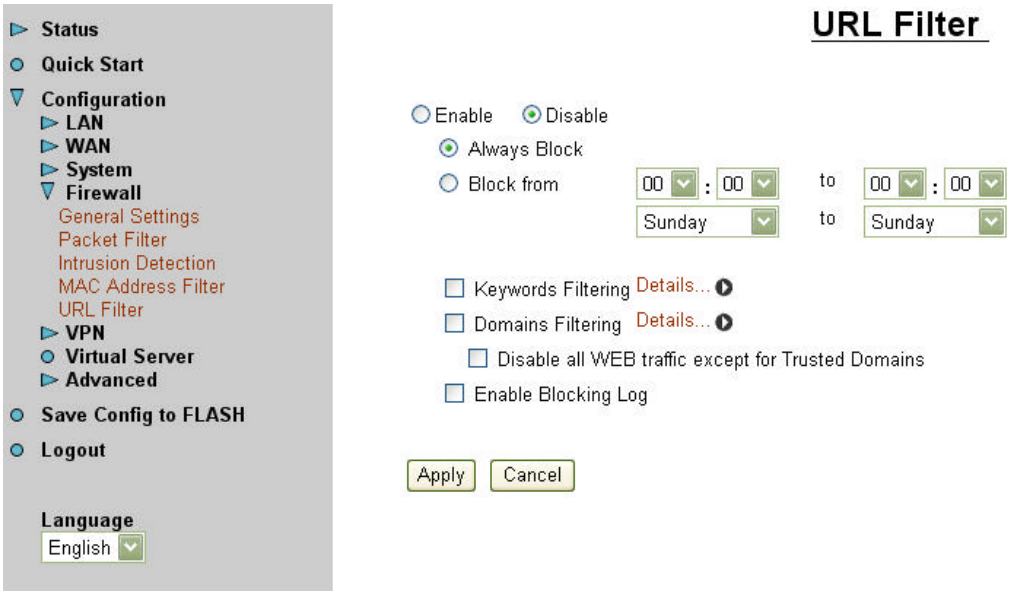
When you click the **MAC Address Filter**, you get the following figure.



The MAC filtering function enables you to configure your router to block internal users (**MAC address**) from Internet access.

⊙ **Enable / Disable:** Check **Enable / Disable** radio button to active / disable, respectively, the MAC address filter function. If you check **Enable,** remember to choose either **Allowed** or **Blocked** the MAC Address listed in the table, as shown above. If you select **Blocked**, the packet with the MAC address in the table will be dropped and others will be forwarded. If you select **Allowed**, the packet with the MAC address in the table will be forwarded and others will be dropped. Then select the **Apply** button to save the setting.

When you click the **URL Filter**, you get the following figure.



The URL filtering function enables you to block unwanted websites from accessing inappropriate material from the entire enterprise.

⊙ **Enable / Disable:** Check **Enable / Disable** radio button to active / disable, respectively the URL filter function.

⊙ **Always Block:** Check this button, if you wish not to access this website through out the entire time. Or choose,

⊙ **Block from:** 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.**

Keyword Filtering: Check if you want to enable the Keyword Filtering function and click Details... button for further configuration options. Please refer below for more information.

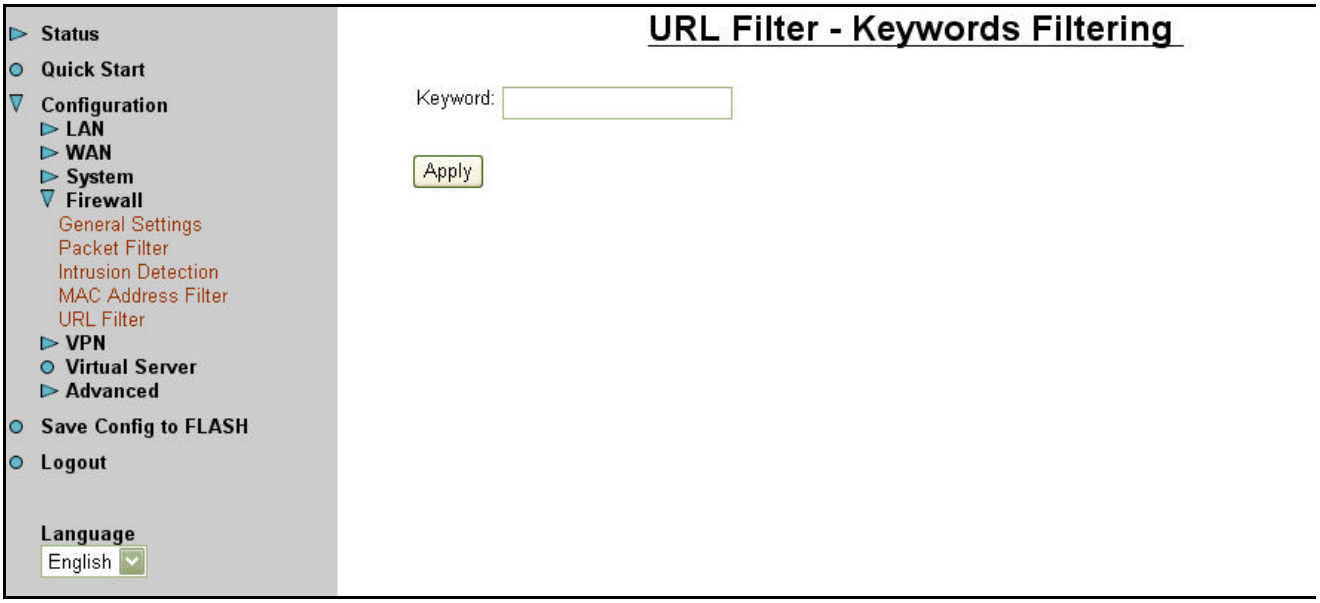
Domain Filtering: Check if you want to enable the Domain Filtering function and click button Details... for further configuration options. Please refer below for more information.

Disable All WEB traffic except for Trusted Domain: It allows internal users to access only the specified/trusted domain. Please refer to the Domain Filtering section first, before checking this option.

Enable Blocking Log: Check this button to log the corresponding logs into the Event Log under Status.

Select the **Apply** button to save the setting.

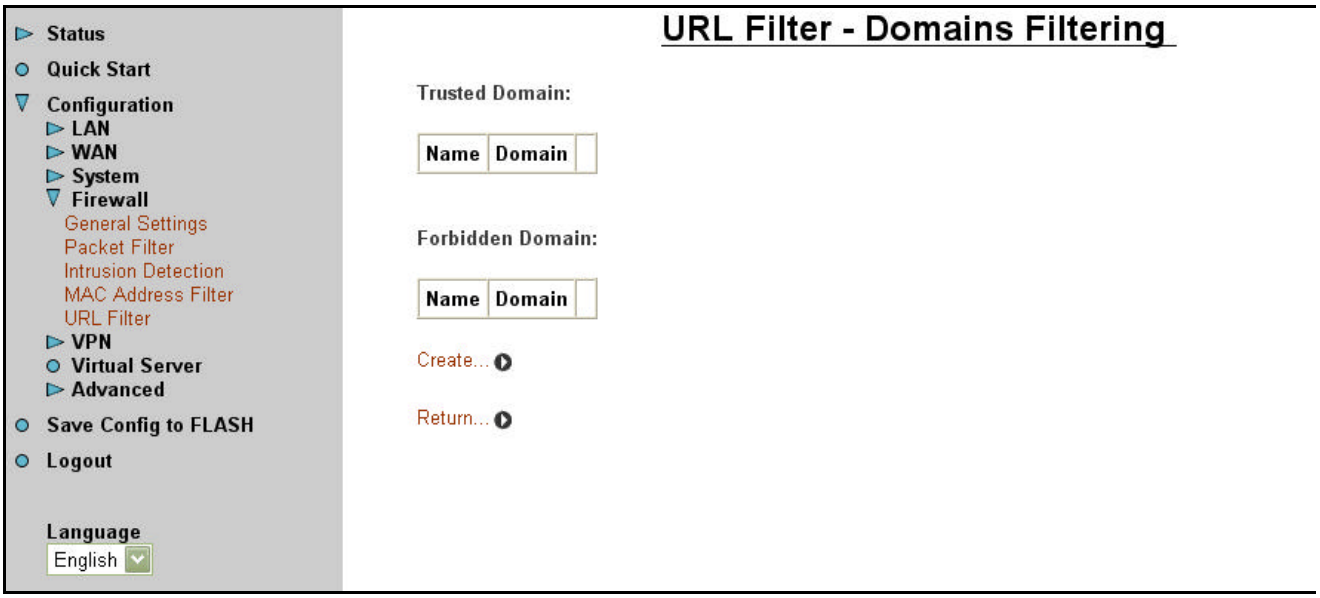
Keyword Filtering:



The ADSL 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 can not be accessed from the LAN.

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

Domain Filtering:



If the router is configured to allow internal users to access only certain specified domains, check add the domain name into the **Trusted Domain** list. If the router is configured to allow internal users to access all websites except for some forbidden domains, add the forbidden domain name into the **Forbidden Domain** list. These Forbidden Domains will be blocked, and 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 select either **Trusted Domain** or **Forbidden Domain,** then click **Apply**. The specified domain will be shown in the **Domain List**. DO NOT include **http://**, ONLY the sub-domain is 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.

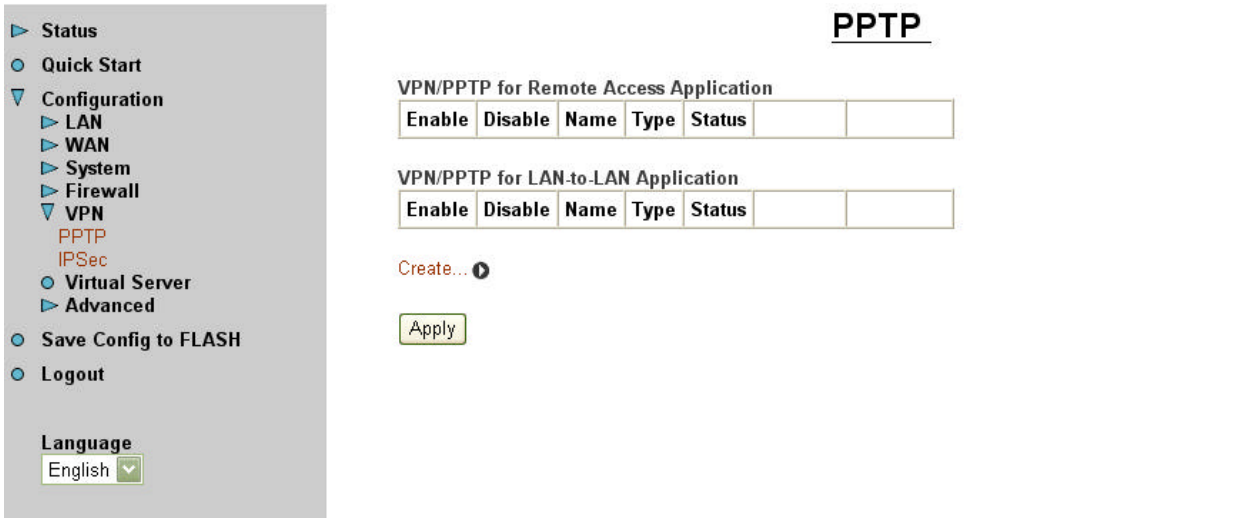
To remove a site that was previously added, select its name in the list box, and click the **Delete** button to eliminate it from the list.

3.6.3.5 VPN

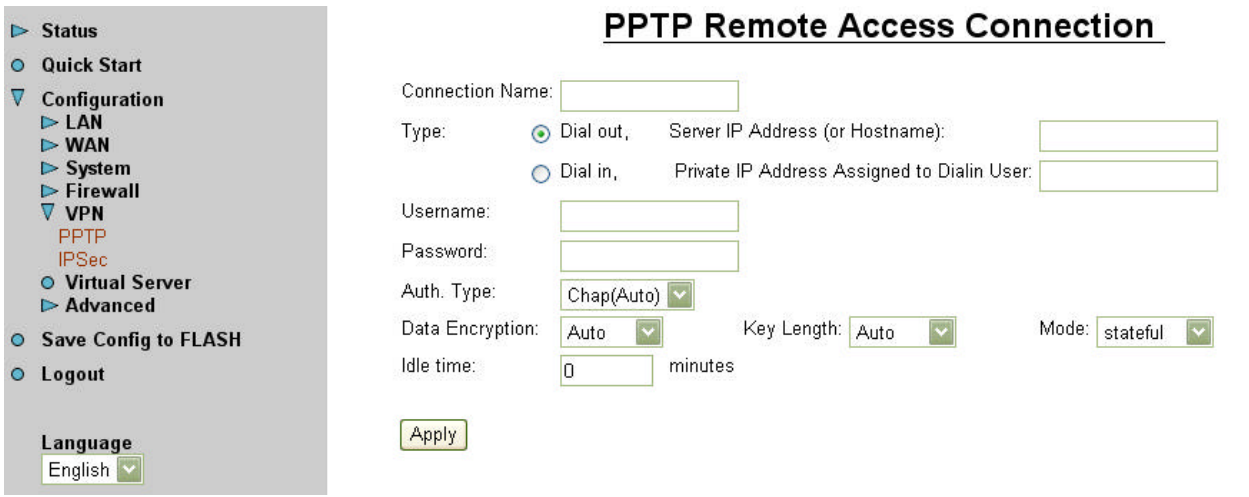
There are two items under **VPN** section, **PPTP** and **IPSec**.

When you click **PPTP**, you get the following figure.

There are two applications provided in PPP, **Remote Access** and **LAN-to-LAN** (please refer below for more information.). Click **Create** to select one of applications to continually setup.



For the Remote Access Application, please refer to the figure below.



Connection Name: Give a name for this connection.

Type: Check **Dial Out** to be a client, check **Dial In** to be a server. When this network router acts as a client, please input the remote **Server IP Address (or Hostname)** to establish a connection.

When this network router acts as a server, please input the **Private IP Address Assigned to Dial in User** address.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.

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

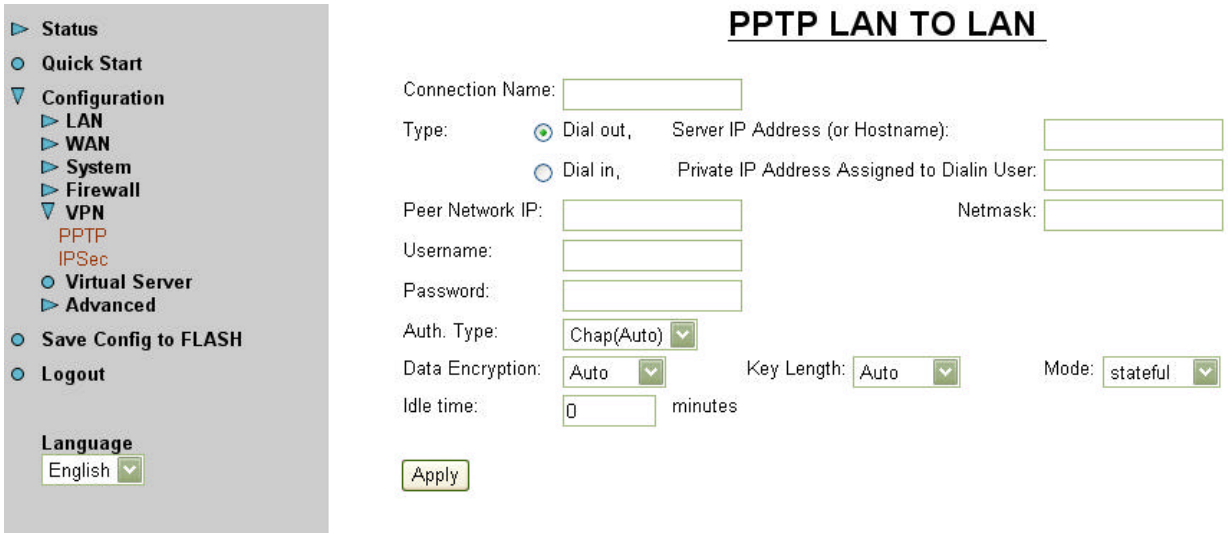
Data Encryption: The data can be encrypted by MPPE algorithm. Default is **Auto,** it is negotiated when establishing a connection.

Key Length: The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is **Auto**, it is negotiated when establishing a connection.

Mode: You may select **Stateful** or **Stateless** mode. The key will be changed in each 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.

Idle Time: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. 0 means this connection is always on.

Click **Apply** after setting.



Connection Name: Give a name for this connection.

Type: Check **Dial Out** to be a client, check **Dial In** to be a server. When this network router acts as a client, please input the remote **Server IP Address (or Hostname)** to establish a connection. When this network router acts as a server, please input the **Private IP Address Assigned to Dial in User** address.

Peer Network IP: Enter Peer network IP address.

Netmask: Enter the subnet mask of peer network based on above Peer Network IP setting.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by the your Host. If you are a Dial-In user (server), enter your own password.

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

Data Encryption: The data can be encrypted by MPPE algorithm. Default is **Auto,** it is negotiated when establishing a connection.

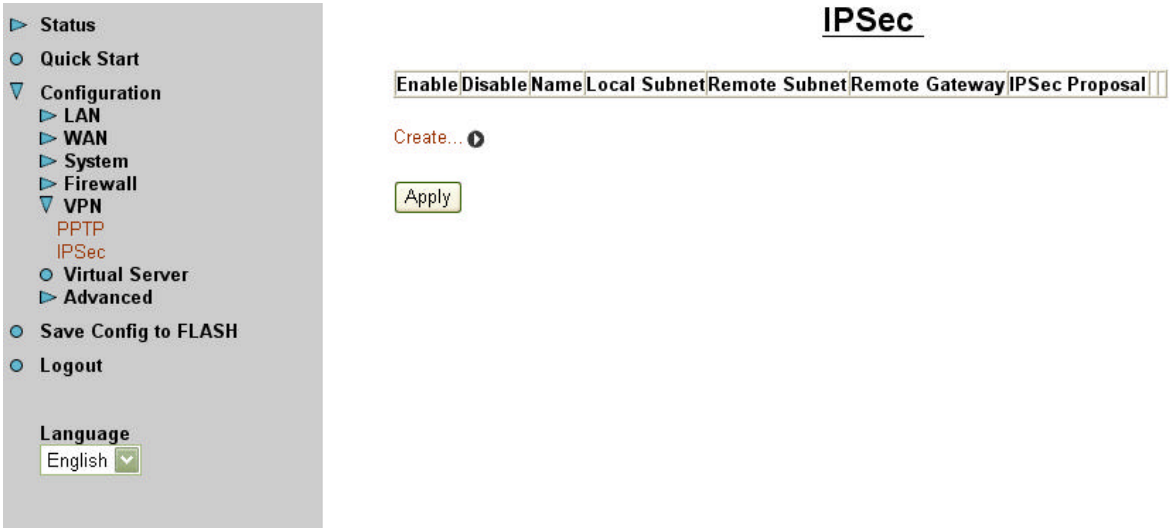
Key Length: The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is **Auto**, it is negotiated when establish a connection.

Mode: You may select **Stateful** or **Stateless** mode. The key will be changed in each 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.

Idle Time: Auto-disconnect the ADSL router when there is no activity on the line for a predetermined period of time. 0 means this connection is always on.

Click **Apply** after setting.

When you click **IPSec**, you get the following figure.



Click **Create…**

Connection Name: Give a name for this connection.

Local:

Local Network: Set the IP address, subnet or address range of the local network.

⊙ **Single Address:** The IP address of the local host.

⊙ **Subnet:** The subnet of the local network. For example, IP: 192.168.1.0 with netmask 255.255.255.0 specifies one class C subnet starting from 192.168.1.1.

⊙ **IP Range:** The IP address range of the local network. For example, IP: 192.168.1.1, end IP: 192.168.1.10

Remote:

Secure Gateway Address (or hostname): The IP address or hostname of remote VPN device that is connected and establishes a VPN tunnel.

Network: Set the IP address, subnet or address range of the remote network.

Proposal:

Proposal: Select the IPSec security method. Check ESP for a higher security, data will be encrypted and authenticated. Check AH, data will be authenticated but not encrypted.

Authentication: There are three options, MD5, SHA1 or NONE. Authenticate the data using MD5, SHA1 or NONE.

Encryption: Select the encryption method. The DES uses 56 bits as an encryption method. The 3DES uses 168 (56*3) bits as an encryption method. The AES uses 128 bits as an encryption method. The NONE means it is a tunnel only, no encryption.

Perfect Forward Secrecy: Enable this to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time.

Pre-shared Key: This is a string from 4 characters to 128 characters. Both sides should use the same key.

Select the **Save** button to save the setting.

Click **Advanced Option** to get the following figure.

SA Lifetime: Specify the number of minutes that a VPN tunnel will stay active before new encryption and authentication key will be exchanged. The SA Lifetime may range from 10 to 10,000 minutes.

Phase 1 (IKE): To issue an initial connection request for a new VPN tunnel. Default 240 minutes, range from 5 to 15,000 minutes.

Phase 2 (IPSec): To negotiate and establish secure authentication. Default 60 minutes, range from 5 to 15,000 minutes.

Select the **Change** button to update the setting.

3.6.3.6 Virtual Server

When you click Virtual Server, you get the following figure.

Virtual Server

Enable	Application	Protocol	Port	IP Address
☐	FTP	TCP	21	192.168.1.
☐	Telnet	TCP	23	192.168.1.
☐	SMTP	TCP	25	192.168.1.
☐	HTTP	TCP	80	192.168.1.
☐	POP3	TCP	110	192.168.1.
☐	NNTP	TCP	119	192.168.1.
☐	NTP	UDP	123	192.168.1.
☐	HTTPS	TCP	443	192.168.1.
☐	IKE	UDP	500	192.168.1.
☐	T.120	TCP	1503	192.168.1.

Being a natural Internet firewall, this network router 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 modem can act as a virtual server. You can set up a local server with specific a port number that stands for the service, e.g. Web (80), FTP (21), Telnet (23), SMTP (25), POP3 (110), When an incoming access request to the router for a 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 from outside users will be forwarded to the local server with IP address of 192.168.1.2. If the port is not listed as a predefined application, you need to add it manually.

DMZ: The DMZ Host is a local computer exposed to the Internet. Therefore, an incoming packet will be checked by the Firewall and NAT algorithms, then passed to the DMZ host when a packet is not sent by a hacker and not limited by the virtual server list.

If you have disabled the NAT option in the WAN-ISP section, this Virtual Server function will hence be invalid.

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 can configure the virtual server IP address manually, but it is still in the same subnet with the router.

3.6.3.7 Advanced

There are four items under the **Advanced** section: **Routing Table, Dynamic DNS**, **Checking Email** and **Device Management.**

Click on the **Routing Table** and then choose **Create Router** to get the below figure to add a routing table.

Destination: Enter the destination subnet IP.

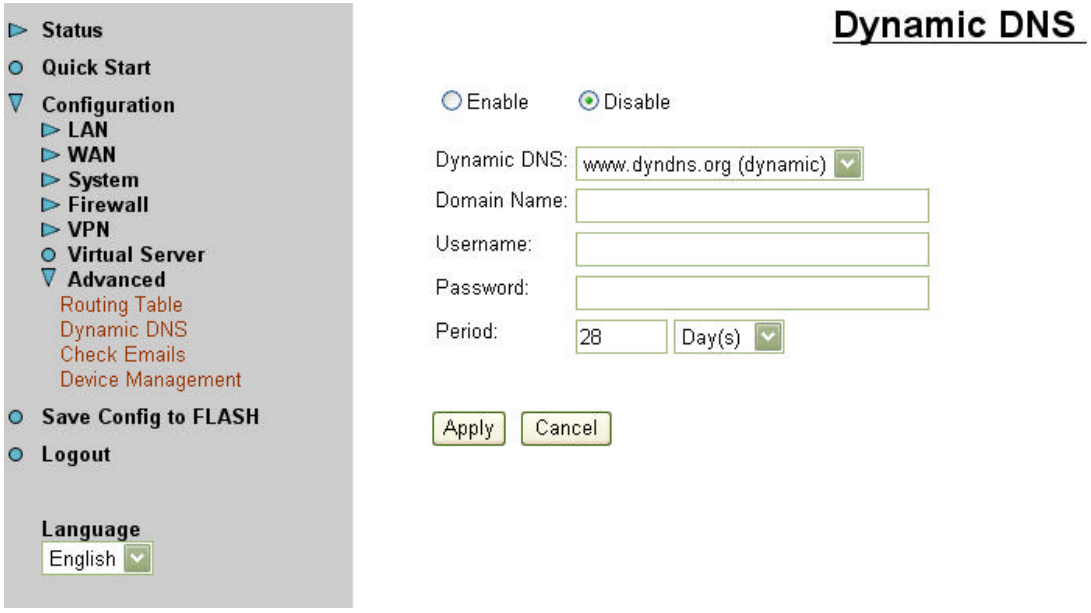
Netmask: Subnet mask of destination IP addresses based on above destination subnet IP.

Gateway: Enter the gateway IP address which the packet is forwarded to.

Interface: Enter the interface which the packet is forwarded to.

Cost: This is the same meaning as Hop. Usually, leave it as 1.

Click **Dynamic DNS** to get the below figure then check the "Enable" button to access the Dynamic DNS service.



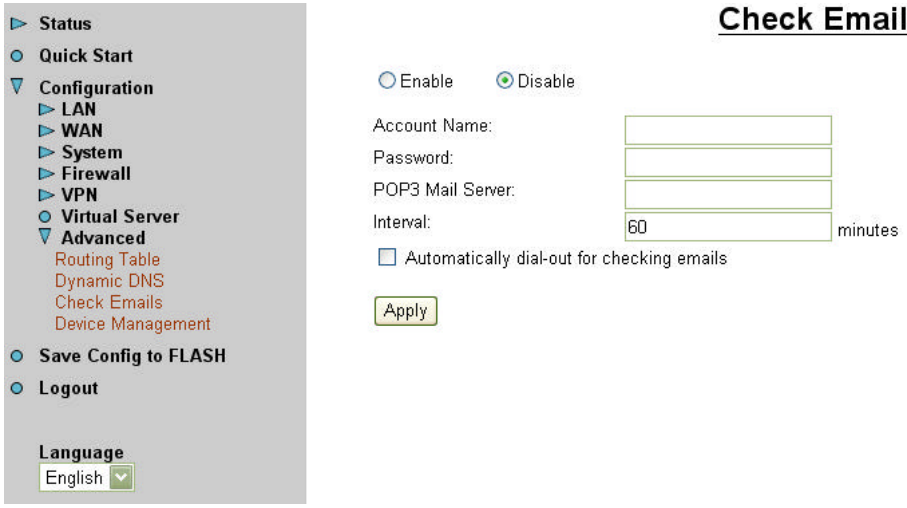
The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. For example, to use the service, you must first apply for an account from this free Web server http://www.dyndns.org/. There are more than 5 DDNS servers supported.

Dynamic DNS: Select the registered DDNS server.

Domain Name, Username and Password: Enter the registered domain name, username and password.

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, the Router will take the same action automatically whenever the assigned IP changes.

Click **Checking Email** to get the below figure then check the "Enable" button to access the service.



⊙ **Disable:** Check to disable the ADSL router from getting the email.

⊙ **Enable:** Check to enable the ADSL router to get the email by providing the required information. Hence, the following fields will be activated and required.

Account Name: Enter the name of the account to which you have the POP access. Normally, it is the text in your email address before the "@" symbol. If you have trouble with it, please contact your ISP.

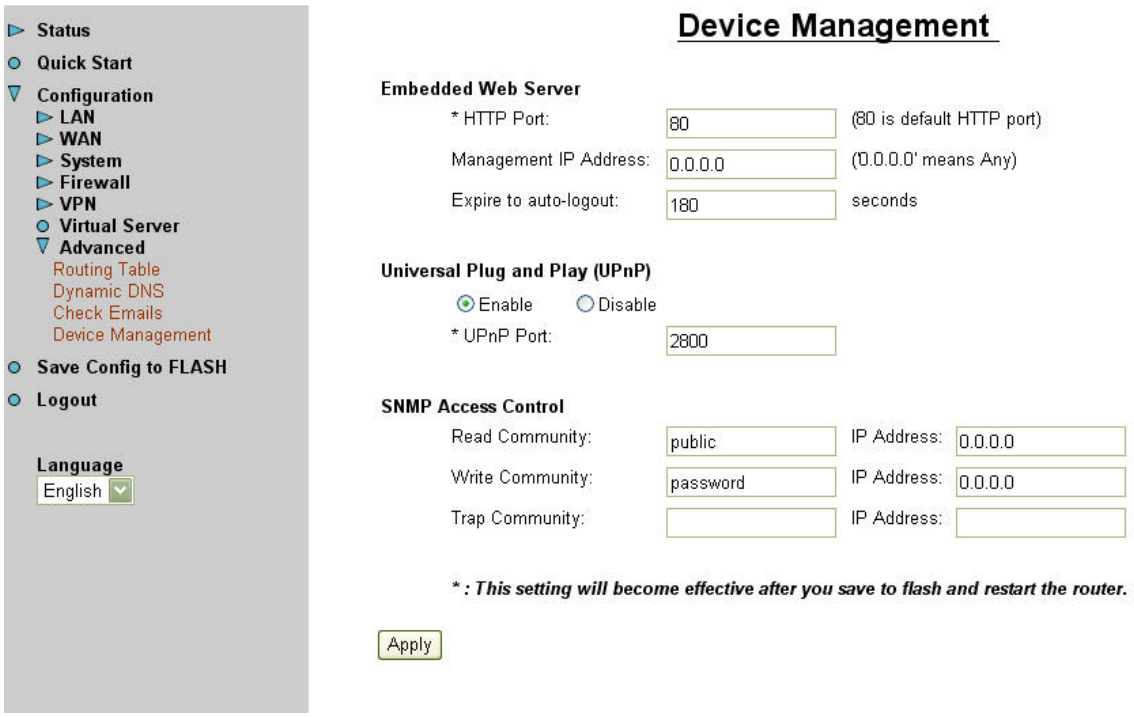
Password: Enter the password of the account

POP3 Mail Server: Enter your (POP) mail server name. If you have trouble with it, you would want to contact your ISP or your external mail server's administrator. For further assistance in tracking down this information, you will need to contact your Internet Service Provider or Network Administrator.

Interval: Enter the value in minutes to check your email account periodically.

Automatically dial-out for checking emails: When the function is enabled, your ADSL router will connect to your ISP automatically to check emails if your Internet connection dropped. Please be careful when using this feature if your ADSL service is charged by time.

Click **Device Management** to protect and obtain system control while allowing device monitoring. This in turn provides enhanced security of the device.



Embedded Web Server

HTTP Port: Default value for HTTP port is 80. A desired value is also allowed. Simply specify a user-defined port number.

Management IP Address: Specify an IP address allowed to logon and access the router's web server.. Note: IP 0.0.0.0 indicates all users who are connected to this router are allowed to logon the device and modify data.]

Expire to auto-logout: Specify a time frame for the system to auto-logout the device.

For Example: User A changes HTTP port number to **100**, specified it's own IP address to be **192.168.1.55**, and set the logout time to be **100** seconds. Device will only allow User A which IP address is **192.168.1.55** to logon to the Web GUI by typing: **192.168.1.254:100**. After 100seconds, the device will automatically logout User A.

Universal Plug and Play (UPnP)

⊙ **Disable:** Check to disable UPnP function.

⊙ **Enable:** Check to enable UPnP function.

UPnP Port: Its default setting is 2800. It is highly recommended for users to use this port value. You may wish to modify this port value, only if this value conflicts with other ports already being used.

SNMP Access Control (downloading SNMP software is required in order to utilize this section)

Read Community: Specify a name in any string to be identified as the Read Community and an IP address. This community string will be checked against the string entered in the

configuration file. Once the string name is matched, user obtains this IP address will be able to view the data.

Write Community: Specify a name in any string to be identified as the Write Community and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user obtains this IP address will be able to view and modify the data.

Trap Community: Specify a name in any string to be identified as the Trap Community and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user obtains this IP address will be notified Traps.

3.6.4 Save Configuration to Flash

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

3.6.5 Logout

To exit the website, choose Logout to exit completely. Please ensure that you have saved the configuration settings before logout.

Be aware that the router is restricted to only one local PC accessing the configuration Web pages. Once a current PC has logged onto the Web pages, other PCs cannot get access except waiting for the current PC to log out of the page. If the previous PC forgets to logout, the second PC can access the page after 3 minutes.

Chapter 4
Troubleshooting

If the MICHELANGELO OFFICE PRO-V ADSL Router 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.

Problems Starting Up the MICHELANGELO OFFICE PRO-V

Problem	Corrective Action
None of the LEDs are on when you turn on the MICHELANGELO OFFICE PRO-V	Check the connection between the adapter and the MICHELANGELO OFFICE PRO-V . If the error persists, you may have a hardware problem. In this case you should contact technical support.

Problems with the WAN Interface

Problem	Corrective Action
Initialization of the PVC connection failed.	Ensure that the cable is connected properly from the ADSL port to the wall jack. The ADSL LED on the front panel of the MICHELANGELO OFFICE PRO-V should be on. Check that your VPI, VCI, type of encapsulation and type of multiplexing settings are the same as what you collected from your telephone company and ISP. Reboot the MICHELANGELO OFFICE PRO-V . If you still have problems, you may need to verify these variables with the telephone company and/or ISP.

Problems with the LAN Interface

Problem	Corrective Action
Can't ping any station on the LAN.	Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a station connected. If it is off, check the cables between your MICHELANGELO OFFICE PRO-V and the station. Make sure you have **uninstalled** any software firewall.
	Verify that the IP address and the subnet mask are consistent between the MICHELANGELO OFFICE PRO-V and the workstations.

*Wireless only on Michelangelo Office Wave Pro-V model

APPENDIX A
Specification

Protocols	IP, NAT, PPTP, ARP, ICMP, DHCP, PPPoE, PPPoA, IPoA, PPTP client, RIP1/2
LAN Port	RJ-45, 4 ports 10/100Base-T LAN Switch
WAN Port	RJ-11, 1 ADSL port
LED Indicators	Power, System, LAN 1 to 4, WLAN, MAIL, PPP and ADSL
Input Power	12V DC @ 1A
Power Consumption	< 10 watts
Agency and Regulatory	CE, A-Tick
Operating Temperature	0? to 45?
Storage Temperature	-10? to 70?
Operating Humidity	5-95% non-condensing

APPENDIX B
Product Support

Most problems can be solved by using the *Troubleshooting* in Chapter 4. If you cannot resolve the problem with the *Troubleshooting* Chapter, please contact the dealer where you purchased this product. For any other questions, please contact ***Digicom*** directly at the following email address: **support@digicom.com**

You can also download upgraded driver or software utilities for free from Digicom's website at **http://www.digicom.com**