

TeleWell TW-EA1000

Wireless ADSL Firewall Router

User's Manual

Table of Content

CHAPTER 1	1
INTRODUCTION	1
1.1 An Overview of the TW-EA1000	1
1.2 Package Contents	2
1.3 TW-EA1000 Features	2
1.4 TW-EA1000 Application	4
CHAPTER 2	5
USING TW-EA1000	5
2.1 Cautions for using the TW-EA1000	5
2.2 The front LEDs	5
2.3 The Rear Ports	6
2.4 Cabling	6
CHAPTER 3	7
CONFIGURATION	7
3.1 Before Configuration	7
3.2 Factory Default Settings	14
3.2.1 Username and Password	15
3.2.2 LAN and WAN Port Addresses	15
3.3 Information from the ISP	16
3.4 Configuring with the Web Browser	16
3.4.1 STATUS	17
3.4.2 Quick Start	17
3.4.3 Configuration	18
3.4.3.1 LAN	19
3.4.3.2 WAN	22
3.4.3.3 System	24
3.4.3.4 Firewall	25
3.4.3.5 VPN	26
3.4.3.6 Virtual Server	29
3.4.3.7 Advanced	30
CHAPTER 4	32
TROUBLESHOOTING	32
Problems Starting Up the TW-EA1000	32
Problems with the WAN Interface	32
Problems with the LAN Interface	32
APPENDIX A	33
SPECIFICATION	33

1.1 An Overview of the TW-EA1000

TW-EA1000 Wireless ADSL Firewall Router provides office and residential users the ideal solution for sharing a high-speed ADSL broadband Internet connection among 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

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. TW-EA1000 Wireless 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. This Quick Start Guide

1.3 TW-EA1000 Features

TW-EA1000 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.

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** 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. It will increase the performance in LAN and WAN, also provide a higher-level security control.

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.

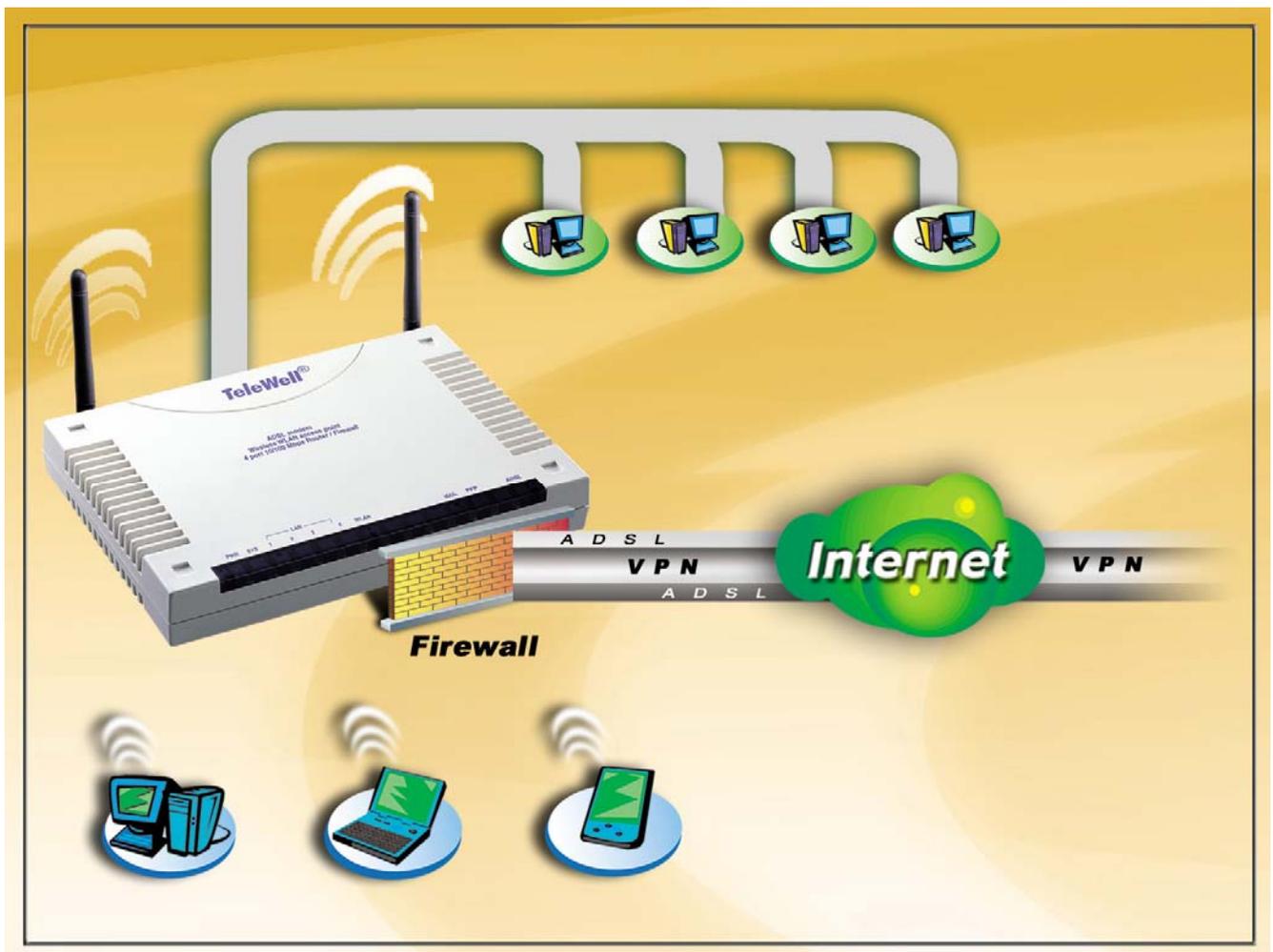
SNTP: An easy way to get the network real time information from an SNTP server.

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.

1.4 TW-EA1000 Application



2.1 Cautions for using the TW-EA1000



Do not place the TW-EA1000 under high humidity and high temperature.

Do not use the same power source for TW-EA1000 with other equipment.

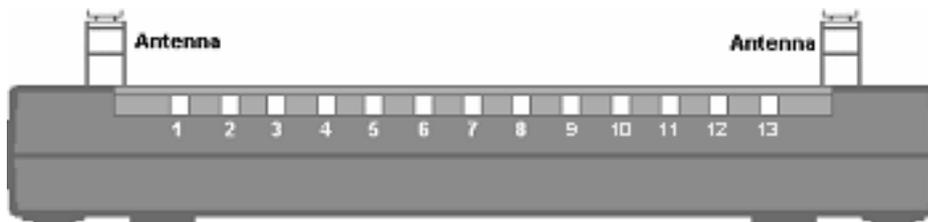
Do not open or repair the case yourself. If the TW-EA1000 is too hot, turn off the power immediately and have a qualified serviceman repair it.



Place the TW-EA1000 on a stable surface.

Only use the power adapter that comes with the package.

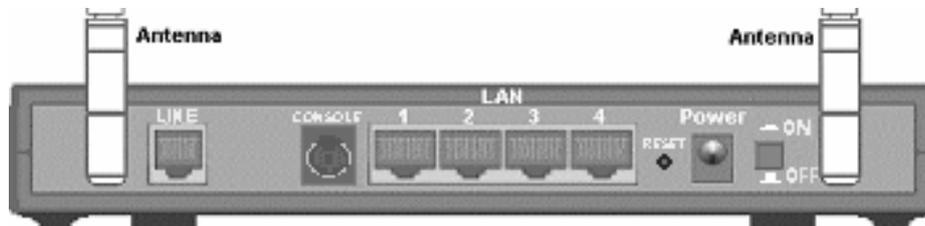
2.2 The front LEDs



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	Press to restore the factory default setting
5	PWR	Connect the supplied power adapter to this jack.
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 TW-EA1000 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 95/98/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 TW-EA1000, either to configure the device, or for network access. These PCs must have an Ethernet interface installed properly, be connected to the TW-EA1000 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 TW-EA1000. The default IP address of the TW-EA1000 is 192.168.0.254 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 TW-EA1000 Router. Also make sure you have UNINSTALLED any kind of software firewall that can cause problems accessing the 192.168.0.254 IP address of the router.

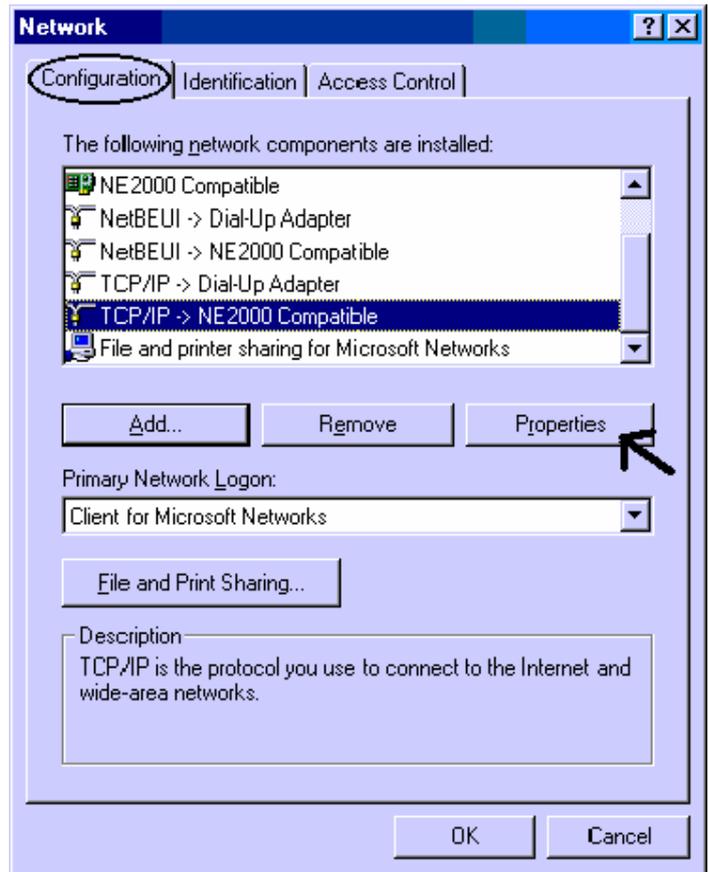
Please follow the steps below for PC's network environment installation. First of all, please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to MS Windows related manuals.



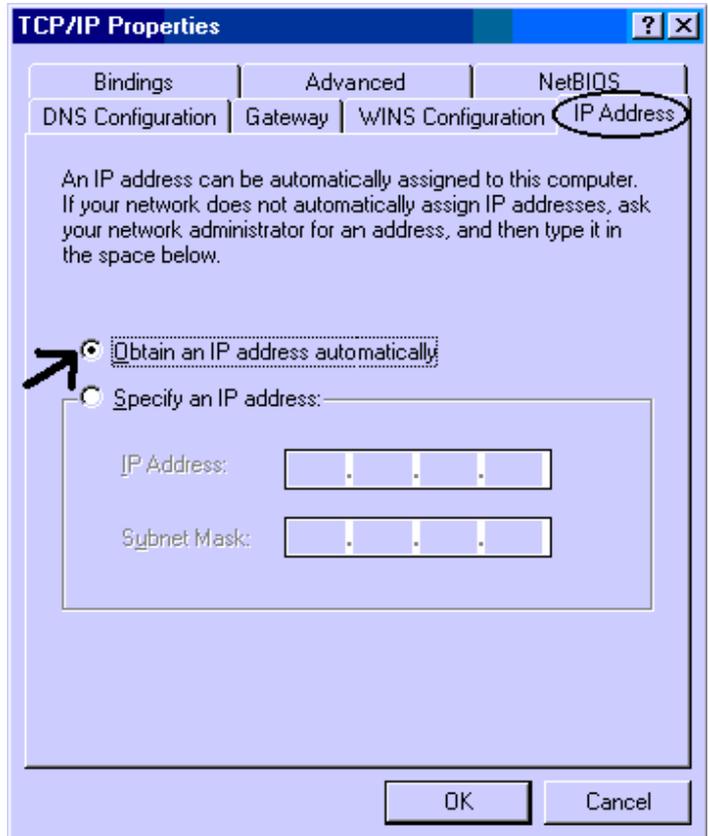
Any TCP/IP capable workstation can be used to communicate with or through the TW-EA1000GE. To configure other types of workstations, please consult the manufacturer's documentation.

Configuring PC in Windows 95/98/ME

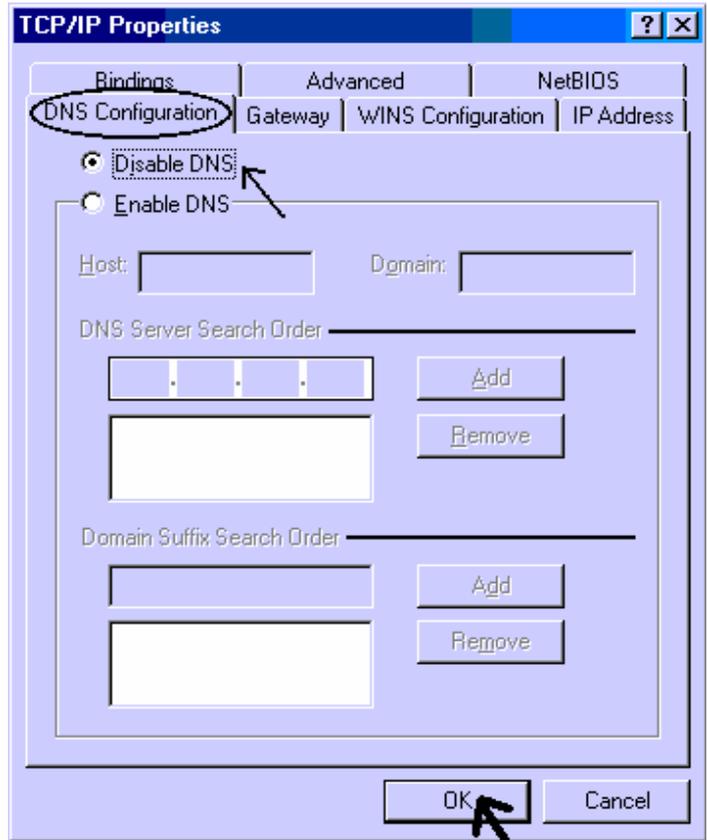
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.
2. Select **TCP / IP -> NE2000 Compatible**, or the name of any Network Interface Card (NIC) in your PC.
3. Click **Properties**.



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

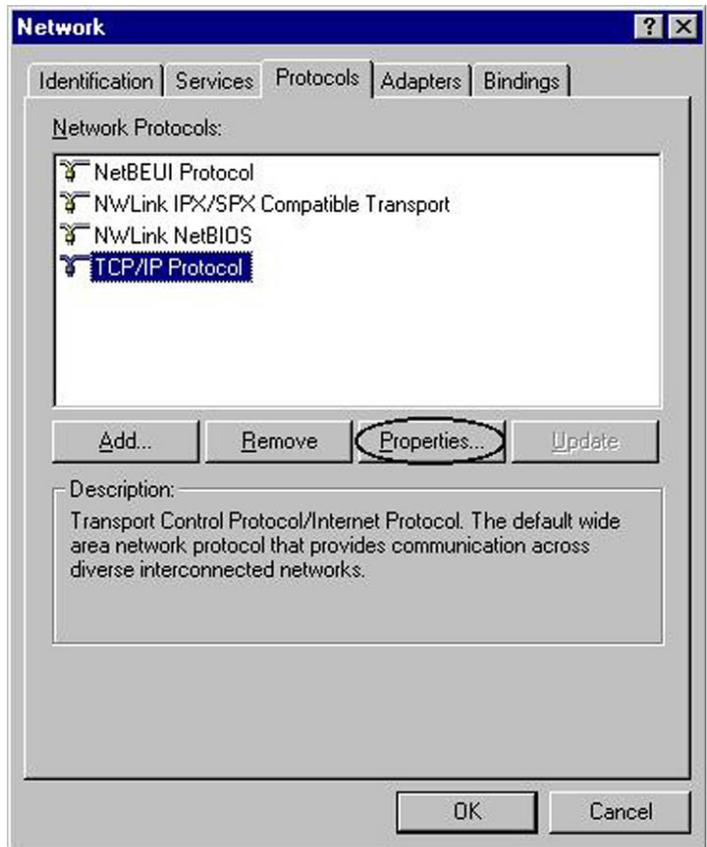


5. Then select the **DNS Configuration** tab.
6. Select the **Disable DNS** radio button and click “**OK**” to finish the configuration.

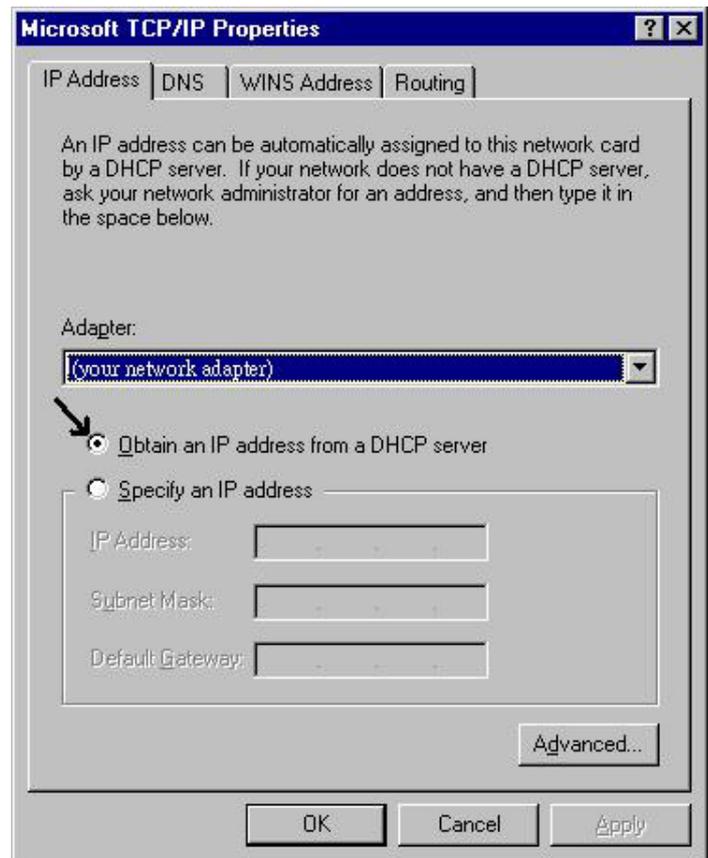


Configuring PC in Windows NT4.0

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**.

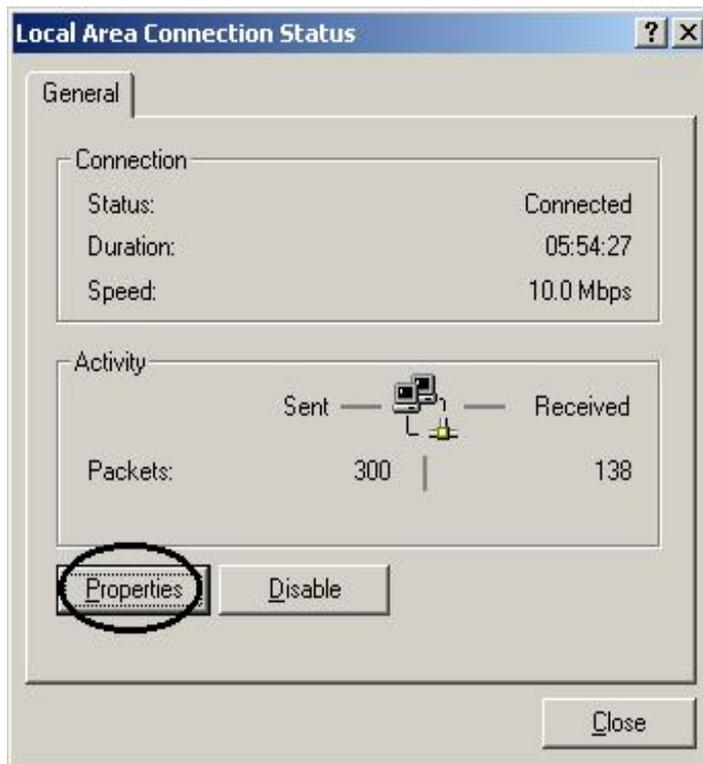


Configuring PC in Windows 2000

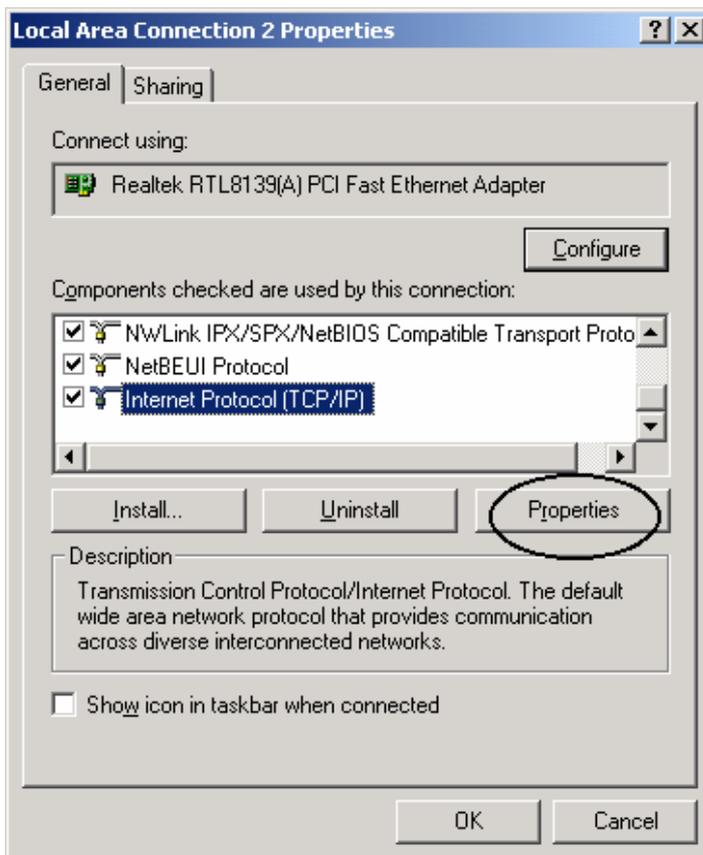
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.
2. Double-click **LAN Area Connection**.



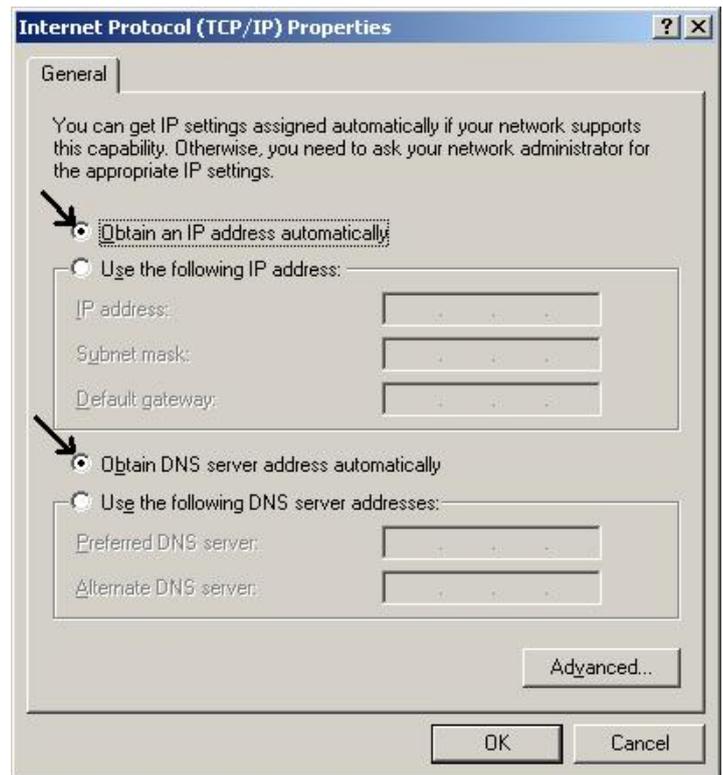
3. In the **LAN Area Connection Status** window, click **Properties**.



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

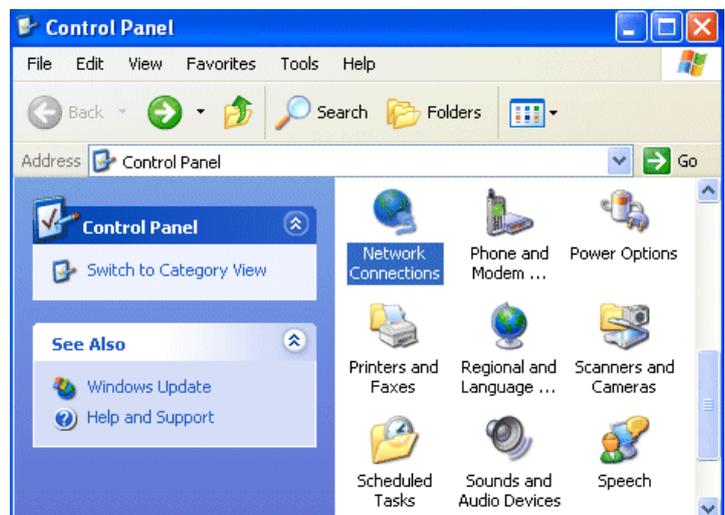


5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.

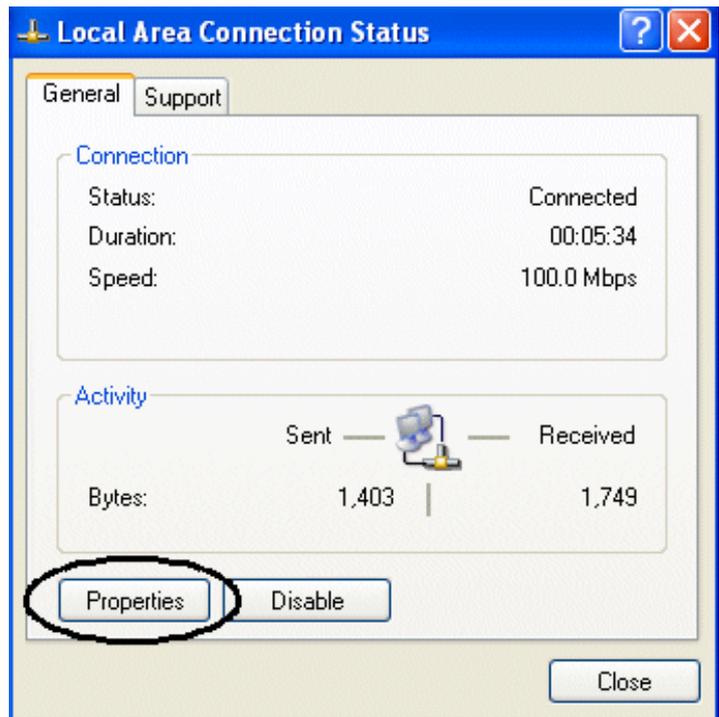


Configuring PC in Windows XP

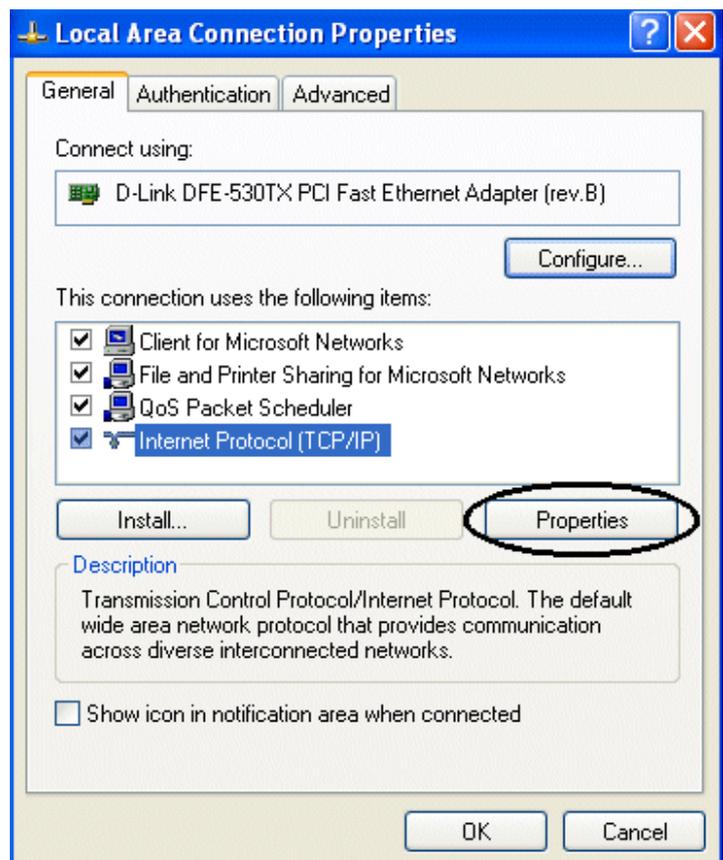
1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections**.
2. Double-click **Local Area Connection**.



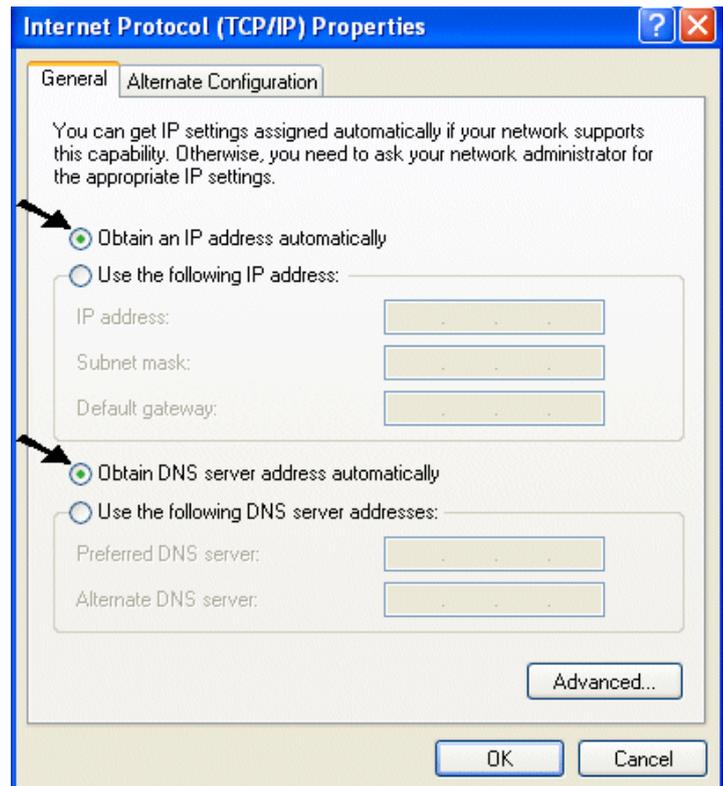
3. In the **LAN Area Connection Status** window, click **Properties**.



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.



3.2 Factory Default Settings

Before you configure this TW-EA1000, 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 : 192.168.0.254

Subnet Mask : 255.255.255.0

3. ISP setting in WAN site

RFC 1483 routed mode with LLC bridged encapsulation

4. DHCP server

DHCP server is enabled.

Start IP Address : 192.168.0.100

IP pool counts : 100

5. NAT is enabled

6. WLAN

ESSID : WLAN-AP

Channel ID : Channel 3

Hide_SSID : False

3.2.1 Username and Password

The default username and password are admin and admin.



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

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	192.168.0.254	The PPPoE function is <i>enabled</i> to automatically get the WAN port configuration from the ISP, but you have to check the VPI/VCI values and 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 192.168.0.100 through 192.168.0.199 (Actually, it can support up to 253 users.)	

3.3 Information from the ISP

Before you start configuring this device, you have to check with your ISP 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).

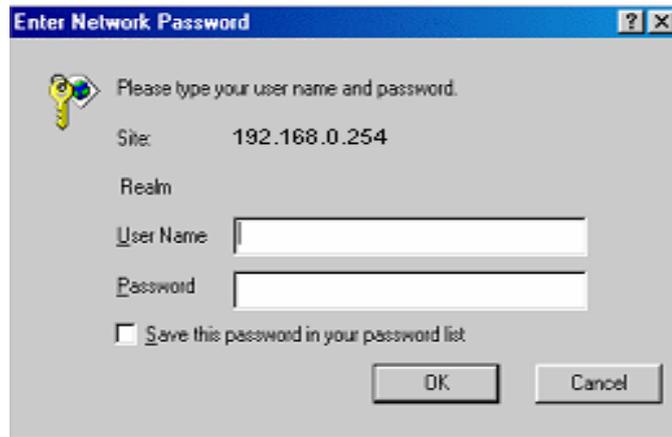
3.4 Configuring with the Web Browser

Open the web browser, enter the local port IP address of this TW-EA1000, which defaults at **192.168.0.254**, and click “Go” to get the status window.



Status		
System Up-Time	00:00:39s	
Current Time	Thu, 01 Jan 1970 - 02:00:26	Set Time...
Hardware Version	ADSL MF-GA v1.00 / He100/2xx CSP v2.3	
Software Version	4.12a	
MAC Address	00:20:2B:74:30:01	
Home URL	EasyTelOy	
LAN		
	IP Address:	192.168.0.254 Lan Settings...
	SubNetmask:	255.255.255.0
	DHCP Server:	Yes DHCP Server Settings...
WAN		
	rfc1483-0	Dynamic, from DHCP Wan Settings...
	VPI/VCI:	0 / 33

If you are going to configure more parameters, the LOGIN IN window will prompt for a username and password. The default username and password are admin and admin.. 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 **Status** (status and PPTP status), **Quick Start**, **Configuration** (LAN, WAN, System, VPN, Virtual Server, Advanced) and **Save Config to FLASH** functions. Besides, it provides user interface in multi-languages.

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

3.4.1 STATUS

In this screen as the above figure, it contains many items including device H/W and S/W information, LAN, WAN, Port status and all defined interfaces. Gives you a quick view to know the TW-EA1000's current status. When you click the Status -> PPTP status, the status of PPTP connection will be shown.

3.4.2 Quick Start

Encapsulation:	1483 Bridged IP LLC
VPI:	PPPoA PPPoE
VCI:	1483 Routed IP VC-Mux 1483 Routed IP LLC Classical IP (1577) 1483 Bridged IP VC-Mux 1483 Bridged IP LLC
NAT:	Pure Bridged VC-Mux Pure Bridged LLC
IP Address:	
SubNetmask:	
Default Gateway:	
DNS	
Primary DNS:	
Secondary DNS:	
PPP	
Username:	
Password:	

Apply Cancel

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, 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 you do not use a Wireless LAN client card. If not please refer to the sections below for more information.

3.4.3 Configuration

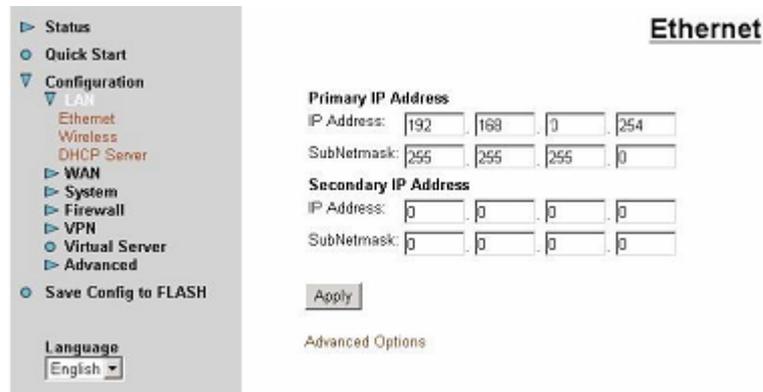
When you click this item, you get following sub-items to configure the Router.

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

These functions are described below in the following sections.

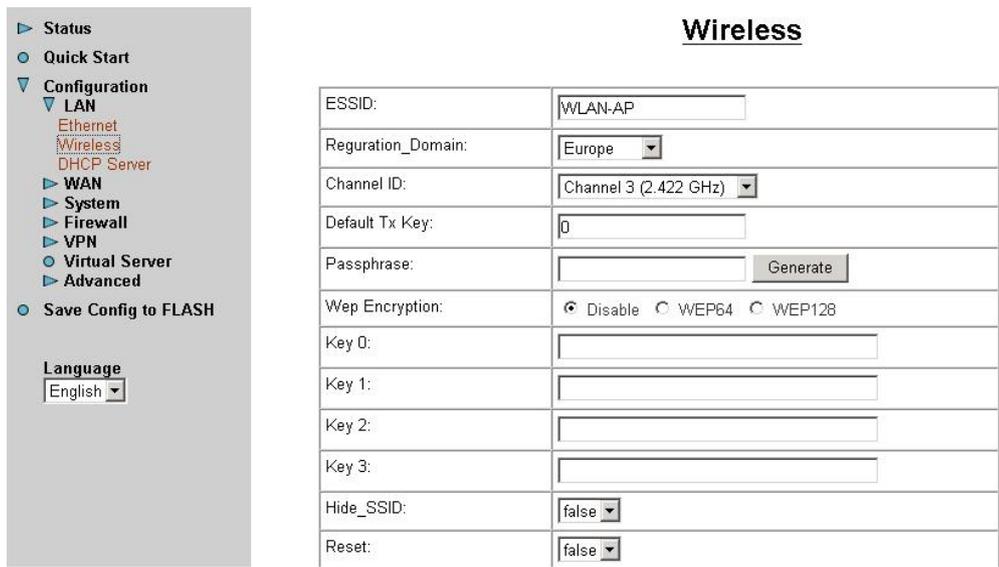
3.4.3.1 LAN

There are three items under the LAN section, Ethernet, Wireless and DHCP Server. When you click **Ethernet**, you will get the following picture as below.



It supports two Ethernet IP addresses in the LAN. With this function, the 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 192.168.0.254 is the default IP address for this Router. The Advanced Options will allow you to configure the routing protocol version 1 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 built in the wireless broadband firewall gateway. To connect to this device, your wireless clients must have the same ESSID as the device.

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

Channel ID: Select the ID of channel 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 input string and pre-defined algorithm in WEP64 or WEP128. You can input same string in both AP and Client card to generate same WEP keys. Please note you do not have to key in **Key (0-3)** as below when **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 **DHCP Server**, you will get the following figure. You can disable or enable the Server or enable the DHCP relay functions.

DHCP Server

DHCP Server Mode

Disable

DHCP Server

DHCP relay agent

DHCP server status:

Default Lease Time: 43200

Allow Bootp: true

Max Lease Time: 86400

Allow Unknown Clients: true

Enabled: true

Subnet definitions:

Subnet Value:	192.168.0.0
Subnet Mask:	255.255.255.0
Max Lease Time:	86400
Default Lease Time:	43200
Use local host address as DNS server:	true
Use local host address as default gateway:	true
Get subnet from IP interface:	ip1an

IP ranges: 192.168.0.1-192.168.0.4 192.168.0.4-192.168.0.4

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 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 Router will find the IP address automatically from the outside network and forward it back to the requesting PC in the LAN.

If you check **DHCP Relay Agent** and click **Next**, 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.

DHCP Server

Disable: Check to disable the TW-EA1000 from distributing IP Addresses to the local network.

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

Enable: Check to enable the TW-EA1000 to distribute IP Addresses, subnet mask and DNS setting to computers. Hence, the following fields will be activated.

Starting IP Address: Enter the starting address of this local IP network address pool. The pool is a piece of continuous IP address segment. The default value is **192.168.0.100**.

Number of DHCP users: Enter the maximum number of computers that you want the DHCP server to assign IP addresses to. The default value is **100**.

With this case, the DHCP pool is from 192.168.0.100 to 192.168.0.199. Therefore, the local computer will randomly pick at an IP address within this range.

3.4.3.2 WAN

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

WAN connections

WAN services currently defined:

Name	Description	Creator	VPI	VCI		
rfc1483-0	RFC 1483 routed mode	WebAdmin	0	33	Edit...	Delete...

Create...

The factory default is RFC 1483 routed mode. 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 routed mode, 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 mode description below.

WAN connections: RFC 1483 routed

Description: RFC 1483 routed mode

VPI: 0

VCI: 33

NAT: Enable

Encapsulation method: LlcBridged

Obtain an IP address automatically via DHCP client

Specify an IP address

IP Address: 0.0.0.0

Netmask: 255.0.0.0

Apply

Advanced Options...

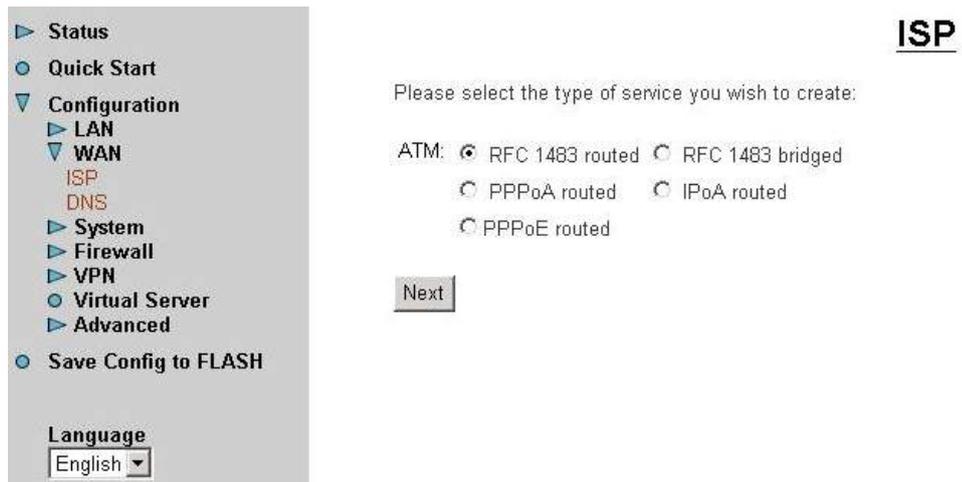
Description: Give a name for this connection.

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.

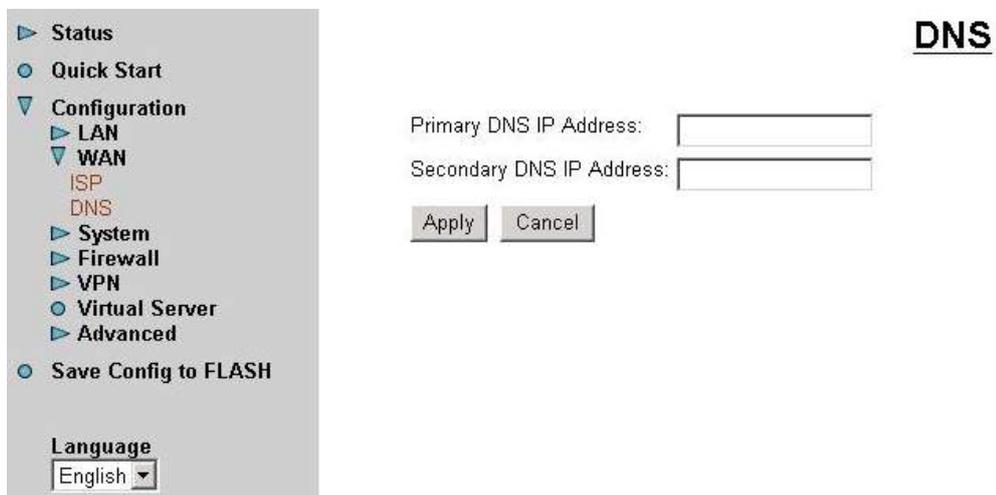
Encapsulation method: Select the protocol format, the default is LlcBridged. Select the one provided by your ISP.

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.



Check one of the access methods among the 5 listed items and click **Next** to configure the right connection method.

The WAN-DNS is shown as below.

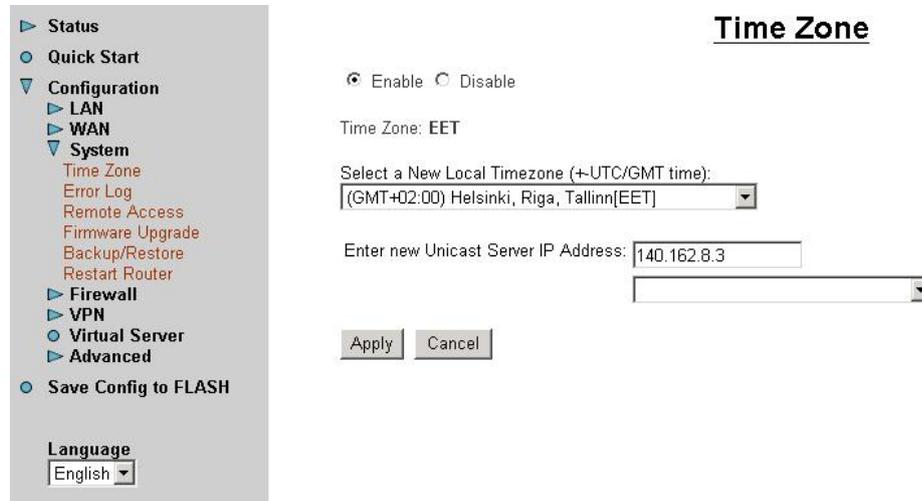


A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. In the Internet, every host has a unique and friendly name such as www.yahoo.com and an IP address. As the IP Address is hard to remember, the DNS converts the friendly name into its equivalent IP Address.

You can obtain a Domain Name System (DNS) IP address automatically if your ISP provides 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.

3.4.3.3 System

There are six items under the **SYSTEM** section, Time Zone, Error Log, Remote Access, Firmware Upgrade, Backup/Restore, and Restart. 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 really establish a connection to the Internet. If you prefer to enter your own SNTP server, please enter and use it as the first choice.

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 **Remote Access** and then click **Enable**, you may temporarily permit remote administration of the TW-EA1000GE Router.

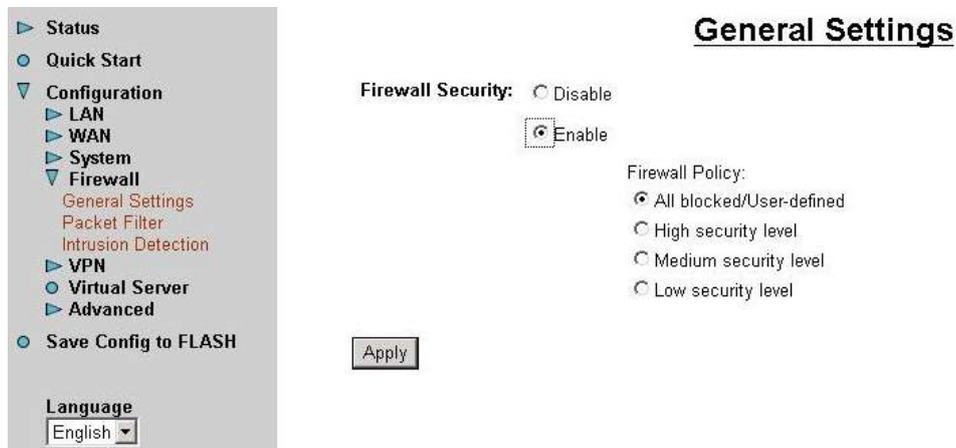
When you click **Firmware Upgrade**, it allows you to input the location of firmware stored on your PC and click the Upgrade button to upgrade to the new firmware.

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**, 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**.

3.4.3.4 Firewall

There are three items under the Firewall section, General settings, Packet Filter, and Intrusion Detection. When you click General Settings, you get the following figure.

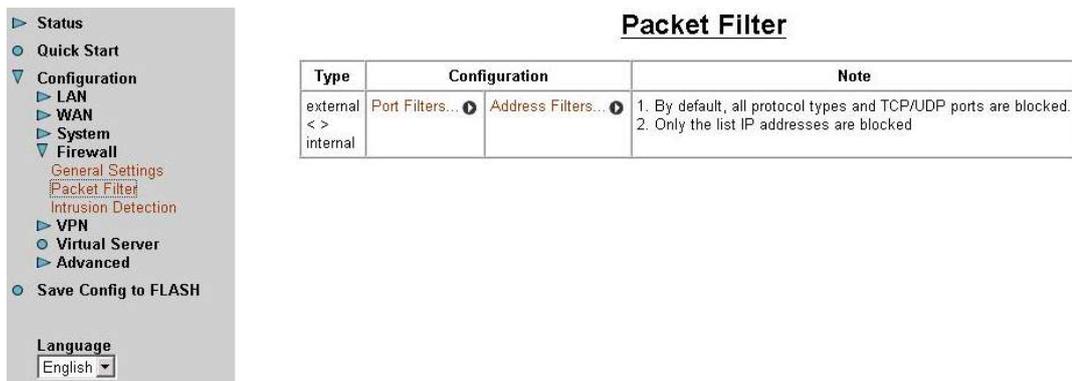


Firewall: When you enable Firewall function, you can select one of the firewall security policies.

All blocked/User-defined: By default, all of 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 use High, Medium or Low firewall security level between WAN and LAN. For example, when you select High, the Port Filters of Packet Filter screen will be set automatically according to High security level settings.

The Firewall – Packet Filter is shown as below.



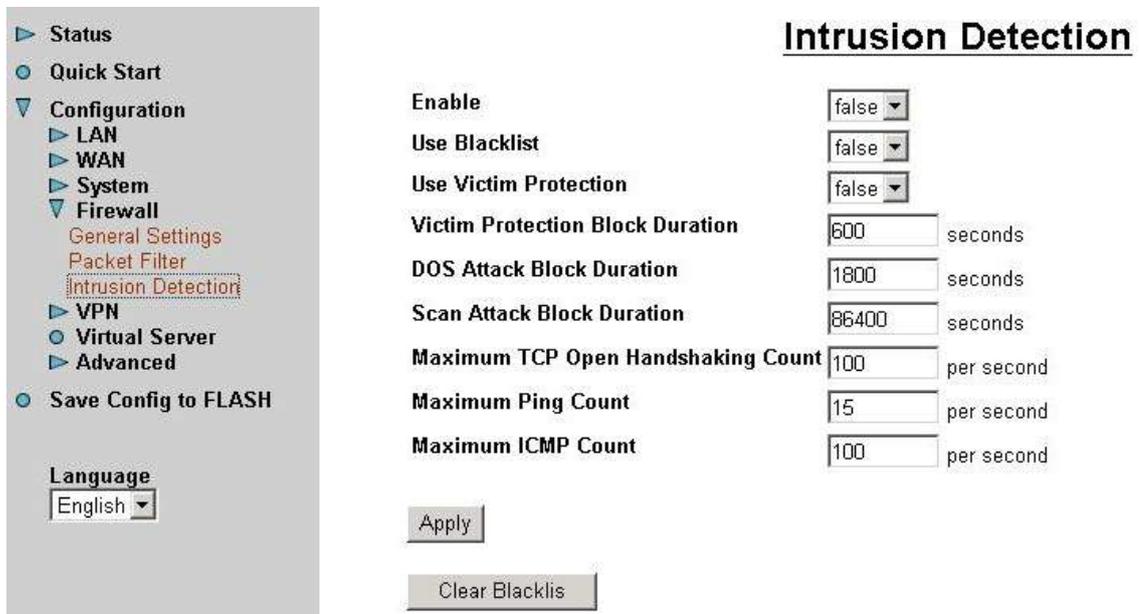
You may configure to filter inbound (incoming) and outbound (outgoing) packets based on PORT or IP address.

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 ICPM. You may enter 1 to protocol number of Raw IP Filtering web page. The port range is supported.

If it is based on the 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 besides block host IP address, 192.168.0.100. 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 192.168.0.100, subnet mask 255.255.255.0 and both direction.

The Firewall – Intrusion Detection is shown as below.



Enable: Set True to enable this Intrusion detection.

Use BlackList: Set True to use router’s default blacklist 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

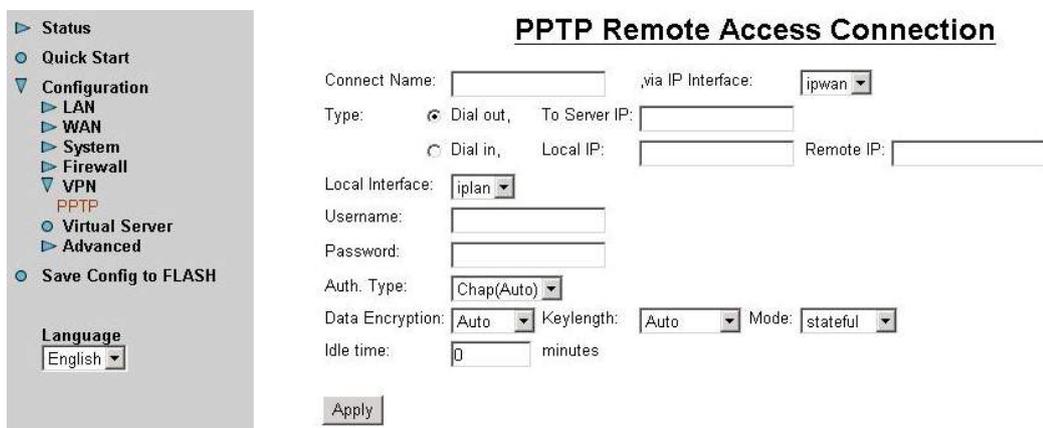
Maximum ICMP Count: Input numbers

3.4.3.5 VPN

There is one item under VPN section, PPTP. There are two applications provided, Remote Access and LAN-to-LAN (please refer below for more information.). Click **Create** to select one of applications and to setup continually.



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



Connection Name: Give a name for this connection.

Via IP Interface: Select an interface that will establish 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 to establish a connection. When this network router acts as a server, please input the **local IP** address and a **remote IP** address assigning it to a dial in PPTP client.

Local Interface: Select an interface that will use this connection to communicate with the remote site.

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).

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.

Via IP Interface: Select an interface that will establish 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 to establish a connection. When this network router acts as a server, please input the **local IP** address and a **remote IP** address assigning it to a dial in PPTP client.

Local Interface: Select an interface that will use this connection to communicate with the remote site.

Peer Network IP: Enter Peer network IP address.

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

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).

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 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.

3.4.3.6 Virtual Server

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

- ▶ Status
- Quick Start
- ▼ Configuration
 - ▶ LAN
 - ▶ WAN
 - ▶ System
 - ▶ Firewall
 - ▶ VPN
 - Virtual Server
 - ▶ Advanced
- Save Config to FLASH

Language
English ▼

Virtual Server

Enable	Application	Protocol	Port	IP Address
<input type="checkbox"/>	FTP	TCP	21	192.168.0. <input style="width: 50px;" type="text"/>
<input type="checkbox"/>	Telnet	TCP	23	192.168.0. <input style="width: 50px;" type="text"/>
<input type="checkbox"/>	SMTP	TCP	25	192.168.0. <input style="width: 50px;" type="text"/>
<input type="checkbox"/>	HTTP	TCP	80	192.168.0. <input style="width: 50px;" type="text"/>
<input type="checkbox"/>	POP3	TCP	110	192.168.0. <input style="width: 50px;" type="text"/>
<input type="checkbox"/>	NNTP	TCP	119	192.168.0. <input style="width: 50px;" type="text"/>
<input type="checkbox"/>	NTP	UDP	123	192.168.0. <input style="width: 50px;" type="text"/>
<input type="checkbox"/>	HTTPS	TCP	443	192.168.0. <input style="width: 50px;" type="text"/>
<input type="checkbox"/>	IKE	UDP	500	192.168.0. <input style="width: 50px;" type="text"/>
<input type="checkbox"/>	T.120	TCP	1503	192.168.0. <input style="width: 50px;" type="text"/>
<input type="checkbox"/>	H.323	TCP	1720	192.168.0. <input style="width: 50px;" type="text"/>
<input type="checkbox"/>	PPTP	TCP	1723	192.168.0. <input style="width: 50px;" type="text"/>

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 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), 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 192.168.0.2, then all the http requests from outside users will be forwarded to the local server with IP address of 192.168.0.2. If the port is not listed as a predefined application, you need to add it manually.

DMZ: Regarding the DMZ Host, it 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 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 two items under the Advanced section, Static Routing and Dynamic DNS. When you click **Static Routing** and then click **Create IP V4Route** to get the below figure to add a routing table.

Name	Value
Destination	<input type="text"/>
Gateway	<input type="text"/>
Netmask	<input type="text"/>
Cost	1
Interface	<input type="text"/>

OK Reset Cancel

Destination: Enter the destination subnet IP.

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

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

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

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

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

Enable Disable

Dynamic DNS:

Domain Name:

Username:

Password:

Period:

via IP Interface:

Apply Cancel

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.

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 Router to exchange information with DDNS server. In addition to update periodically according to this period setting, Router will take the same action automatically whenever the assigned IP is changed.

3.4.4 Save Configuration to Flash

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



Save Config to FLASH

Please confirm that you wish to save the configuration.

There will be a delay while saving as configuration information is written to flash.

Save

If the 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 TW-EA1000

Problem	Corrective Action
None of the LEDs are on when you turn on the TW-EA1000.	Check the connection between the adapter and the TW-EA1000. 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 TW-EA1000 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 TW-EA1000. 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 TW-EA1000 and the station. Make sure you have uninstalled any software firewall.
	Verify that the IP address and the subnet mask are consistent between the TW-EA1000 and the workstations.

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°C to 45°C
Storage Temperature	-10°C to 70°C
Operating Humidity	5-95% non-condensing