DrayTek

VigorFly 200

WiFi Router

Your reliable networking solutions partner

User's Guide

V1.04

VigorFly 200
Wi-Fi Router
User's Guide

Version: 1.04

Date: 18/05/2011

Copyright Information

Copyright Declarations

Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions and Approval

Safety Instructions

- Read the installation guide thoroughly before you set up the router.
- The router is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the router yourself.
- Do not place the router in a damp or humid place, e.g. a bathroom.
- The router should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
- Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
- Keep the package out of reach of children.
- When you want to dispose of the router, please follow local regulations on conservation of the environment.

Warranty

We warrant to the original end user (purchaser) that the router will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Be a Registered Owner

Web registration is preferred. You can register your Vigor router via http://www.draytek.com.

Firmware & Tools Updates

Due to the continuous evolution of DrayTek technology, all routers will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.

http://www.draytek.com

European Community Declarations

Manufacturer: DrayTek Corp.
Address: No. 26, Fu Shing Road, HuKou County, HsinChu Industrial Park, Hsin-Chu, Taiwan 303
Product: VigorFly 200 Series Router

DrayTek Corp. declares that VigorFly 200 is in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

The product conforms to the requirements of Electro-Magnetic Compatibility (EMC) Directive 2004/108/EC by complying with the requirements set forth in EN55022/Class B and EN55024/Class B.

The product conforms to the requirements of Low Voltage (LVD) Directive 2006/95/EC by complying with the requirements set forth in EN60950-1.

Regulatory Information

Federal Communication Commission Interference Statement

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device may accept any interference received, including interference that may cause undesired operation.

Please visit http://www.draytek.com/user/AboutRegulatory.php

This product is designed for 2.4GHz WLAN network throughout the EC region and Switzerland with restrictions in France. Please see the user manual for the applicable networks on your product.

Table of Contents

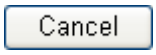
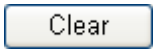
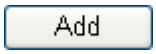
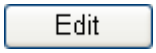
1 Preface

VigorFly 200 is a compact broadband router with 802.11n WLAN network. Its Ethernet WAN port can connect to VDSL/VDSL2/GPON/G.SHDSL /ADSL2+/ADSL/cable modem while you have fixed line. The NAT throughput can easily manage time-critical multimedia streaming. It's easy for family or friends to hook up PCs via embedded 10/100 Ethernet LAN switch to enjoy multimedia applications. Two antennas provide you with speedy WLAN networking. If you are out of coverage of fixed line, you can directly plug 3.5G USB modem to USB port on VigorFly 200. Or, you can use WiMAX USB modem with VigorFly 200. The sharing 3.5G / WiMAX connection accommodates adequate downstream/upstream capacity for residential needs.

The integrated 802.11n Draft 2.0 WLAN network offers users stable and reliable wireless connections for high speed multimedia and data traffic by means of WMM (WiFi Multimedia).

1.1 Web Configuration Buttons Explanation

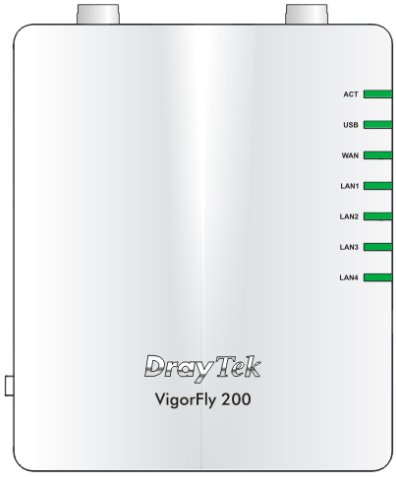
Several main buttons appeared on the web pages are defined as the following:

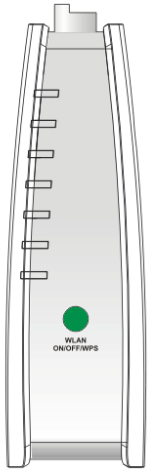
	Save and apply current settings.
	Cancel current settings and recover to the previous saved settings.
	Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings.
	Add new settings for specified item.
	Edit the settings for the selected item.
	Delete the selected item with the corresponding settings.

Note: For the other buttons shown on the web pages, please refer to the following chapters for detailed explanation.

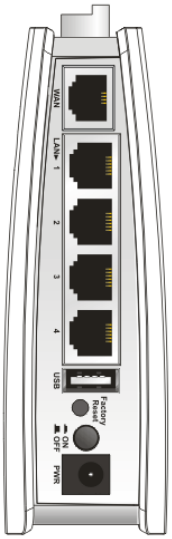
1.2 LED Indicators and Connectors

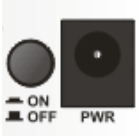
Before you use the Vigor router, please get acquainted with the LED indicators and connectors first.





LED	Status	Explanation
ACT	Off	The system is not ready or is failed.
	Blinking	The system is ready and can work normally.
USB	On	A USB device is connected and active.
	Blinking	The data is transmitting.
WAN	On	The WAN port is connected.
	Blinking	It will blink while transmitting data.
LAN 1 - 4	On	A normal connection is through its corresponding port.
	Off	LAN is disconnected.
	Blinking	Data is transmitting (sending/receiving).
WLAN (Green LED) on WLAN button	On	Wireless access point is ready.
	Off	Wireless access point is not ready.
	Blinking (Green)	Blink when wireless traffic goes through.
WPS (Orange LED) on WLAN button	Off	The WPS is off.
	Blinking (Orange)	Blink with 1 second cycle for 2 minutes - - WPS is enabled and waiting for wireless client to connect with it.
	Blinking (Orange)	Blink when wireless traffic goes through.
WPS Button	Press this button for 2 seconds to wait for client device making network connection through WPS. When the orange LED lights up, the WPS will be on.	

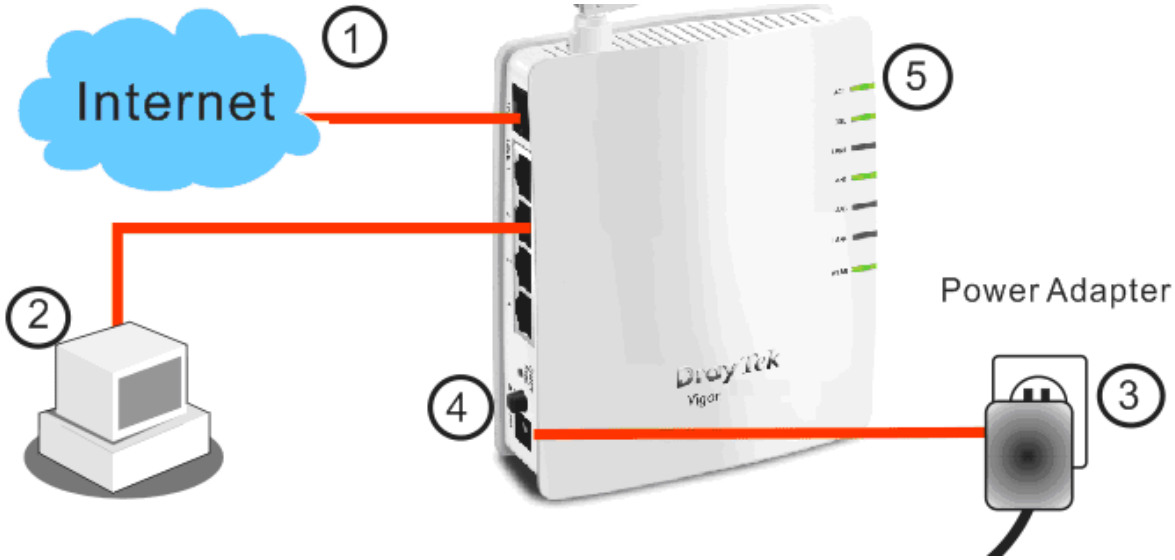


Interface	Description
WAN	Connector for accessing the Internet.
LAN (1-4)	Connectors for local networked devices.
USB	Connector for a printer or 3G backup.
	Restore the default settings. Usage: Turn on the router. Press the button and keep for more than 10 seconds. Then the router will restart with the factory default configuration.
	ON/OFF: Power switch. PWR: Connecter for a power adapter.

1.3 Hardware Installation

Before starting to configure the router, you have to connect your devices correctly.

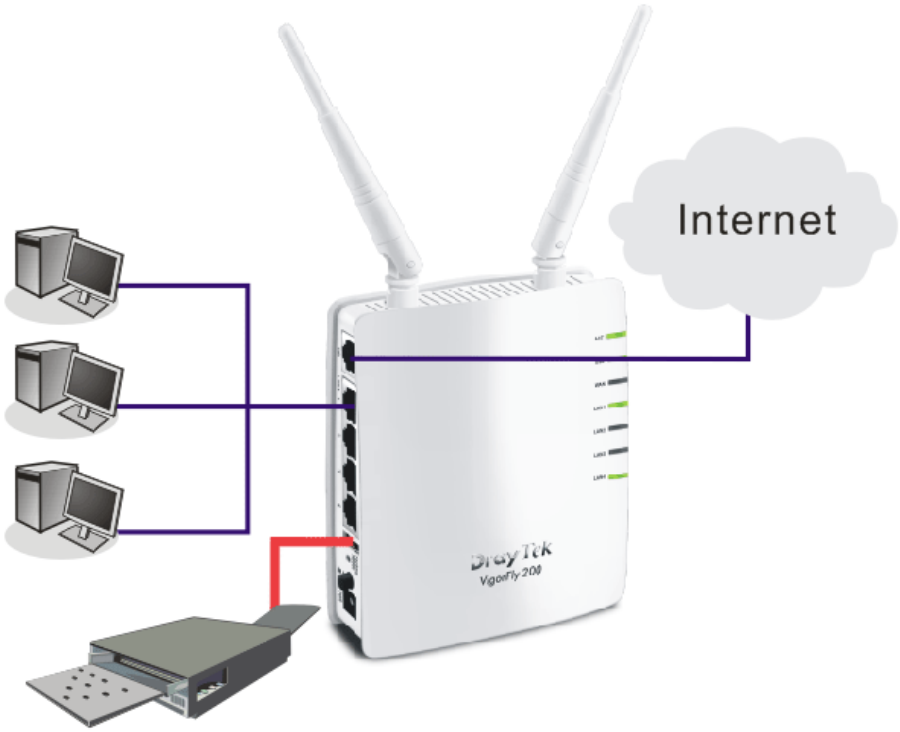
1. Connect this device to a modem with an Ethernet cable.
2. Connect the LAN port to your computer with a RJ-45 cable.
3. Connect one end of the power adapter to the Power port of this device. Connect the other end to the wall outlet of electricity.
4. Power on the router.
5. Check the **ACT, WAN** and **LAN** LEDs to assure network connections.



(For the detailed information of LED status, please refer to section 1.1.)

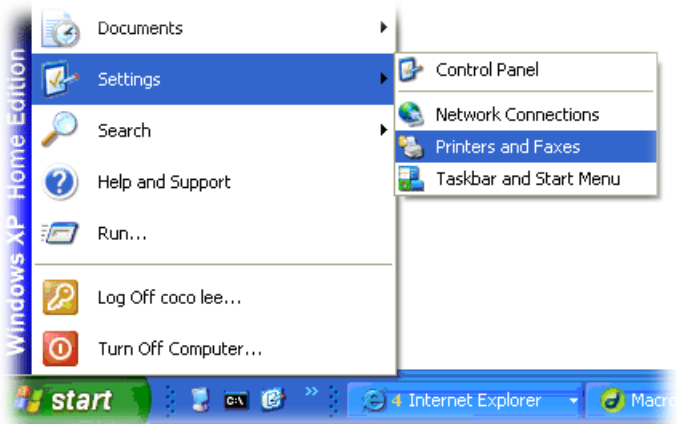
1.4 Printer Installation

You can install a printer onto the router for sharing printing. All the PCs connected this router can print documents via the router. The example provided here is made based on Windows XP/2000. For Windows 98/SE/Vista, please visit **www.draytek.com**.

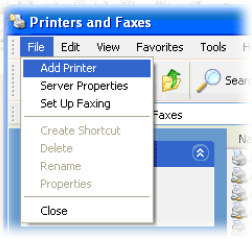


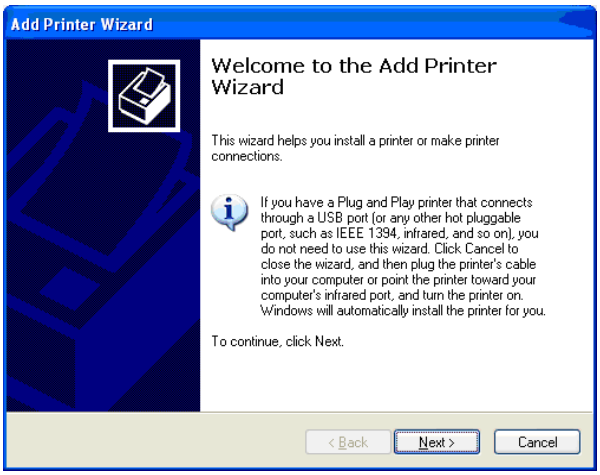
Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

1. Connect the printer with the router through USB/parallel port.
2. Open **Start->Settings-> Printer and Faxes**.

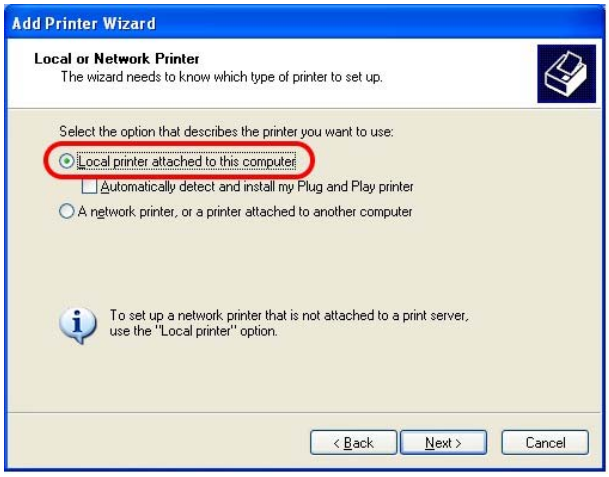


3. Open **File->Add a New Computer**. A welcome dialog will appear. Please click **Next**.

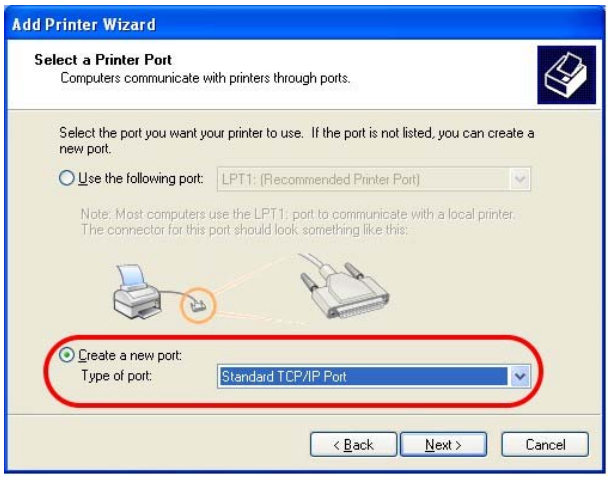




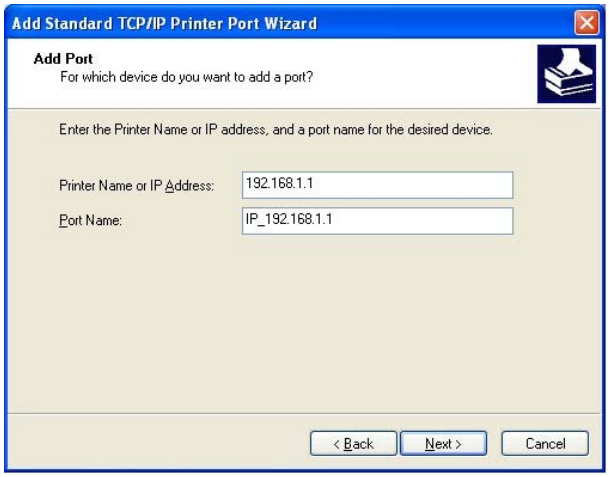
4. Click Local printer attached to this computer and click Next.



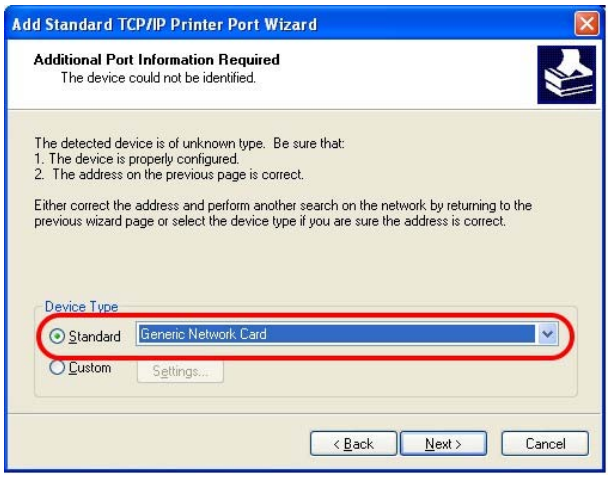
5. In this dialog, choose **Create a new port Type of port** and use the drop down list to select **Standard TCP/IP Port**. Click **Next**.



6. In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Printer Name or IP Address** and type **IP_192.168.1.1** as the port name. Then, click **Next**.

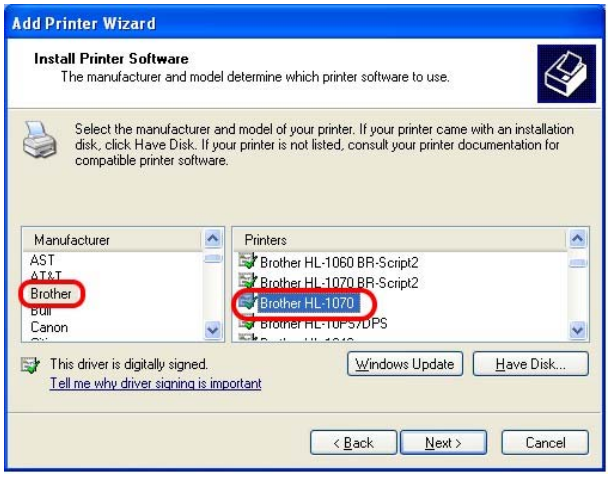


7. Click Standard and choose Generic Network Card.

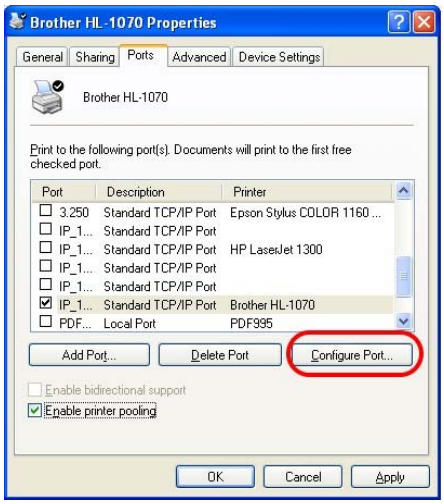


8. Then, in the following dialog, click **Finish**.

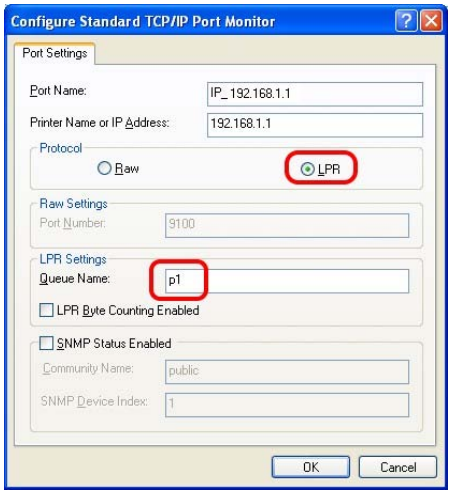
9. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



10. For the final stage, you need to go back to **Control Panel-> Printers** and edit the property of the new printer you have added.



11. Select "**LPR**" on Protocol, type **p1** (number 1) as Queue Name. Then click **OK**. Next please refer to the red rectangle for choosing the correct protocol and UPR name.



The printer can be used for printing now. Most of the printers with different manufacturers are compatible with vigor router.

Note 1: Some printers with the fax/scanning or other additional functions are not supported. If you do not know whether your printer is supported or not, please visit www.draytek.com to find out the printer list. Open **Support >FAQ**; find out the link of **Printer Server** and click it; then click the **What types of printers are compatible with Vigor router**? link.

Note 2: Vigor router supports printing request from computers via LAN ports but not WAN port.

2 Configuring Basic Settings

For using the router properly, it is necessary for you to change the password of web configuration for security and adjust primary basic settings.

2.1 Two-Level Management

This chapter explains how to setup a password for an administrator/user and how to adjust basic/advanced settings for accessing Internet successfully.

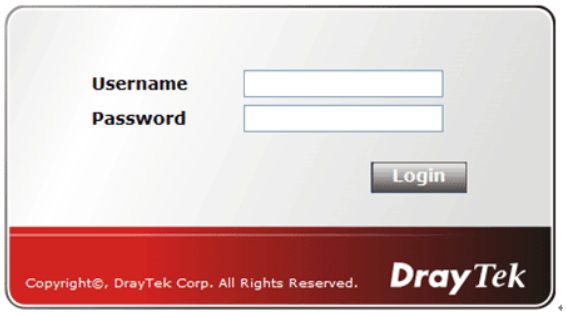
For user mode operation, do not type any word on the window and click **Login** for the simple web pages for configuration. Yet, for admin mode operation, please type "admin/admin" on Username/Password and click **Login** for full configuration.

2.2 Accessing Web Page

1. Make sure your PC connects to the router correctly.

> **Notice:** You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be the same subnet as **the default IP address of Vigor router 192.168.1.1**. For the detailed information, please refer to the later section - Trouble Shooting of the guide.

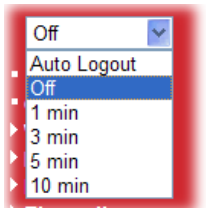
2. Open a web browser on your PC and type **http://192.168.1.1.** The following window will be open to ask for username and password.



3. For user mode operation, do not type any word on the window and click **Login** for the simple web pages for configuration. Yet, for admin mode operation, please type "admin/admin" on Username/Password and click **Login** for full configuration.

> **Notice:** If you fail to access to the web configuration, please go to "Trouble Shooting" for detecting and solving your problem.

4. The web page can be logged out according to the chosen condition. The default setting is **Auto Logout**, which means the web configuration system will logout after 5 minutes without any operation. Change the setting for your necessity.

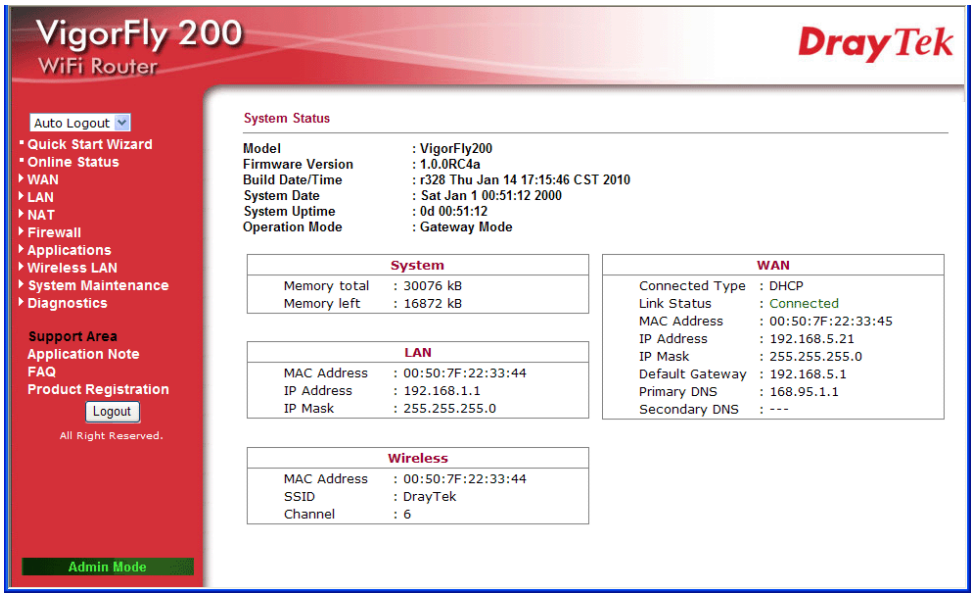


2.3 Changing Password

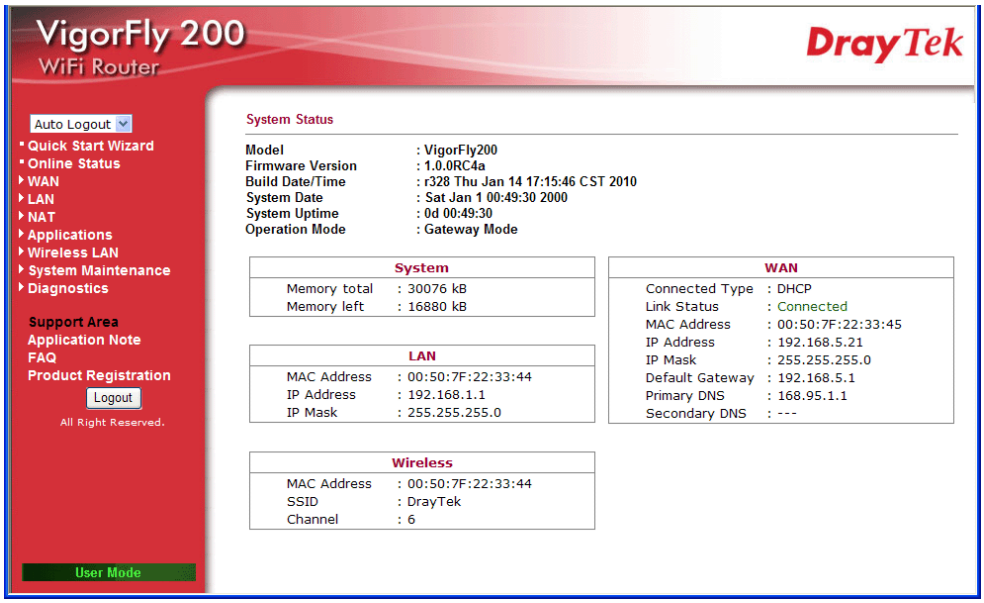
Before configuring the web pages, please change the password for the original security of the router. Such action can be done in **Admin Mode** only.

1. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for username and password.

2. Please type “admin/admin” on Username/Password for admin mode. Otherwise, do not type any word (both username and password are Null for user mode) on the window and click **Login** on the window.



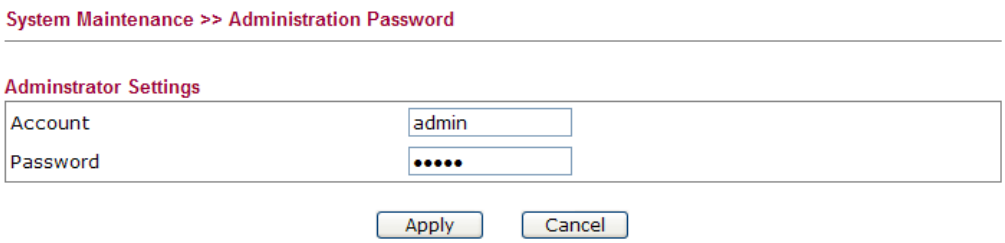
Main screen for admin mode operation (full configuration)



Main screen for user mode operation (simple configuration)

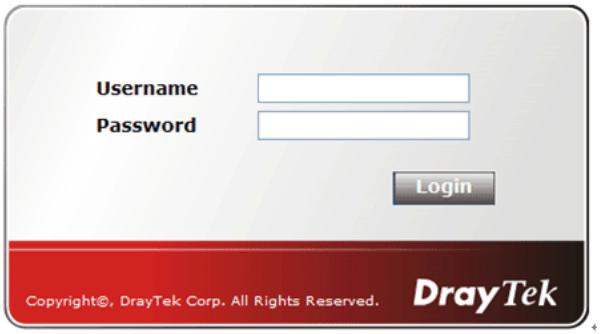
Note: The home page will change slightly in accordance with the type of the router you have.

3. To change the password, please access into **Admin Mode**. Then, go to **System Maintenance** page and choose **Administration Password.**



4. Type **new user name** in the field of **Account** and new password in the field of **Password**. Then click **OK** to continue.

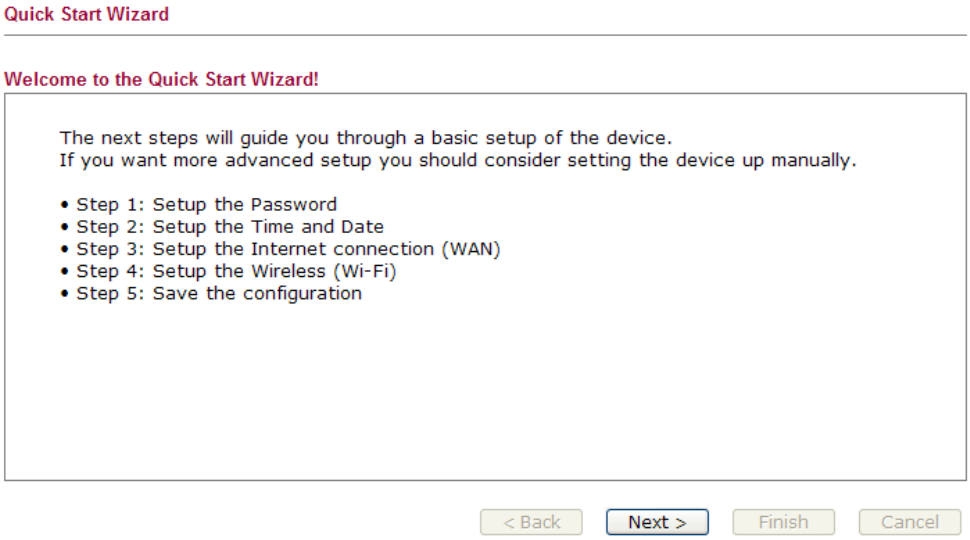
5. Now, the password has been changed. Next time, use the new username / password to access the Web Configurator of this router.



2.4 Quick Start Wizard

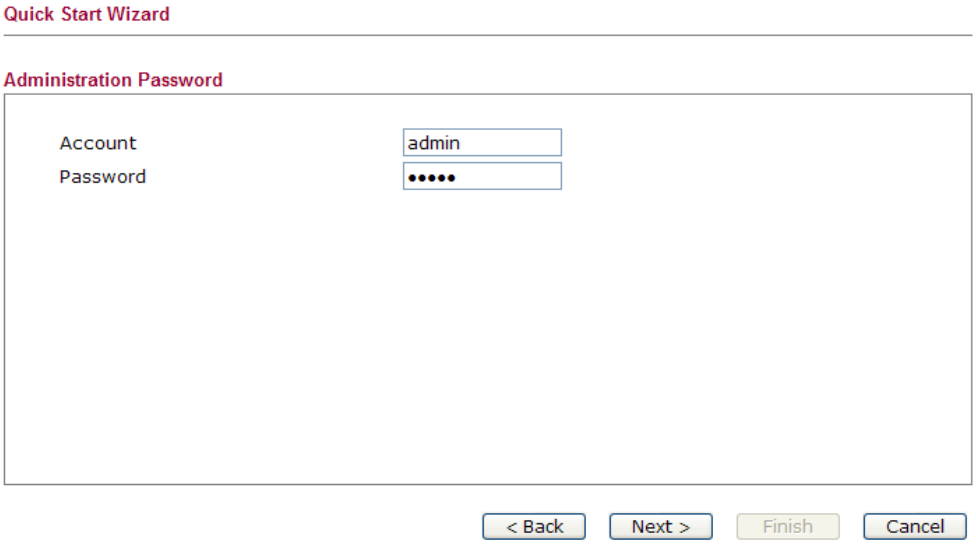
Notice: Quick Start Wizard for user mode operation is the same as for admin mode operation.

If your router can be under an environment with high speed NAT, the configuration provide here can help you to deploy and use the router quickly. The first screen of **Quick Start Wizard** is welcome page, please click **Next**.



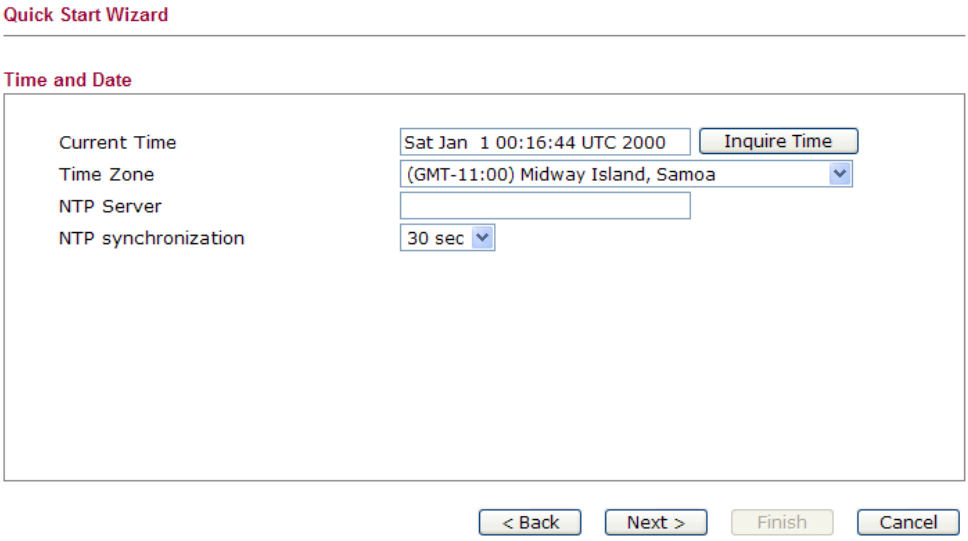
2.4.1 Setting up the Password

The first screen of **Quick Start Wizard** is entering login account and password. After typing a new password, please click **Next**.



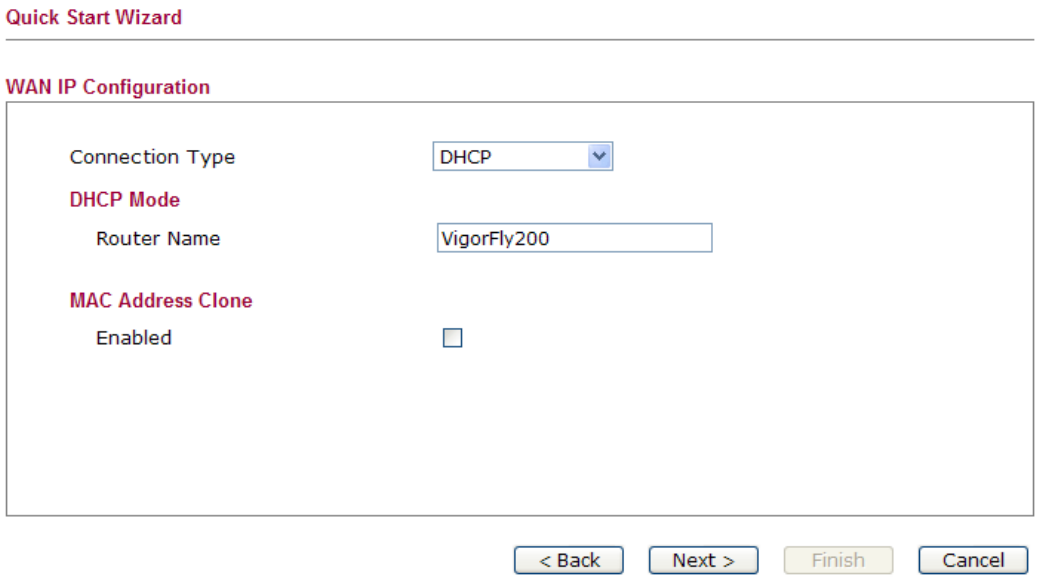
2.4.2 Setting up the Time and Date

On the next page as shown below, please select the Time Zone for the router installed and specify the NTP server(s). Then click **Next** for next step.



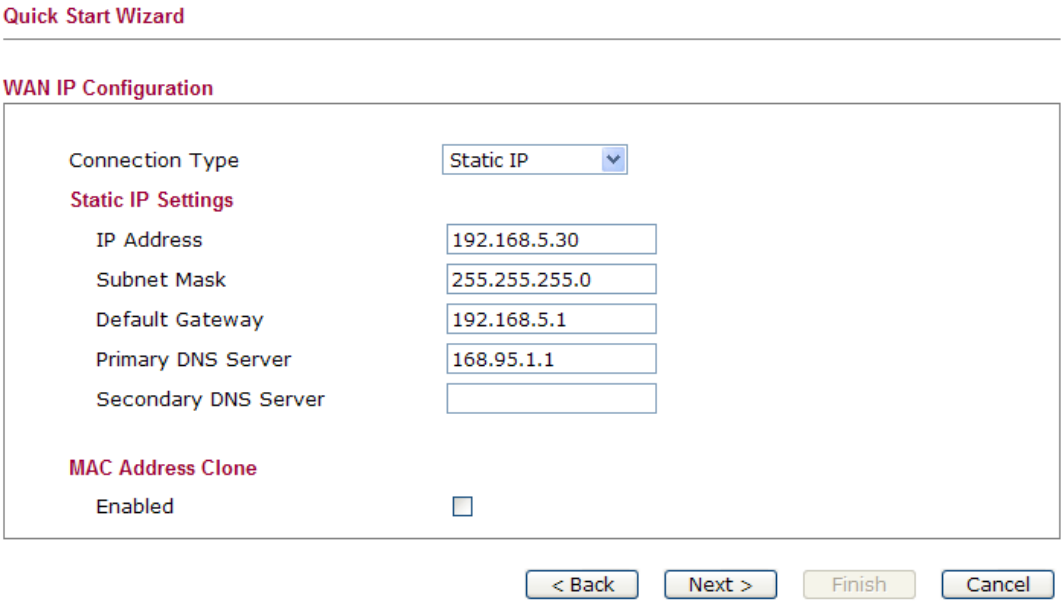
2.4.3 Setting up the Internet Connection

On the next page as shown below, please select the appropriate connection type according to the information from your ISP. There are five types offered in this page. Each connection type will bring out different web page.



Static IP

You will receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your DSL or Cable ISP service providers. In most cases, a Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you have a public subnet, you could assign an IP address or many IP address to the WAN interface.



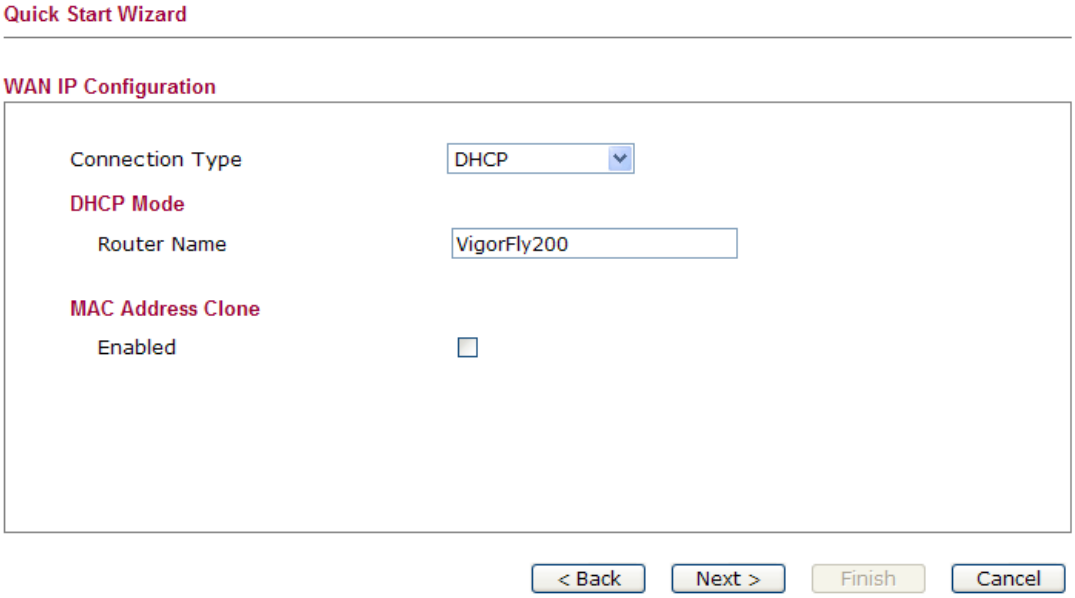
IP Address	Type the IP address.
Subnet Mask	Type the subnet mask.
Default Gateway	Type the gateway IP address.
Primary DNS Server	Type in the primary IP address for the router.
Secondary DNS Server	Type in secondary IP address for necessity in the future.
Enable	The router will detect the MAC address automatically. Or, check the box to enable MAC address cloning.
MAC Address Clone	It is available when the box of **Enabled** is checked. Click **MAC Address Clone.** The router will detect the MAC address automatically. And the result will be displayed in the field of MAC Address.

Besides, if you want to change the MAC address for WAN interface, simply click **Enable** and type the MAC address in this field manually.

After finishing the settings here, please click **Next.**

DHCP

It is not necessary for you to type any IP address manually. Simply choose this type and the system will obtain the IP address automatically from DHCP server.



DHCP Mode

Router Name – Default setting is VigorFly200.

Enable

The router will detect the MAC address automatically. Or, check the box to enable MAC address cloning.

MAC Address Clone

It is available when the box of **Enabled** is checked. Click **MAC Address Clone.** The router will detect the MAC address automatically. And the result will be displayed in the field of MAC Address.

Besides, if you want to change the MAC address for WAN interface, simply click **Enable** and type the MAC address in this field manually.

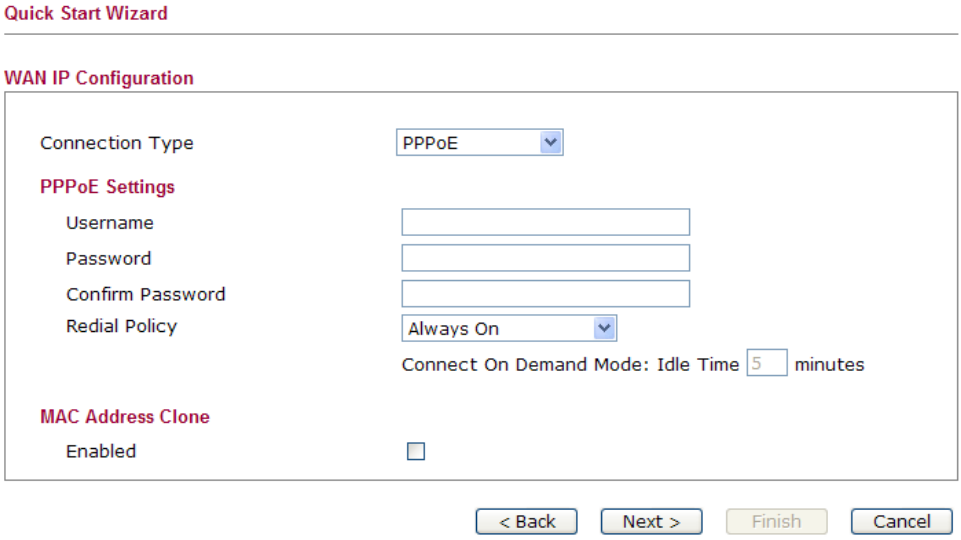
After finishing the settings here, please click **Next.**

PPPoE

PPPoE stands for **Point-to-Point Protocol over Ethernet**. It relies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet can share a common connection.

PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.

If your ISP provides you the **PPPoE** connection, please select **PPPoE** for this router. The following page will be shown:

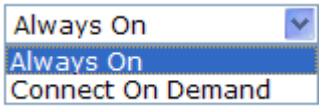


User Name Assign a specific valid user name provided by the ISP.

Password Assign a valid password provided by the ISP.

Confirmed Password Type the password again for confirmation.

Redial Policy If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, choose **Connect on Demand**.



Always On – Choose it to enable router always keep connection.

Connect On Demand - If the connection has been idled over the value, the router will drop the connection.

Idle Time - Set the timeout for breaking down the Internet after passing through the time without any action. The unit is seconds. The range is XX ~ XX.

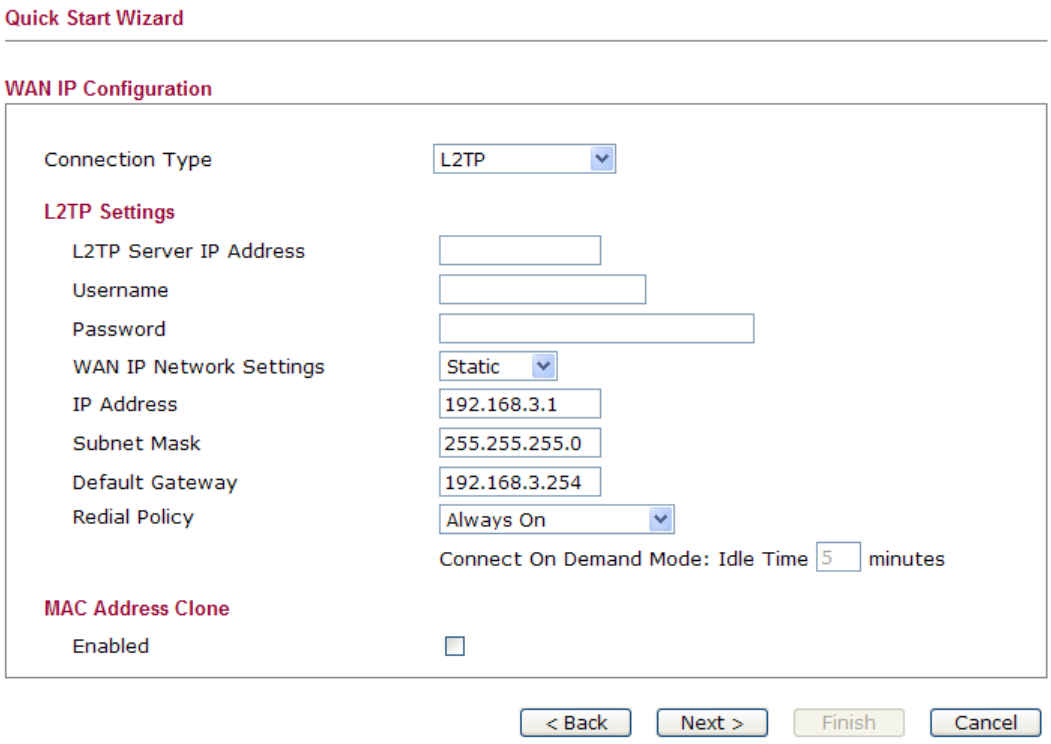
MAC Address Clone It is available when the box of **Enabled** is checked. Click **MAC Address Clone** The router will detect the MAC address automatically. And the result will be displayed in the field of MAC Address.

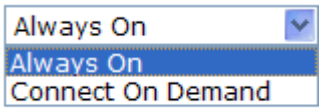
Besides, if you want to change the MAC address for WAN interface, simply click **Enable** and type the MAC address in this field manually.

After finishing the settings here, please click **Next.**

PPTP/L2TP

If you click PPTP/L2TP as the connection type, please manually enter the Username/Password provided by your ISP and all the required information.



L2TP/PPTP Server IP Address	Specify the IP address of the PPTP/L2TP server.
User Name	Assign a specific valid user name provided by the ISP.
Password	Assign a valid password provided by the ISP.
WAN IP Network Settings	You can choose Static IP or DHCP as address mode setting.
IP Address	Type the IP address if you choose Static IP as the WAN IP network setting.
Subnet Mask	Type the subnet mask if you chose Static IP as the WAN IP.
Redial Policy	If you want to connect to Internet all the time, you can choose **Always On**.  **Always On –** Choose it to enable router always keep connection. **Connect On Demand -** If the connection has been idled over the value, the router will drop the connection. **Idle Time -** Set the timeout for breaking down the Internet after passing through the time without any action. The unit is seconds. The range is XX ~ XX.
MAC Address Clone	It is available when the box of **Enabled** is checked. Click **Clone MAC Address.** The router will detect the MAC

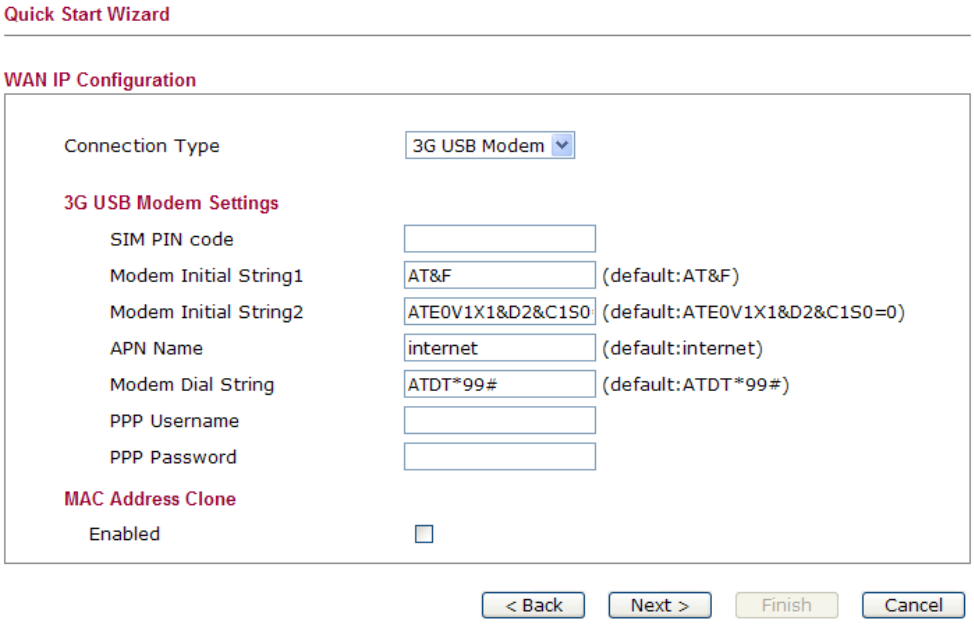
address automatically. And the result will be displayed in the field of MAC Address.

Besides, if you want to change the MAC address for WAN interface, simply click **Enable** and type the MAC address in this field manually.

After finishing the settings here, please click **Next.**

3G USB Modem

If you want to access Internet by 3G USB modem, choose this mode as the protocol and type the required information in this web page.



SIM PIN code Type PIN code of the SIM card that will be used to access Internet.

Modem Initial String1/2 Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.

APN Name APN means Access Point Name which is provided and required by some ISPs.

Modem Dial String Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.

PPP Username Type the PPP username (optional).

PPP Password Type the PPP password (optional).

MAC Address Clone It is available when the box of **Enabled** is checked. Click **MAC Address Clone.** The router will detect the MAC address automatically. And the result will be displayed in the

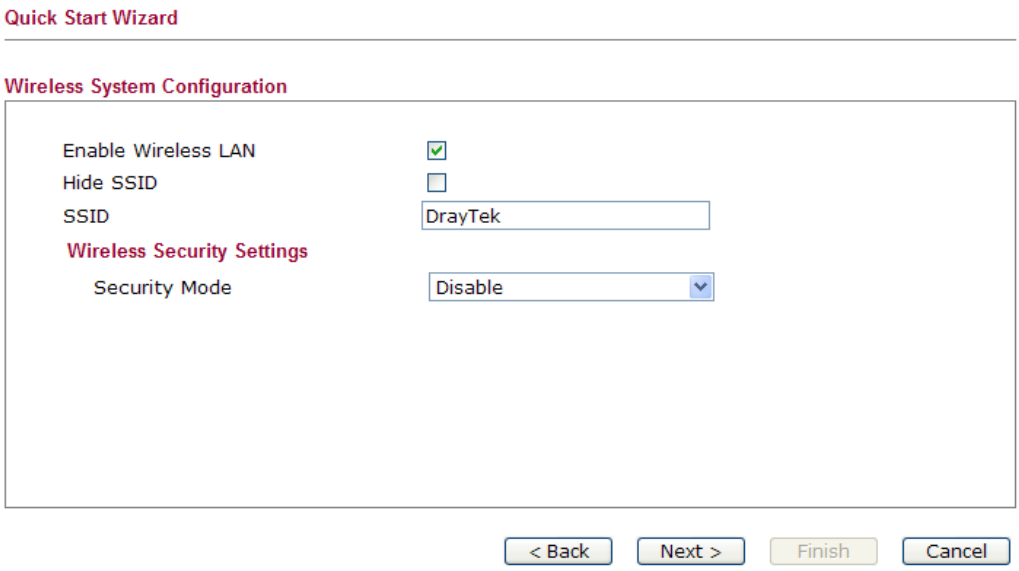
field of MAC Address.

Besides, if you want to change the MAC address for WAN interface, simply click **Enable** and type the MAC address in this field manually.

After finishing the settings here, please click **Next.**

2.4.4 Setting up the Wireless Connection

Now, you have to set up the wireless connection.

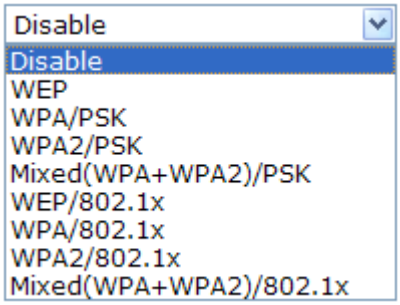


Enable Wireless LAN — Check the box to enable the wireless function.

Hide SSID — Check this box to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN.

SSID — It means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "DrayTek". We suggest you to change it.

Security Mode — Choose the wireless mode for this router.

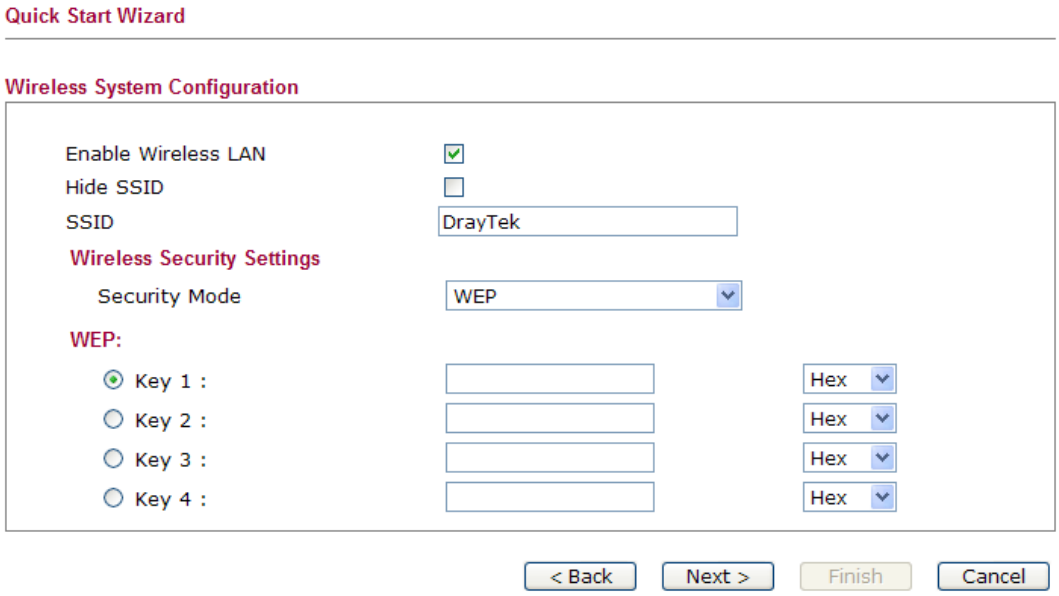


Each encryption mode will bring out different web page and

ask you to offer additional configuration.

WEP

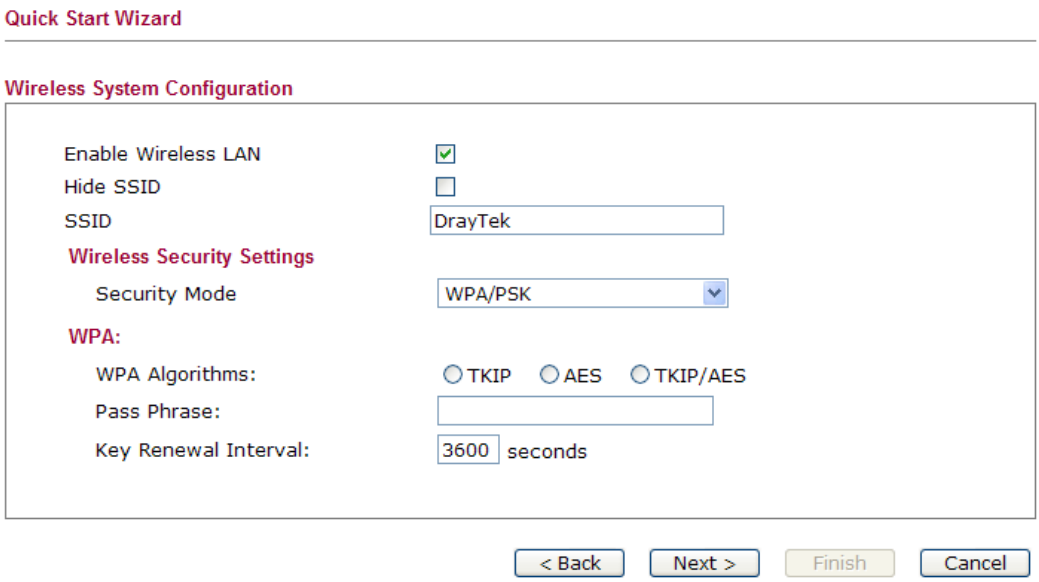
If you choose WEP as the security configuration, you have to specify encryption key (Key 1 ~ Key 4) and authentication mode (open or shared). All wireless devices must support the same WEP encryption bit size and have the same key.



Key 1 ~ Key 4 Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','.

WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK

Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.



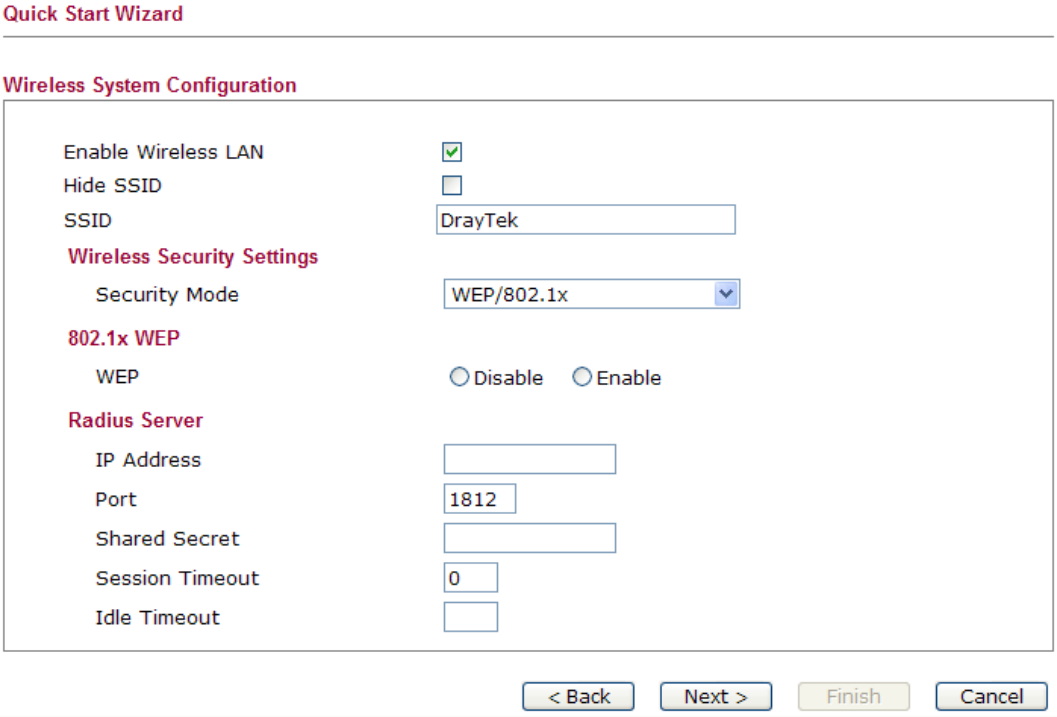
WPA Algorithm	Choose the WPA algorithm, TKIP, AES or TKIP/AES.
Pass Phrase	Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key.

WEP/802.1x

Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet service providers. It is the most common method of authenticating and authorizing dial-up and tunneled network users.

The built-in RADIUS client feature enables the router to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.

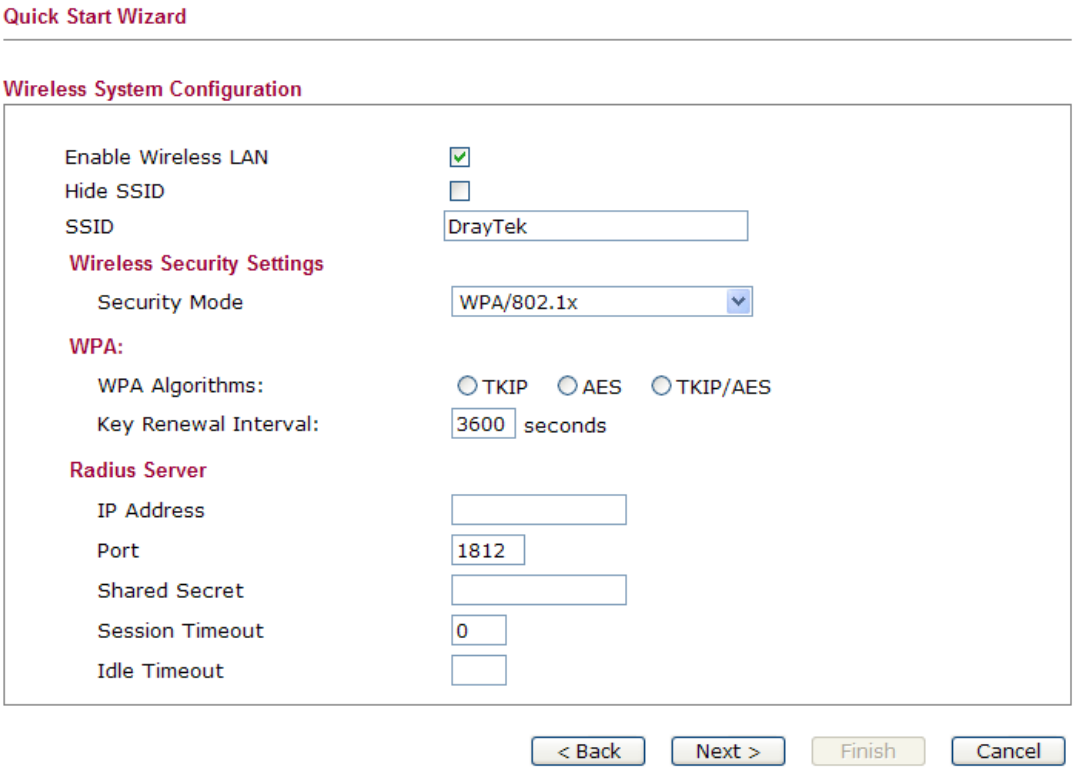
If you choose WPA-Radius as the security configuration, you have to specify WPA mode, algorithm, Radius server, Radius server port and Radius server secret respectively.



WEP	**Disable** - Disable the WEP Encryption. Data sent to the AP will not be encrypted. **Enable** - Enable the WEP Encryption.
IP Address	Enter the IP address of RADIUS server.
Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)
Idle Timeout	Set the maximum time that a wireless device may remain idle. (The unit is second.)

WPA/802.1x

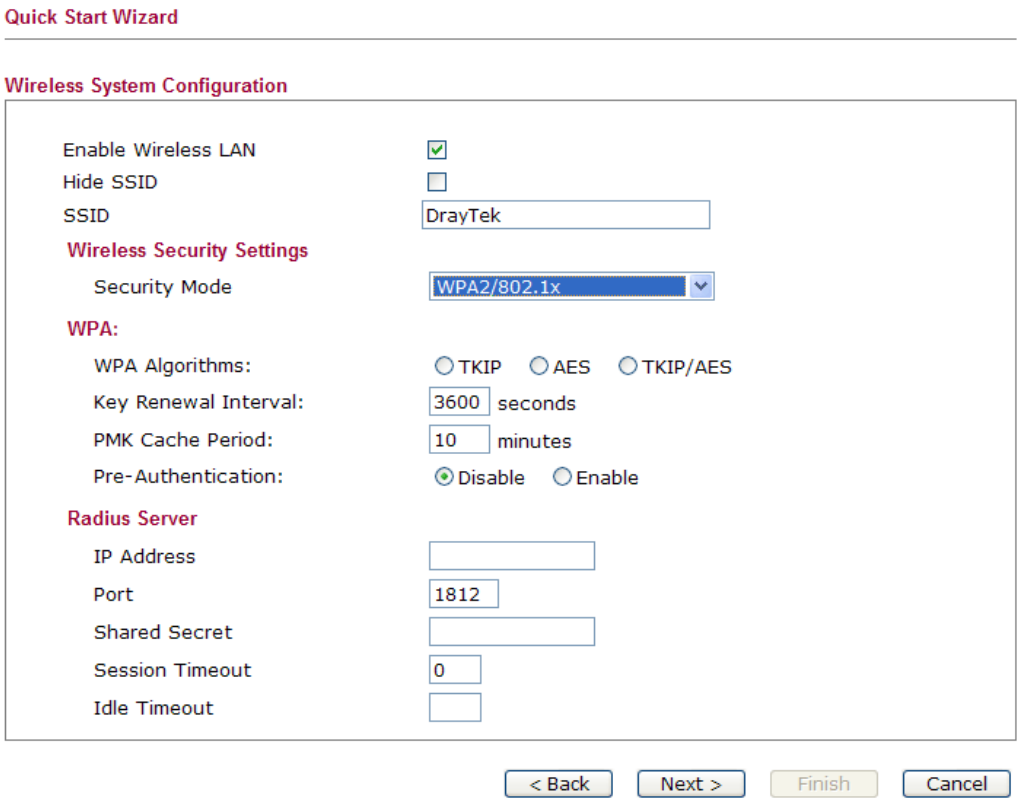
The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.



WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key.
IP Address	Enter the IP address of RADIUS server.
Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)
Idle Timeout	Set the maximum time that a wireless device may remain idle. (The unit is second.)

WPA2/802.1x

The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.

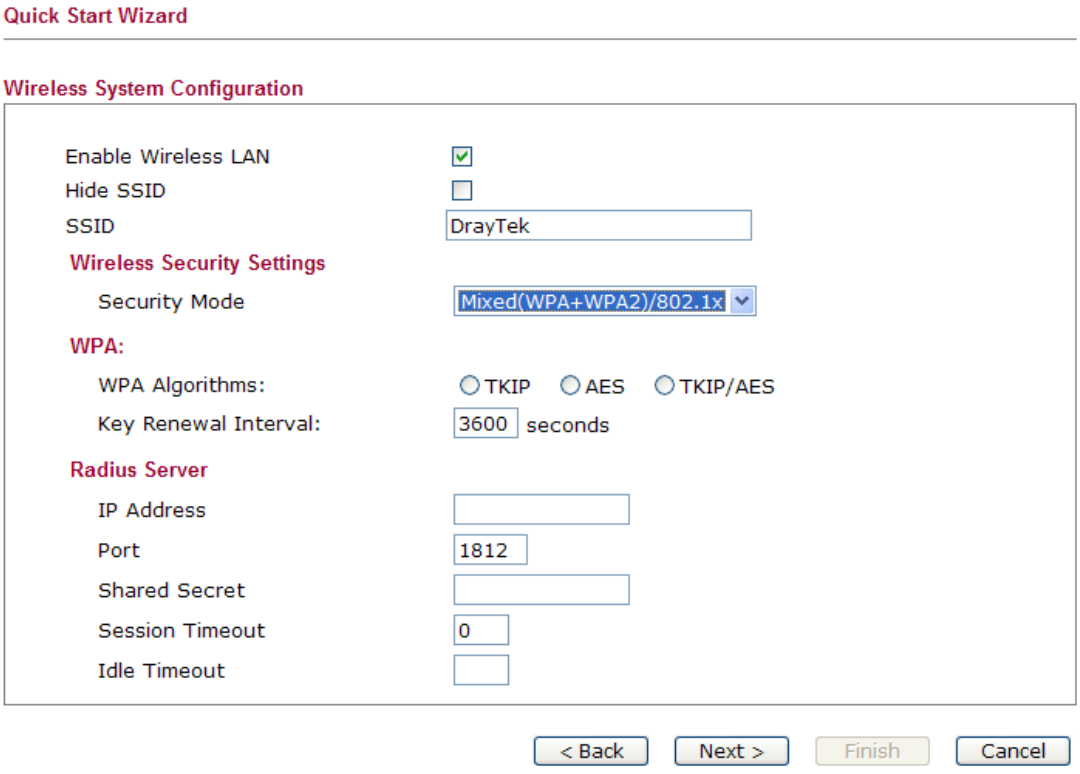


WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key.
PMK Cache Period	Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated.
Pre-Authentication	Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2) **Enable** - Enable IEEE 802.1X Pre-Authentication. **Disable** - Disable IEEE 802.1X Pre-Authentication.
IP Address	Enter the IP address of RADIUS server.
Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to

	authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)
Idle Timeout	Set the maximum time that a wireless device may remain idle. (The unit is second.)

Mixed (WPA+WPA2)/802.1x

The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.



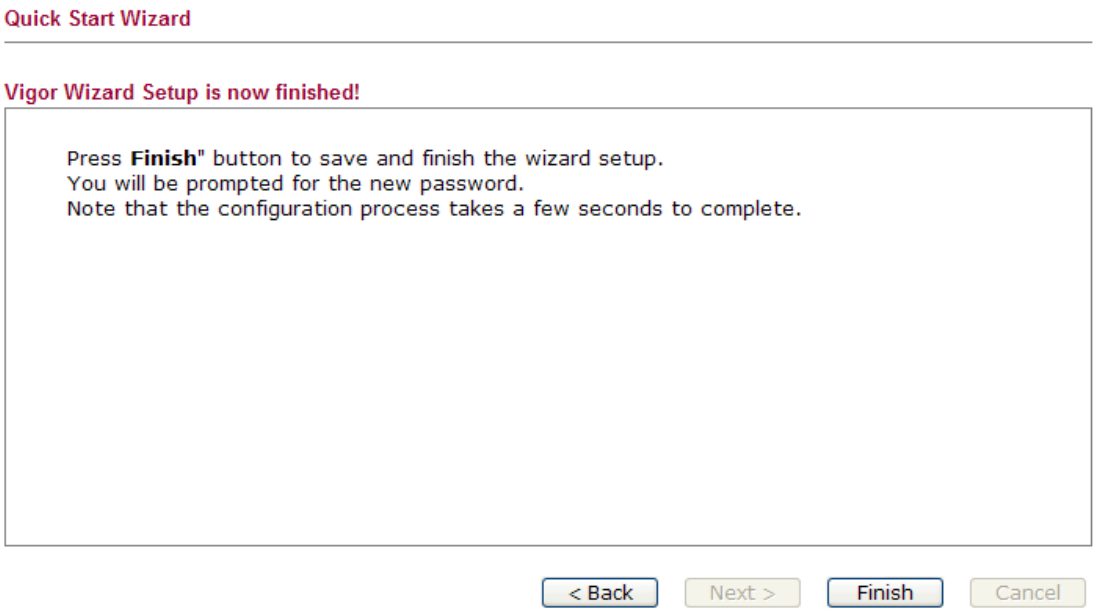
WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key.
IP Address	Enter the IP address of RADIUS server.
Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.

Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)
Idle Timeout	Set the maximum time that a wireless device may remain idle. (The unit is second.)

After finishing the settings here, please click **Next.**

2.4.5 Saving the Wizard Configuration

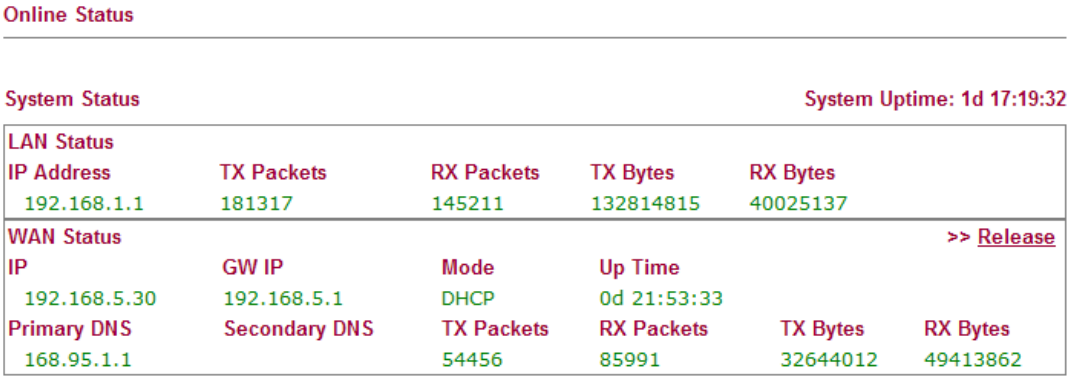
Now you can see the following screen. It indicates that the setup is complete. Different types of connection modes will have different summary. Click **Finish** and then restart the router.



2.5 Online Status

The online status shows the system status, WAN status, and other status related to this router within one page. If you select **PPPoE** as the protocol, you will find out a link of **Dial PPPoE** or **Drop PPPoE** in the Online Status web page.

Online status for DHCP



Detailed explanation is shown below:

LAN Status

IP Address	Displays the IP address of the LAN interface.
TX Packets	Displays the total transmitted packets at the LAN interface.
RX Packets	Displays the total number of received packets at the LAN interface.
WAN Status	
IP	Displays the IP address of the WAN interface.
GW IP	Displays the IP address of the default gateway.
Mode	Displays the type of WAN connection (e.g., PPPoE).
Up Time	Displays the total uptime of the interface.
Primary DNS	Displays the primary DNS setting.
Secondary DNS	Displays the secondary DNS setting.
TX Packets	Displays the total transmitted packets at the WAN interface.
TX Rate	Displays the speed of transmitted octets at the WAN interface.
RX Packets	Displays the total number of received packets at the WAN interface.
RX Rate	Displays the speed of received octets at the WAN interface.

Note: The words in green mean that the WAN connection of that interface is ready for accessing Internet; the words in red mean that the WAN connection of that interface is not ready for accessing Internet.

2.6 Saving Configuration

Each time you click **OK** on the web page for saving the configuration, you can find messages showing the system interaction with you.

Ready indicates the system is ready for you to input settings.

Settings Saved means your settings are saved once you click **Finish** or **OK** button.

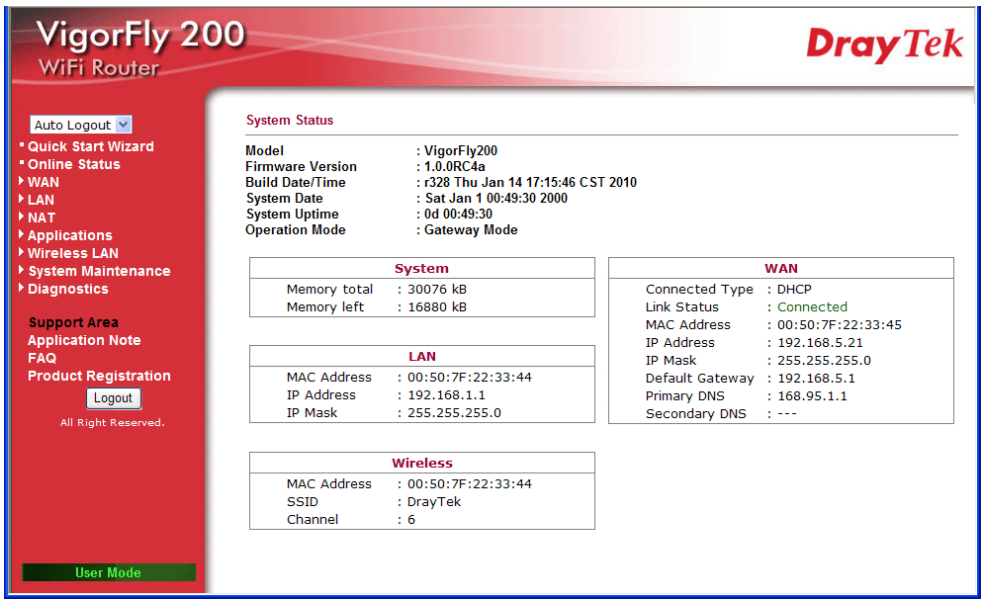
This page is left blank.

3 User Mode Operation

This chapter will guide users to execute simple configuration through user mode operation.

1. Open a web browser on your PC and type **http://192.168.1.1.** The window will ask for typing username and password.
2. **Do not** type any word (both username and password are Null for user operation) on the window and click **Login** on the window.

Now, the **Main Screen** will appear. Be aware that "User mode" will be displayed on the bottom left side.



3.1 WAN

Quick Start Wizard offers user an easy method to quick setup the connection mode for the router. Moreover, if you want to adjust more settings for different WAN modes, please go to **WAN** group.

Basics of Internet Protocol (IP) Network

IP means Internet Protocol. Every device in an IP-based Network including routers, print server, and host PCs, needs an IP address to identify its location on the network. To avoid address conflicts, IP addresses are publicly registered with the Network Information Centre (NIC). Having a unique IP address is mandatory for those devices participated in the public network but not in the private TCP/IP local area networks (LANs), such as host PCs under the management of a router since they do not need to be accessed by the public. Hence, the NIC has reserved certain addresses that will never be registered publicly. These are known as ***private*** IP addresses, and are listed in the following ranges:

From 10.0.0.0 to 10.255.255.255
From 172.16.0.0 to 172.31.255.255
From 192.168.0.0 to 192.168.255.255

What are Public IP Address and Private IP Address

As the router plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor router. The router itself will also use the default **private IP** address: 192.168.1.1 to communicate with the local hosts. Meanwhile, Vigor router will communicate with other network devices through a **public IP** address. When the data flow passing through, the Network Address Translation (NAT) function of the router will dedicate to translate public/private addresses, and the packets will be delivered to the correct host PC in the local area network. Thus, all the host PCs can share a common Internet connection.

Get Your Public IP Address from ISP

In ADSL deployment, the PPP (Point to Point)-style authentication and authorization is required for bridging customer premises equipment (CPE). Point to Point Protocol over Ethernet (PPPoE) connects a network of hosts via an access device to a remote access concentrator or aggregation concentrator. This implementation provides users with significant ease of use. Meanwhile it provides access control, billing, and type of service according to user requirement.

When a router begins to connect to your ISP, a serial of discovery process will occur to ask for a connection. Then a session will be created. Your user ID and password is authenticated via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information will usually be assigned by your ISP.

Network Connection by 3G USB Modem

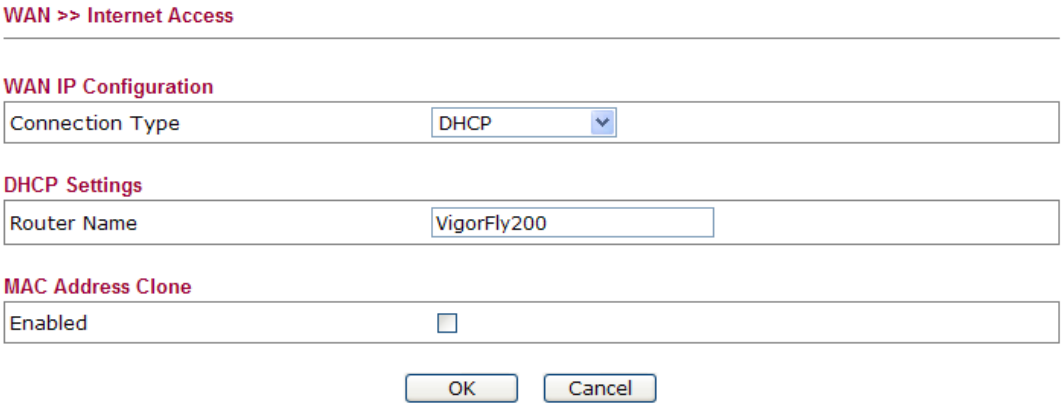
For 3G mobile communication through Access Point is popular more and more, Vigor router adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor router, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor router with 3G USB Modem allows you to receive 3G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use four LAN ports on the router to access Internet. Also, they can access Internet via wireless function of Vigor router, and enjoy the powerful firewall, bandwidth management features of Vigor router.

3G USB Modem can be used as backup device. Therefore, when WAN is not available, the router will use 3G USB Modem for supporting automatically. The supported 3G USB Modem will be listed on DrayTek web site. Please visit www.draytek.com for more detailed information.

Below shows the menu items for **WAN**.

3.1.1 Internet Access

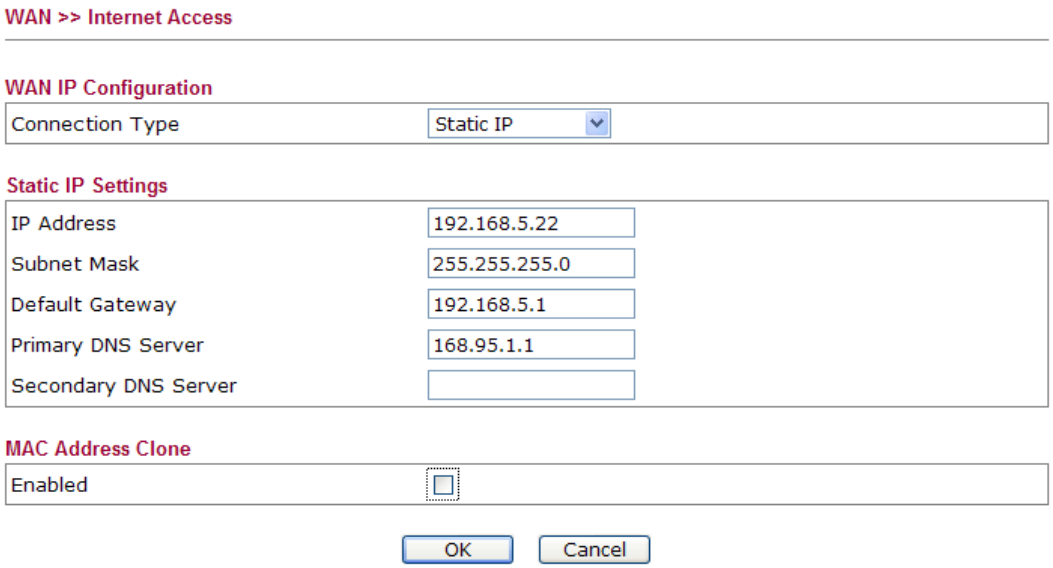
This page allows you to set WAN configuration with different modes. Use the **Connection Type** drop down list to choose one of the WAN modes. The corresponding page will be displayed.



Static IP

For static IP mode, you usually receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your DSL or Cable ISP service providers. In most cases, a Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you have a public subnet, you could assign an IP address or many IP address to the WAN interface.

To use **Static** as the accessing protocol of the internet, please choose **Static IP** mode from **Connection Type** drop down menu. The following web page will be shown.



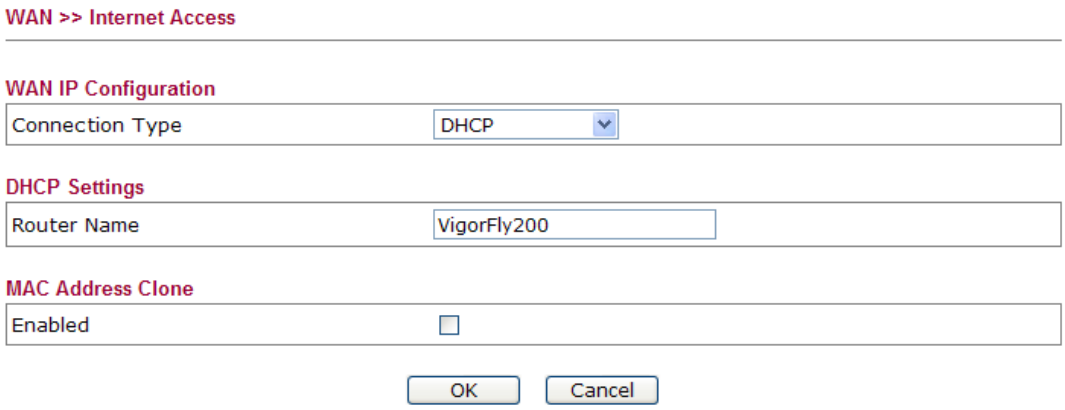
IP Address	Type the IP address.
Subnet Mask	Type the subnet mask.
Default Gateway	Type the gateway IP address.
Primary DNS Server	You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will

	automatically apply default DNS Server IP address: 198.95.1.1 to this field.
Secondary DNS Server	You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address.
MAC Address Clone	**MAC Address Clone** is available when the box of **Enable** is checked. The router will detect the MAC address automatically. The result will be displayed in the field of MAC Address.

After finishing all the settings here, please click **OK** to activate them.

DHCP

DHCP allows a user to obtain an IP address automatically from a DHCP server on the Internet. If you choose **DHCP** mode, the DHCP server of your ISP will assign a dynamic IP address for your router automatically. It is not necessary for you to assign any setting,



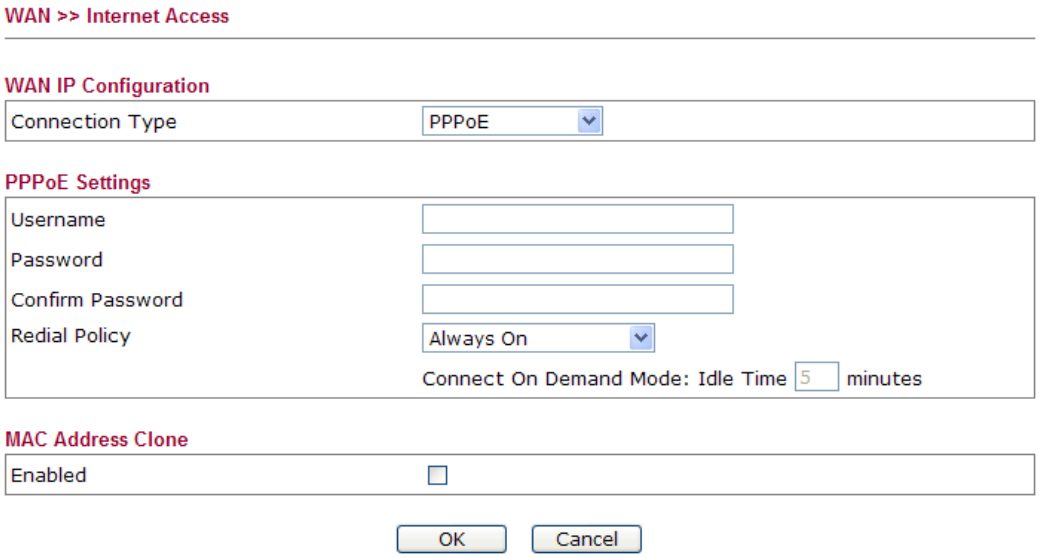
Router Name Type in a name for the router. It must be the same as the name used in Syslog.

MAC Address Clone **MAC Address Clone** is available when the box of **Enable** is checked. The router will detect the MAC address automatically. The result will be displayed in the field of MAC Address.

After finishing all the settings here, please click **OK** to activate them.

PPPoE

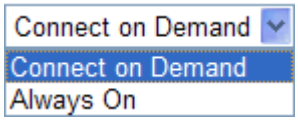
To choose PPPoE as the accessing protocol of the internet, please select **PPPoE** from the **Internet Access** menu. The following web page will be shown.



Username Type in the username provided by ISP in this field.

Password Type in the password provided by ISP in this field.

Redial Policy If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, choose **Connect on Demand**.



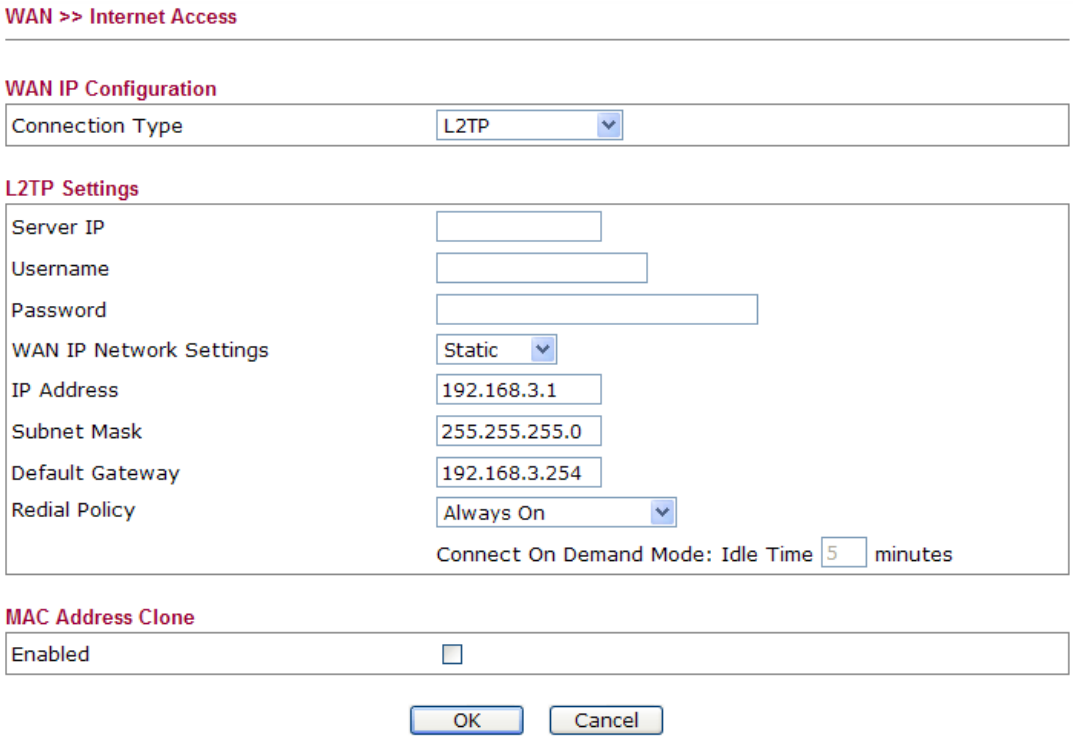
Idle Time - Set the timeout for breaking down the Internet after passing through the time without any action. When you choose **Connect on Demand,** you have to type value here.

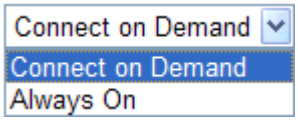
MAC Address Clone **MAC Address Clone** is available when the box of **Enable** is checked. The router will detect the MAC address automatically. The result will be displayed in the field of MAC Address.

After finishing all the settings here, please click **OK** to activate them.

PPTP/L2TP

To use **PPTP/L2TP** as the accessing protocol of the internet, please choose **PPTP/L2TP** from **Connection Type** drop down menu. The following web page will be shown.



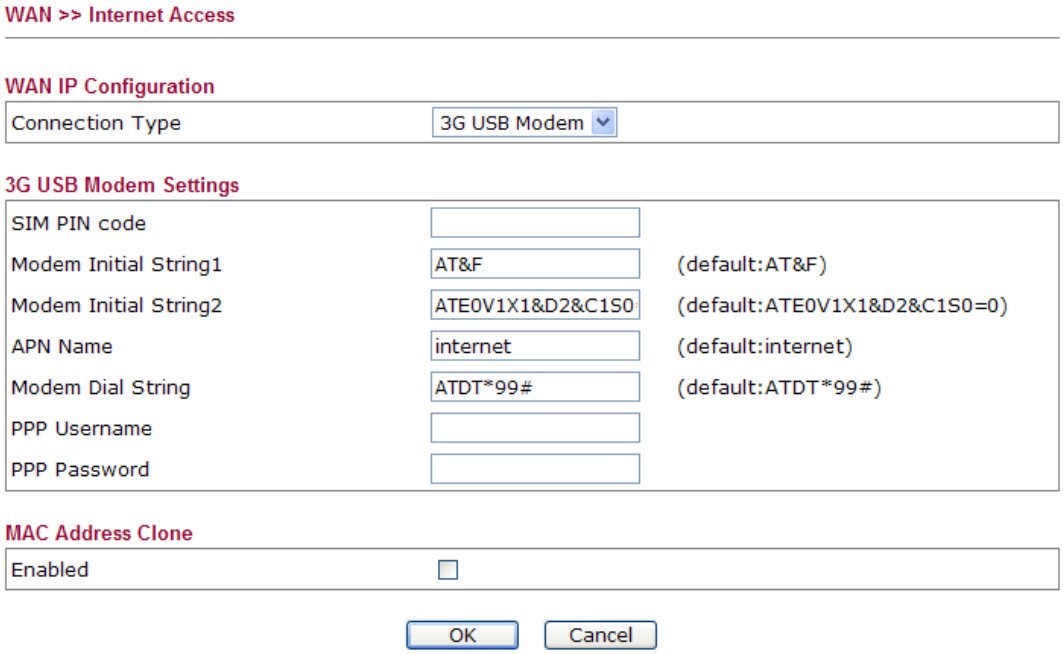
Server IP	Type in the IP address of the **PPTP/L2TP** server.
User Name	Type in the username provided by ISP in this field.
Password	Type in the password provided by ISP in this field.
Address Mode	You can choose **Static IP** or **DHCP** as WAN IP network setting.
IP Address	Type the IP address if you choose Static IP as the WAN IP network setting.
Subnet Mask	Type the subnet mask if you chose Static IP as the WAN IP.
Default Gateway	Type the gateway address for this router.
Redial Policy	If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, choose **Connect on Demand.**  **Idle Time -** Set the timeout for breaking down the Internet after passing through the time without any action. When you choose **Connect on Demand,** you have to type value here.
MAC Address Clone	**MAC Address Clone** is available when the box of **Enable** is checked. The router will detect the MAC address automatically. The result will be displayed in the field of

MAC Address.

After finishing all the settings here, please click **OK** to activate them.

3G USB Modem

If your router connects to a 3G modem and you want to access Internet via 3G modem, choose 3G as connection type and type the required information in this web page.



SIM PIN code — Type PIN code of the SIM card that will be used to access Internet.

Modem Initial String1/2 — Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.

APN Name — APN means Access Point Name which is provided and required by some ISPs.

Modem Dial String — Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.

PPP Username — Type the PPP username (optional).

PPP Password — Type the PPP password (optional).

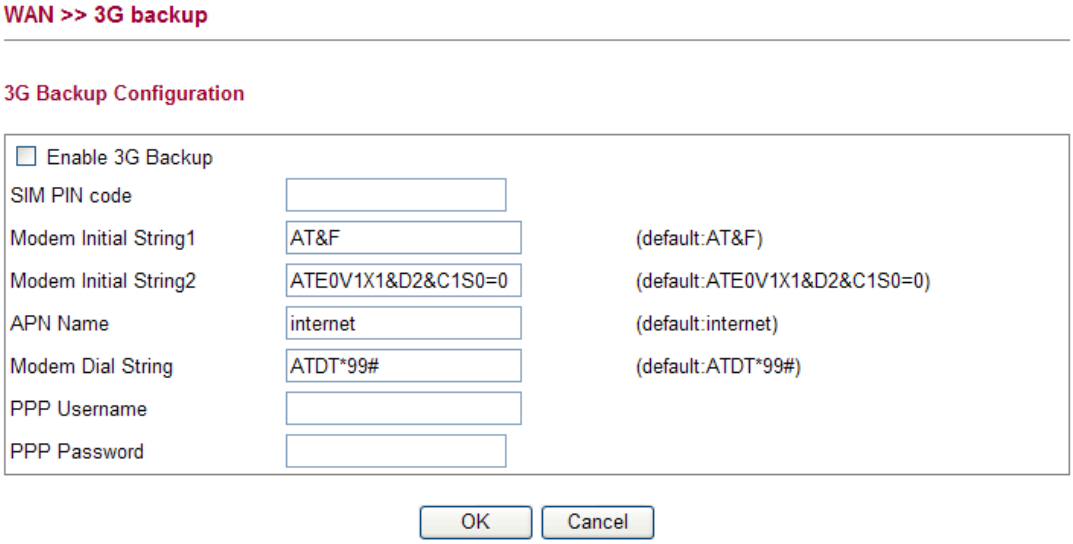
MAC Address Clone — **MAC Address Clone** is available when the box of **Enable** is checked. The router will detect the MAC address automatically. The result will be displayed in the field of MAC Address.

.

After finishing all the settings here, please click **OK** to activate them.

3.1.2 3G Backup

This page is used to setup 3G backup function. If you enable 3G backup, make sure your WAN connection type is not in 3G mode. When the WAN connection is broken, router will try to keep the connection with 3G mode. After WAN connection is recovered, router will disconnect the 3G connection automatically.



Enable 3G Backup	Check this box to enable the 3G backup feature.
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet.
Modem Initial String1/2	Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.
APN Name	APN means Access Point Name which is provided and required by some ISPs.
Modem Dial String	Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.
PPP Username	Type the PPP username (optional).
PPP Password	Type the PPP password (optional).

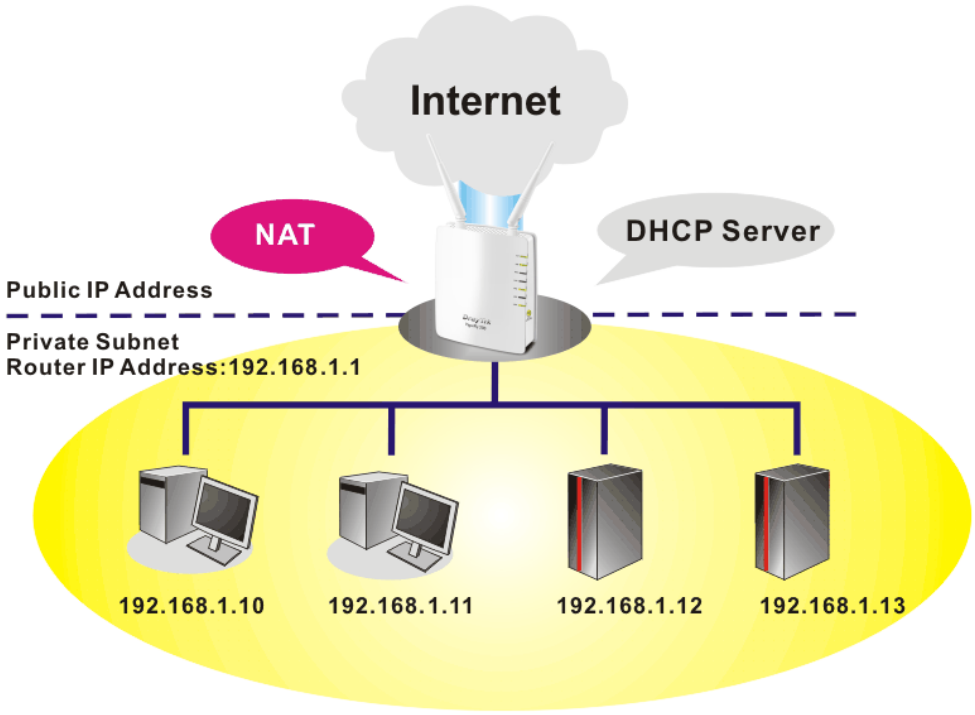
After finishing all the settings here, please click **OK** to activate them.

3.2 LAN

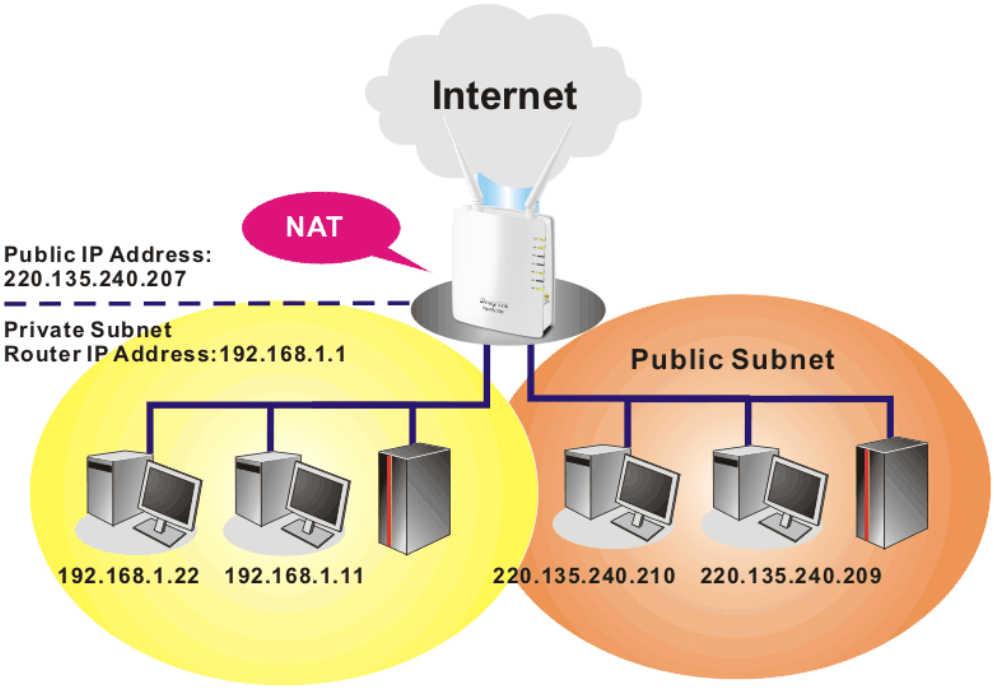
Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

Basics of LAN

The most generic function of Vigor router is NAT. It creates a private subnet of your own. As mentioned previously, the router will talk to other public hosts on the Internet by using public IP address and talking to local hosts by using its private IP address. What NAT does is to translate the packets from public IP address to private IP address to forward the right packets to the right host and vice versa. Besides, Vigor router has a built-in DHCP server that assigns private IP address to each local host. See the following diagram for a briefly understanding.



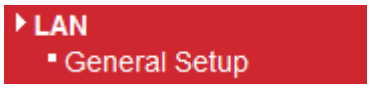
In some special case, you may have a public IP subnet from your ISP such as 220.135.240.0/24. This means that you can set up a public subnet or call second subnet that each host is equipped with a public IP address. As a part of the public subnet, the Vigor router will serve for IP routing to help hosts in the public subnet to communicate with other public hosts or servers outside. Therefore, the router should be set as the gateway for public hosts.



What is Routing Information Protocol (RIP)

Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

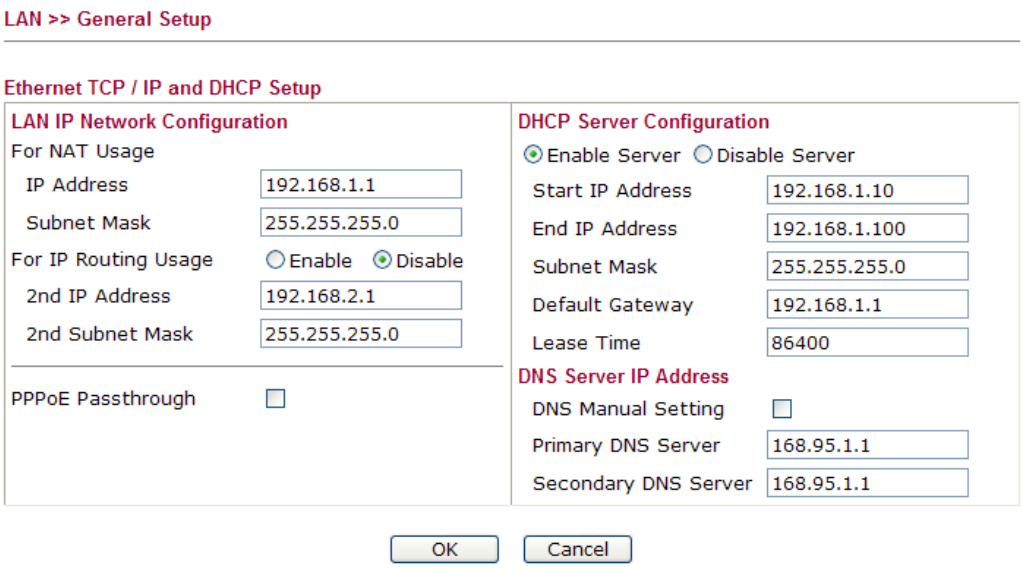
Below shows the LAN menu:



3.2.1 General Setup

This page provides you the general settings for LAN.

Click **LAN** to open the LAN settings page and choose **General Setup**.



IP Address Type in private IP address for connecting to a local private

	network (Default: 192.168.1.1).
Subnet Mask	Type in an address code that determines the size of the network. (Default: 255.255.255.0)
For IP Routing Usage	Click **Enable** to invoke this function. The default setting is **Disable**.
2nd IP Address	Type in secondary IP address for connecting to a subnet. (Default: 192.168.2.1)
2nd Subnet Mask	An address code that determines the size of the network.
PPPoE Passthrough	If you want to use PPPoE server in the network via Vigor router, please check this box to redirect the PPPoE frames to the specified location.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network. If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
Enable Server	Let the router assign IP address to every host in the LAN.
Disable Server	Let you manually assign IP address to every host in the LAN.
Start IP Address	Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.
End IP Address	Enter a value of the IP address pool for the DHCP server to end with when issuing IP addresses.
Subnet Mask	Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
Default Gateway	Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.
Lease Time	It allows you to set the leased time for the specified PC.
DNS Manual Setting	If this function is enabled, LAN PCs use Primary DNS Server and Secondary DNS Server as their DNS servers. Otherwise, LAN PCs use the router as their DNS server and the router will do DNS proxy for them.
Primary DNS Address	You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
Secondary DNS Address	You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will

automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.

If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.

If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.

After finishing all the settings here, please click **OK** to activate them.

3.3 NAT

Usually, the router serves as an NAT (Network Address Translation) router. NAT is a mechanism that one or more private IP addresses can be mapped into a single public one. Public IP address is usually assigned by your ISP, for which you may get charged. Private IP addresses are recognized only among internal hosts.

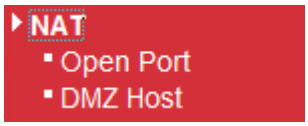
When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize this address/port-mapping relationship. When the public server response, the incoming traffic, of course, is destined to the router's public IP address and the router will do the inversion based on its table. Therefore, the internal host can communicate with external host smoothly.

The benefit of the NAT includes:

- **Save cost on applying public IP address and apply efficient usage of IP address.** NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- **Enhance security of the internal network by obscuring the IP address.** There are many attacks aiming victims based on the IP address. Since the attacker cannot be aware of any private IP addresses, the NAT function can protect the internal network.

On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by using port mapping methods.

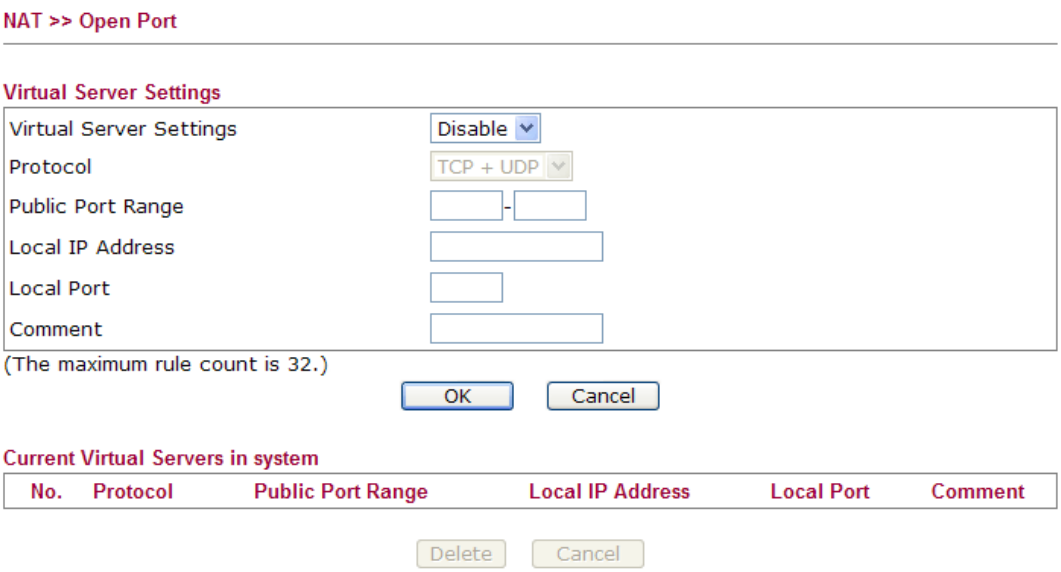
Below shows the menu items for NAT.



3.3.1 Open Ports

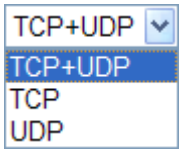
Open Ports allows you to open a range of ports for the traffic of special applications.

Common application of Open Ports includes P2P application (e.g., BT, KaZaA, Gnutella, WinMX, eMule and others), Internet Camera etc. Ensure that you keep the application involved up-to-date to avoid falling victim to any security exploits.



Virtual Server Settings — Choose **Enable** to invoke this setting.

Protocol — Specify the transport layer protocol. It could be **TCP**, **UDP** and **TCP+UDP**.



Public Port Range — Specify the starting port number and ending port number of the service offered by the local host.

Local IP Address — Enter the private IP address of the local host.

Local Port — If it is configured, the forwarded traffic is mapped to this port on the local host.

Comment — Type words as notification for such virtual server.

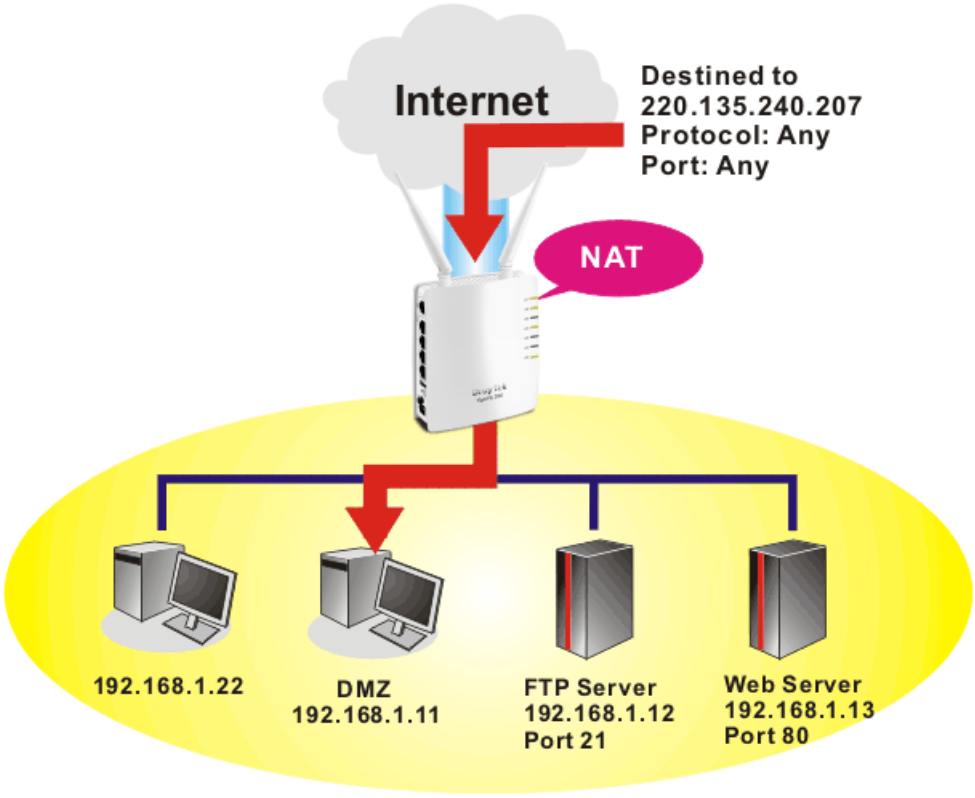
OK — When you finish the above settings, simply click this button to save it and display on the field of **Current Virtual Servers in system**.

Cancel — Click this button to clear current configuration.

Delete — Click this button to remove the selected virtual server configuration.

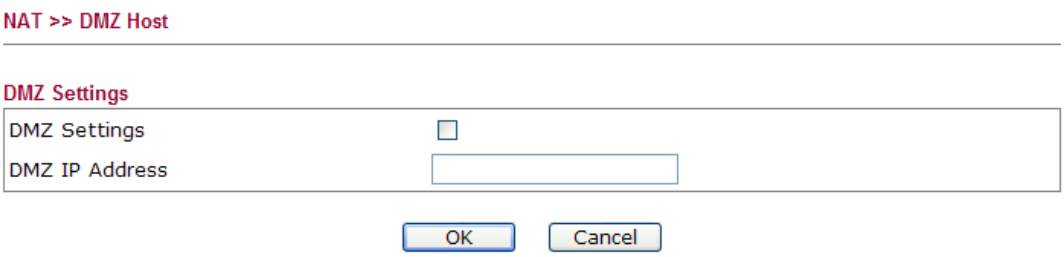
3.3.2 DMZ Host

Vigor router provides a facility **DMZ Host** that maps ALL unsolicited data on any protocol to a single host in the LAN. Regular web surfing and other such Internet activities from other clients will continue to work without inappropriate interruption. **DMZ Host** allows a defined internal user to be totally exposed to the Internet, which usually helps some special applications such as Netmeeting or Internet Games etc.



Note: The security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

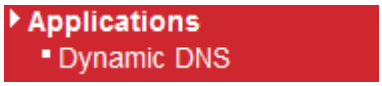
Click **DMZ Host** to open the following page:



DMZ Settings	Check this box to enable the DMZ Host function.
DMZ IP Address	Enter the private IP address of the DMZ host.
OK	Click this button to save such profile.
Cancel	Click this button to clear information on this page.

3.4 Applications

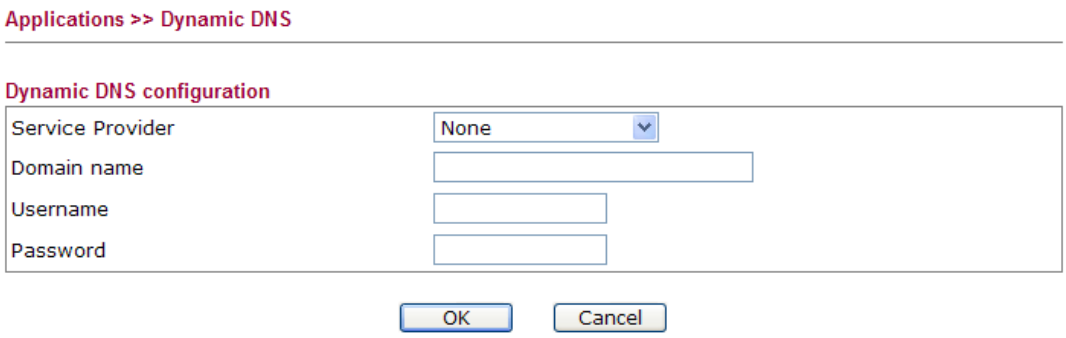
Below shows the menu items for Applications.



3.4.1 Dynamic DNS

The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router to update its online WAN IP address mappings on the specified Dynamic DNS server. Once the router is online, you will be able to use the registered domain name to access the router or internal virtual servers from the Internet. It is particularly helpful if you host a web server, FTP server, or other server behind the router.

Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The router provides up to three accounts from three different DDNS service providers. Basically, Vigor routers are compatible with the DDNS services supplied by most popular DDNS service providers such as **www.dyndns.org, www.no-ip.com, www.dtdns.com, www.changeip.com, www.dynamic- nameserver.com.** You should visit their websites to register your own domain name for the router.



Service Provider	Select the service provider for the DDNS account. If you choose **None**, such function will be disabled.
Domain name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
Username	Type in the login name that you set for applying domain.
Password	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.

Click **OK** button to activate the settings. You will see your setting has been saved.

3.5 Wireless LAN

3.5.1 Basic Concepts

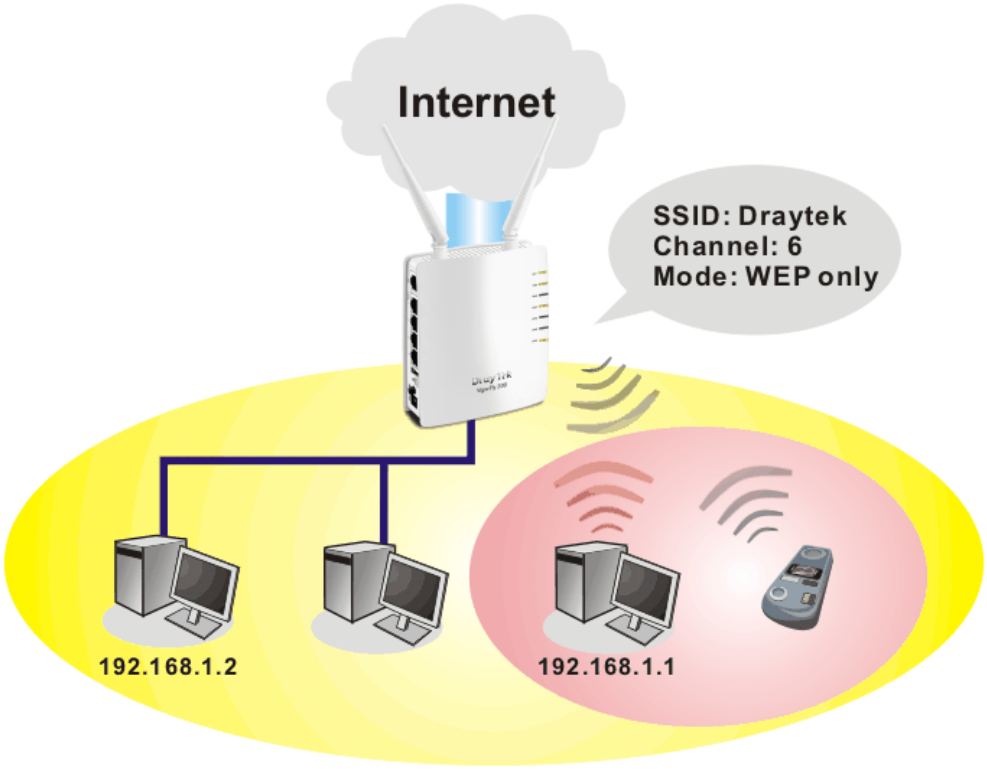
Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor router is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling

holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps*. Hence, you can finally smoothly enjoy stream music and video.

Note: * The actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via Vigor wireless router. The **General Settings** will set up the information of this wireless network, including its SSID as identification, located channel etc.



Security Overview

Real-time Hardware Encryption: Vigor Router is equipped with a hardware AES encryption engine so it can apply the highest protection to your data without influencing user experience.

Complete Security Standard Selection: To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

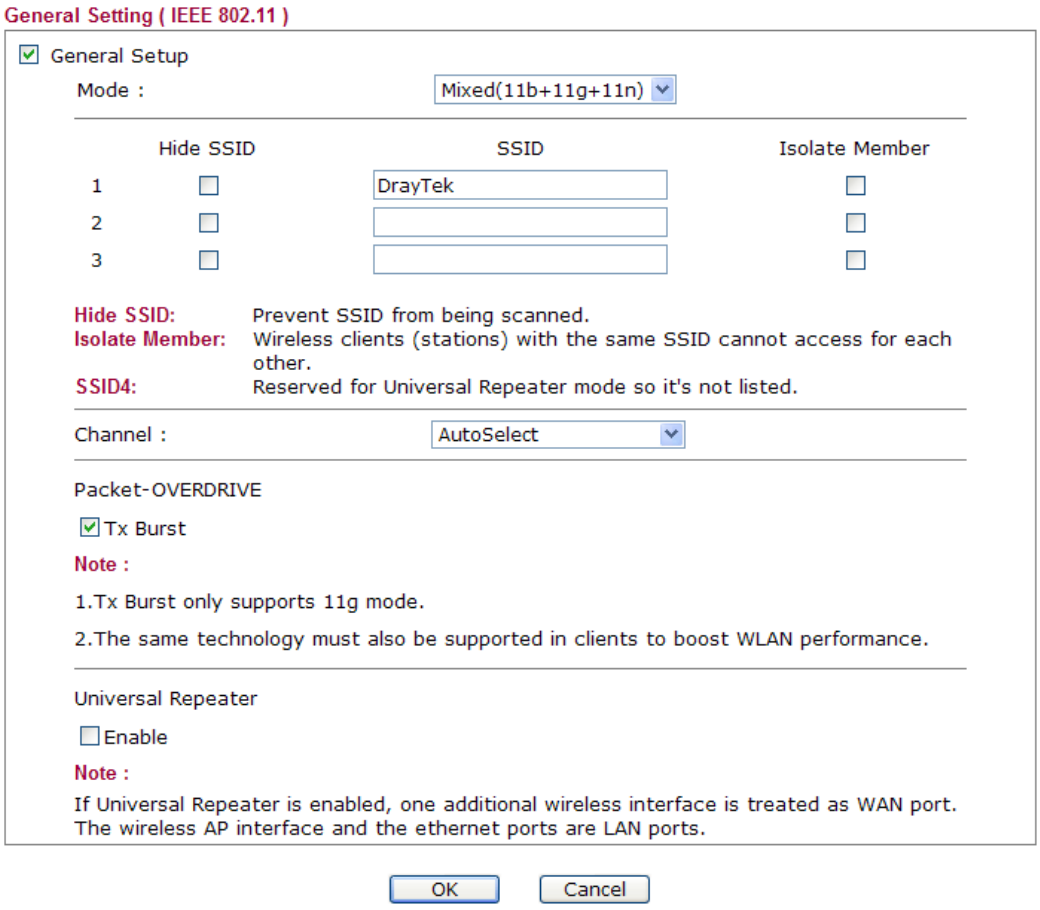
Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The Vigor wireless router is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

Below shows the menu items for Wireless LAN.

3.5.2 General Setup

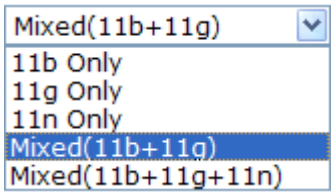
By clicking the **General Setup**, a new web page will appear so that you could configure the SSID and the wireless channel.

Please refer to the following figure for more information.



Enable Wireless LAN Check the box to enable wireless function.

Mode At present, the router can connect to Mixed (11b+11g), 11g Only, 11b Only, 11n Only and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mix (11b+11g+11n) mode.

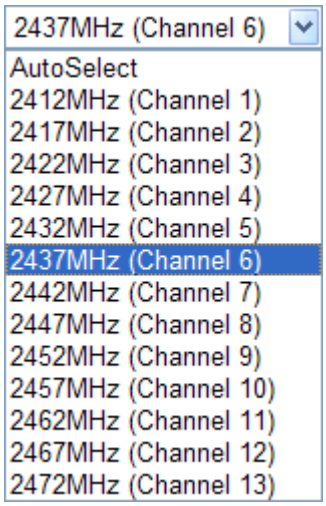


Hide SSID Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set three sets of SSID for different usage.

SSID Set a name for the router to be identified.

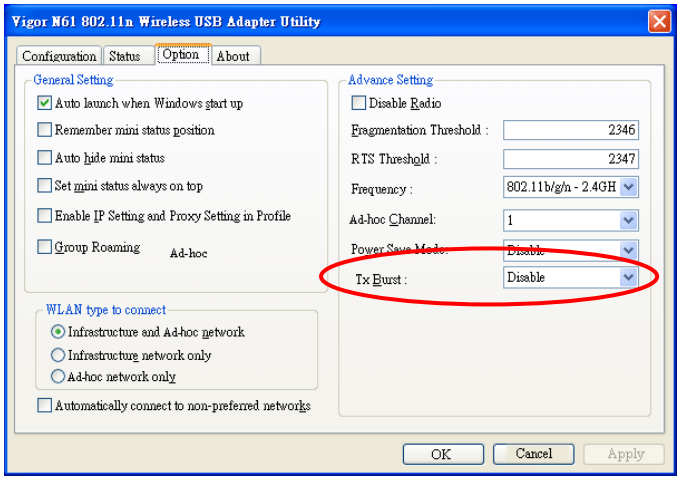
Isolate Member Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.

Channel Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select AutoSelect to let system determine for you.



Packet-OVERDRIVE This feature can enhance the performance in data transmission about 40%* more (by checking **Tx Burst**). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.

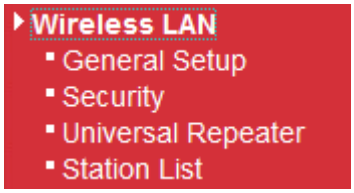
Note: Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose **Enable** for **TxBurst** on the tab of **Option**).



Universal Repeater

If such mode is enabled, the access point can act as a wireless repeater; it can be Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to service all wireless stations within its coverage.

Check this box to enable the function. Besides, it will be displayed on the **Wireless LAN** for you to access for detailed configuration.

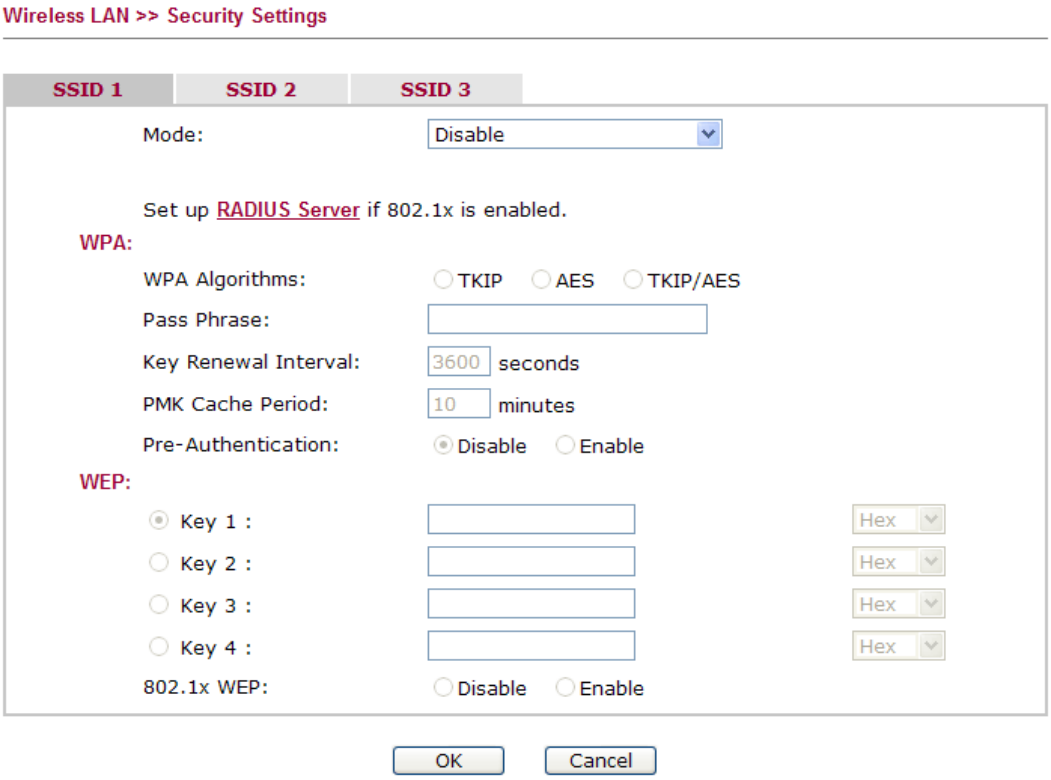


Open Wireless **LAN>>Universal Repeater**. Please refer to the corresponding section for detailed information.

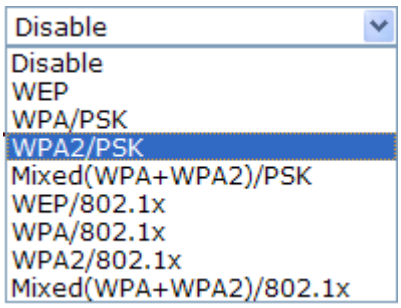
3.5.3 Security

This page allows you to set security with different modes for SSID 1, 2 and 3 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

By clicking the **Security Settings**, a new web page will appear so that you could configure the settings.



Mode There are several modes provided for you to choose.

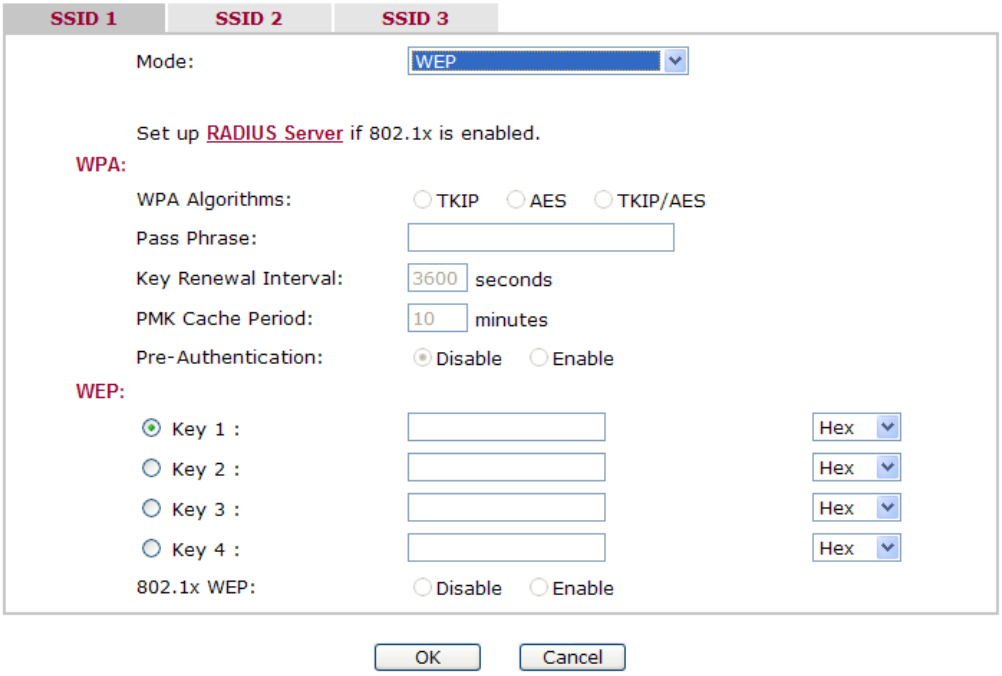


- **Disable**

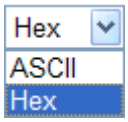
  The encryption mechanism is turned off.

- **WEP**

  Accepts only WEP clients and the encryption key should be entered in WEP Key.

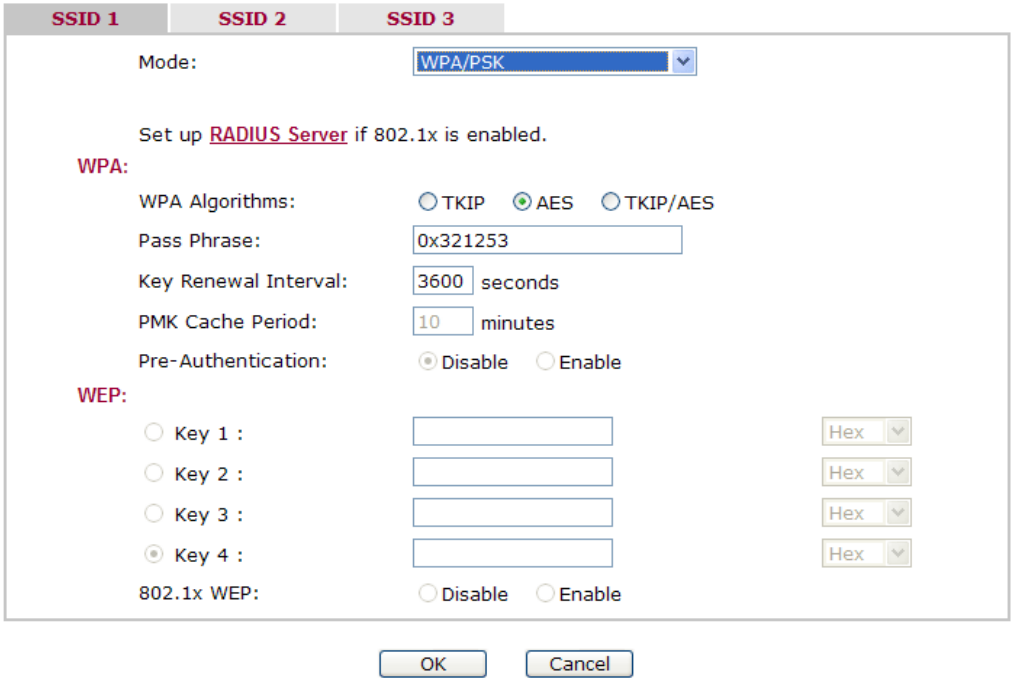


WEP Key1-Key4 Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','.



- **WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK**

  Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.

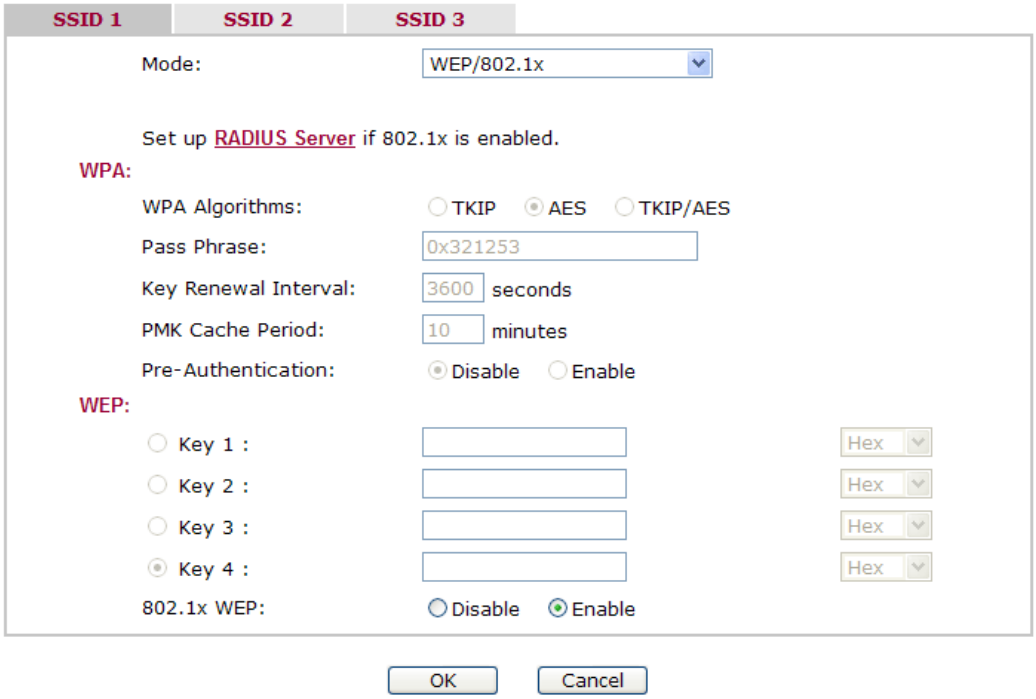


WPA Algorithm	Select TKIP, AES or TKIP/AES as the algorithm for WPA.
Pass Phrase	Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key.

- **WEP/802.1x**

  The built-in RADIUS client feature enables the router to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.

  The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode.

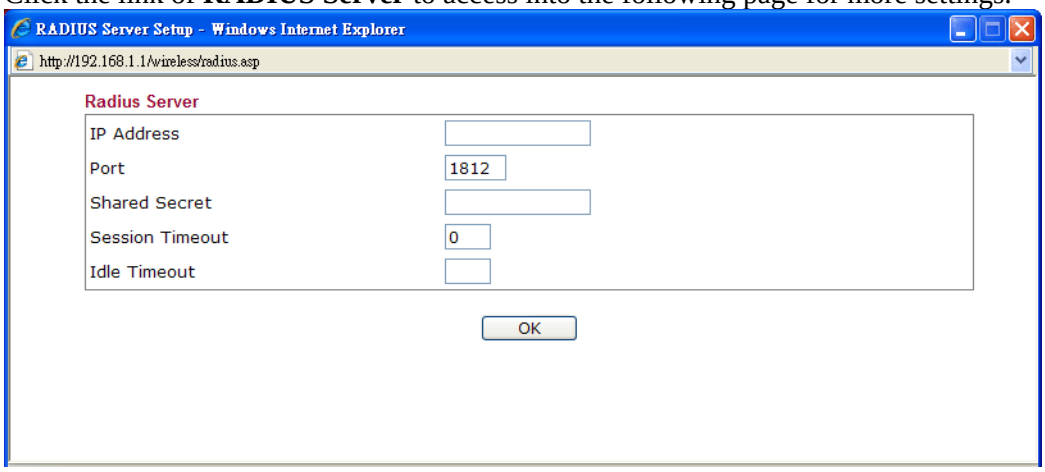


802.1x WEP

Disable - Disable the WEP Encryption. Data sent to the AP will not be encrypted.

Enable - Enable the WEP Encryption.

Click the link of **RADIUS Server** to access into the following page for more settings.



IP Address Enter the IP address of RADIUS server.

Port The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.

Shared Secret The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.

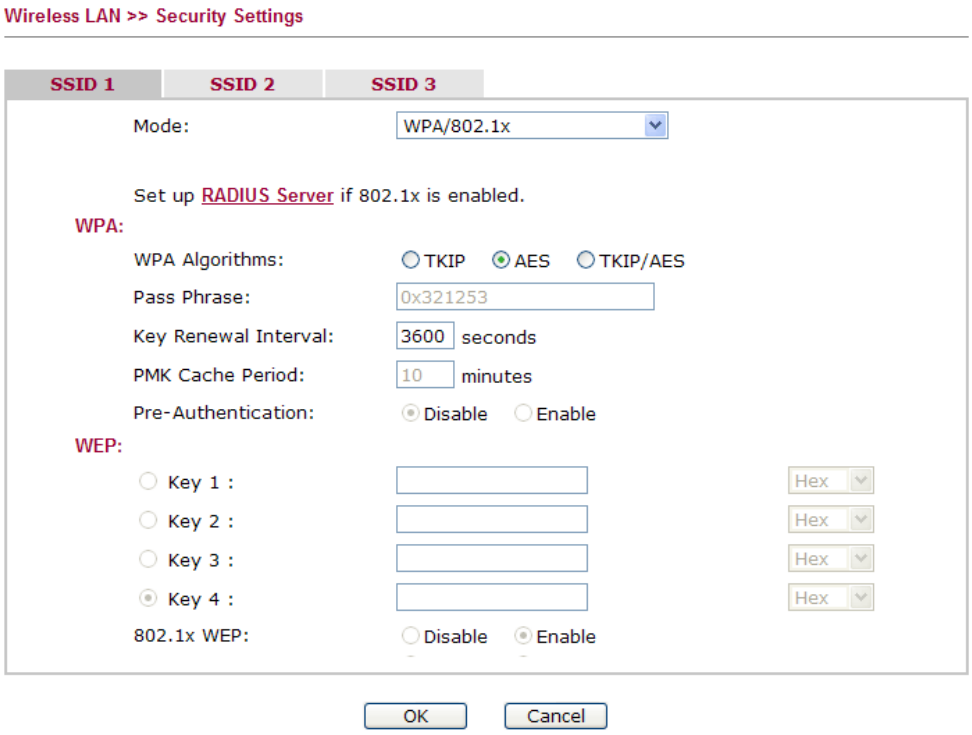
Session Timeout Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)

Idle Timeout Set the maximum time that a wireless device may remain

idle. (The unit is second.)

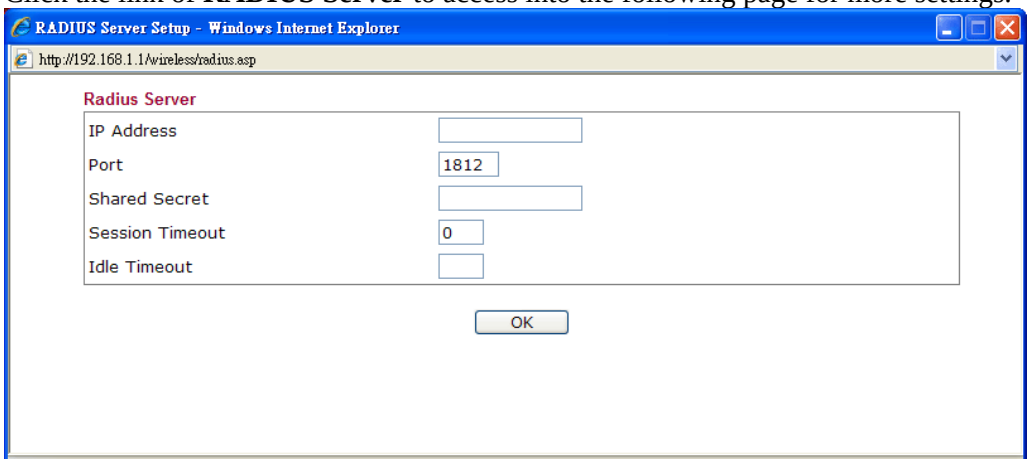
- **WPA/802.1x**

The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.



WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key.

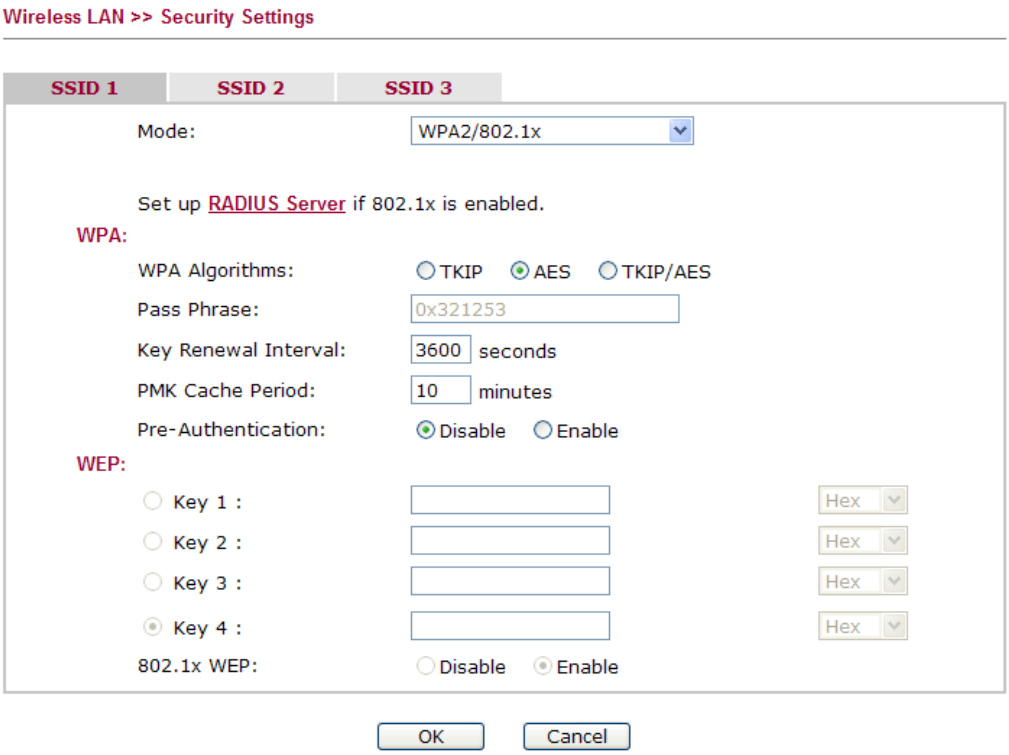
Click the link of **RADIUS Server** to access into the following page for more settings.



IP Address	Enter the IP address of RADIUS server.
Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)
Idle Timeout	Set the maximum time that a wireless device may remain idle. (The unit is second.)

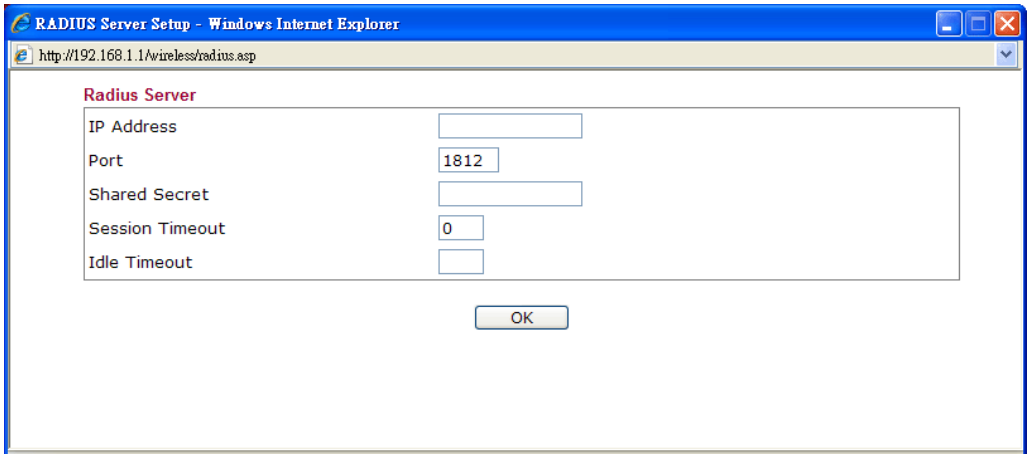
- **WPA2/802.1x**

The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.



WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key.
PMK Cache Period	Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated.
Pre-Authentication	Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2) **Enable** - Enable IEEE 802.1X Pre-Authentication. **Disable** - Disable IEEE 802.1X Pre-Authentication.

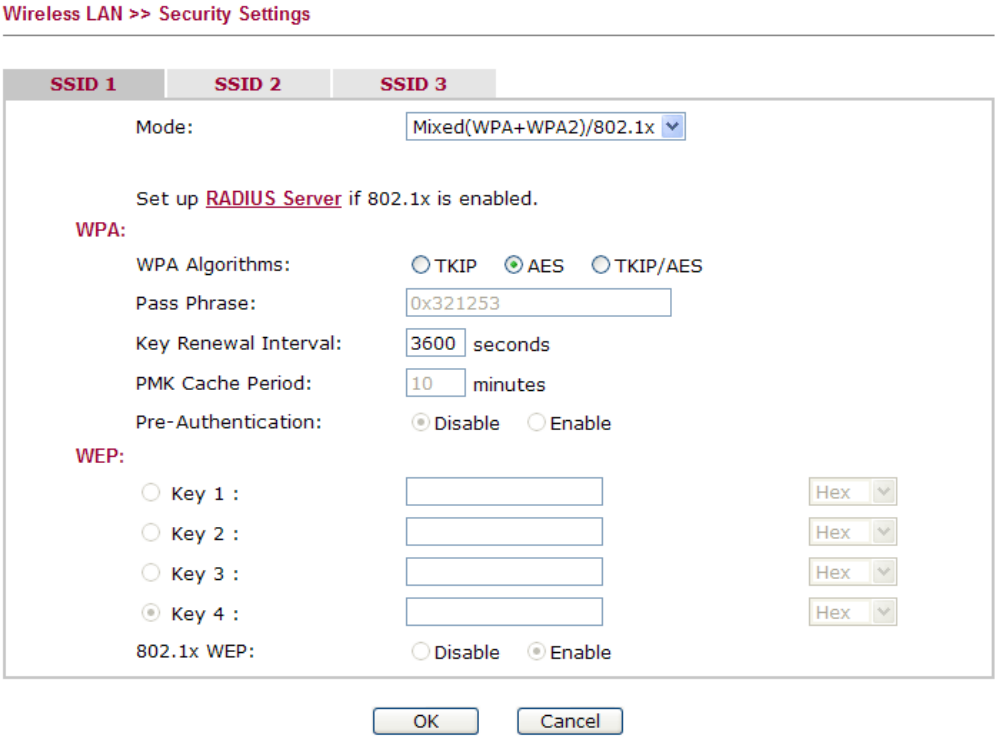
Click the link of **RADIUS Server** to access into the following page for more settings.



IP Address	Enter the IP address of RADIUS server.
Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)
Idle Timeout	Set the maximum time that a wireless device may remain idle. (The unit is second.)

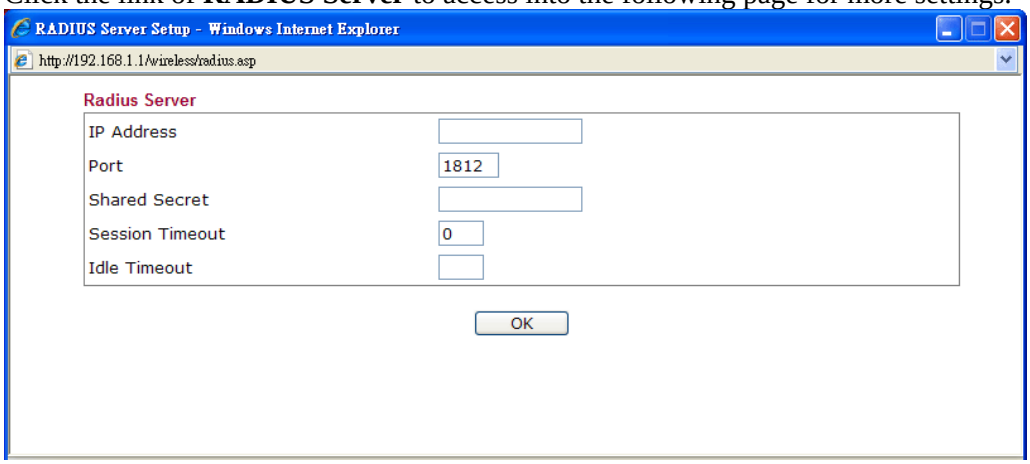
- **Mixed (WPA+WPA2)/802.1x**

  The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.



WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key.?

Click the link of **RADIUS Server** to access into the following page for more settings.



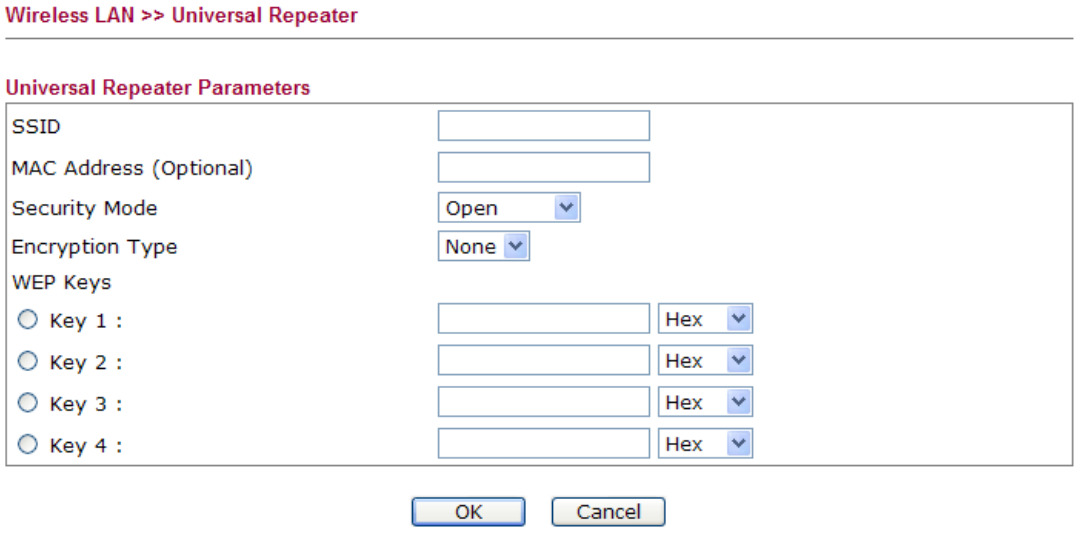
IP Address	Enter the IP address of RADIUS server.
Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.

Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)
Idle Timeout	Set the maximum time that a wireless device may remain idle. (The unit is second.)

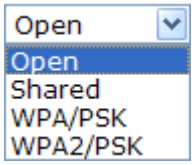
3.5.4 Universal Repeater

This menu is available only when it is enabled in **Wireless LAN>>General Setup**. It allows you to specify which AP that remote client can connect to. VigorFly 200 can act as a wireless repeater; it can be Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to serve all wireless stations within its coverage.

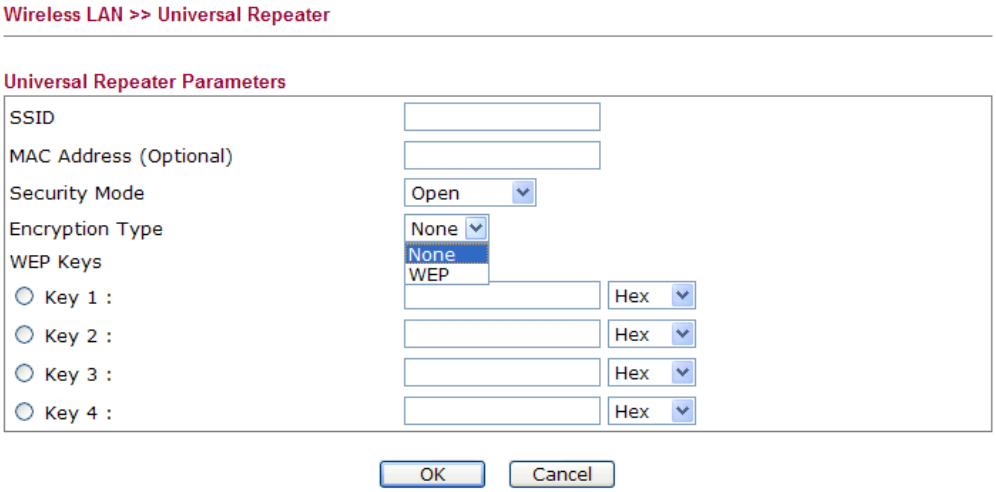
> **Note:** While using Universal Repeater Mode, the access point will demodulate the received signal. Please check if this signal is noise for the operating network, then have the signal modulated and amplified again. The output power of this mode is the same as that of WDS and normal AP mode.



SSID	Set a name for the router to be identified.
MAC Address (Optional)	Type the MAC address of the Access Point that VigorFly 200 wants to connect to.
Security Mode	There are several modes provided for you to choose. Each mode will bring up different parameters (e.g., WEP keys, Pass Phrase) for you to configure.

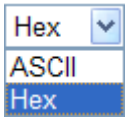


- **Open / Shared Mode**

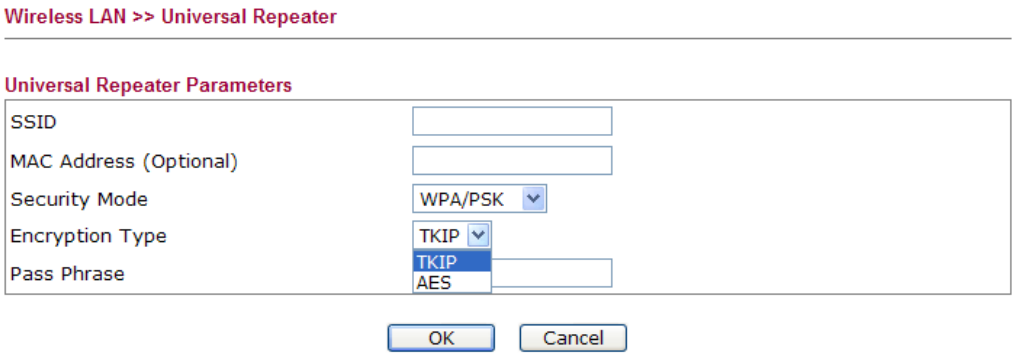


Encryption Type Choose **None** to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose **WEP**.

WEP Keys Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','.



- **WPA/PSK Mode and WPA2/PSK Mode**



Encryption Type Select TKIP or AES as the algorithm for WPA.

Pass Phrase Either **8~63** ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

3.5.5 Station List

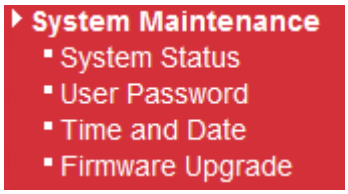
Station List provides the knowledge of connecting wireless clients now along with its status code.

MAC Address	Display the MAC Address for the connecting client.
SSID	Display the SSID of the connecting client.
Auth	Display the authentication mode of the connecting client.
Encrypt	Display the encryption method of the connecting client.
Refresh	Click this button to refresh current page.

3.6 System Maintenance

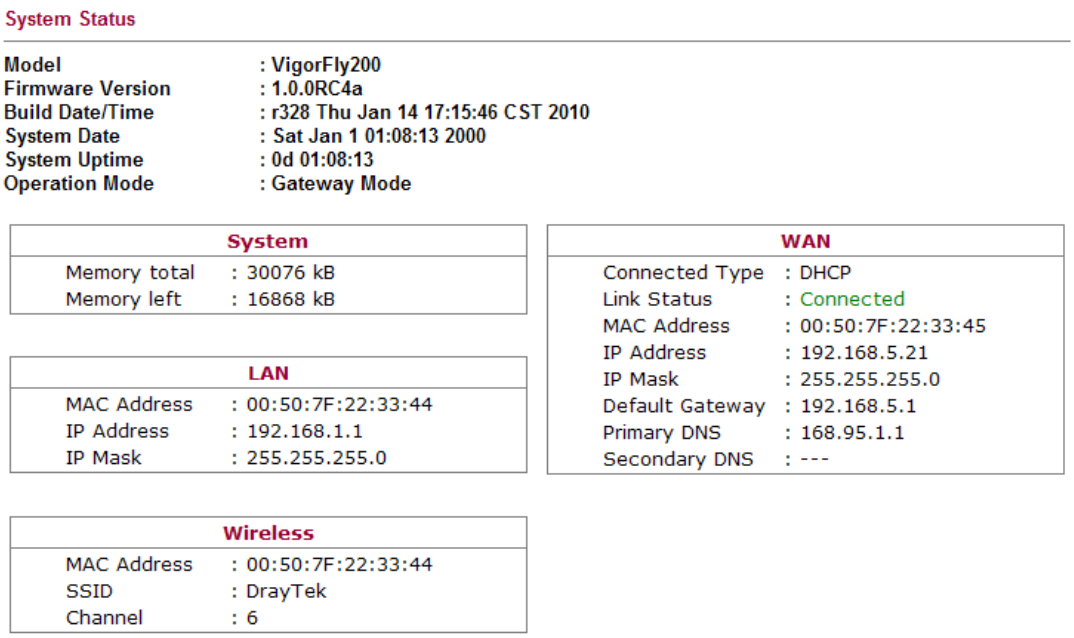
For the system setup, there are several items that you have to know the way of configuration: Status, Time and Date, and Firmware Upgrade.

Below shows the menu items for System Maintenance.



3.6.1 System Status

The **System Status** provides basic network settings of Vigor router. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.

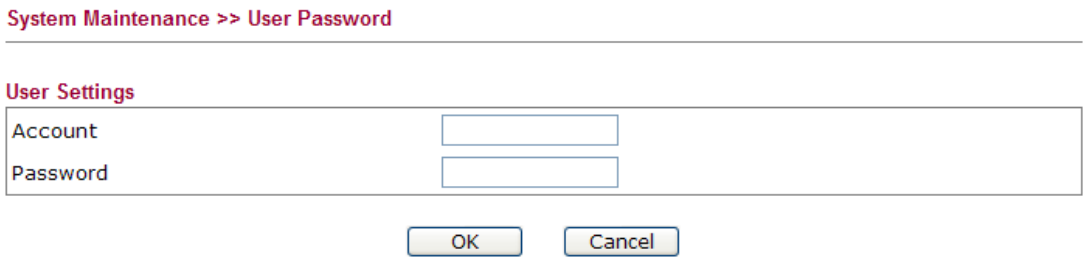


Model	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
System Date	Display current time and date for the system server.
System Uptime	Display the connection time for the system server.
Operation Mode	Display the connection mode for the router.
Memory total	Display the total dynamic RAM size for the whole system.
Memory left	Display the remaining RAM size for the whole system.
MAC Address	Display the MAC address of the LAN or WAN or WLAN Interface.
IP Address	Display the MAC address of the LAN or WAN Interface.
IP Mask	Display the subnet mask address of the LAN or WAN

	interface.
Device Type	Display the device type used for wireless LAN.
SSID	Display the SSID of this router.
Channel	Display the channel that wireless LAN used.
Connected Type	Display the network connection type for this router.
Link Status	Display if current network is connected or not.
Default Gateway	Display the gateway address of the WAN interface.
Primary DNS	Display the specified primary DNS setting.
Secondary DNS	Display the specified secondary DNS setting.

3.6.2 User Password

This page allows you to set new password for user operation.

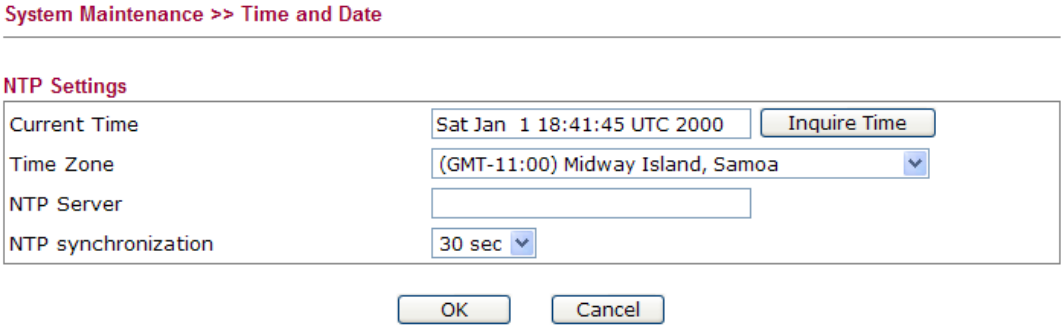


Account	Type in the name for login.
Password	Type in new password in this filed.

When you click **OK**, the login window will appear. Please use the new password to access into the web configurator for user operation again.

3.6.3 Time and Date

It allows you to specify where the time of the router should be inquired from.



Current Time	Click **Inquire Time** to get the current time.
Time Zone	Select the time zone where the router is located.
NTP Server	Type a new NTP server.
NTP synchronization	Select a time interval for updating from the NTP server.

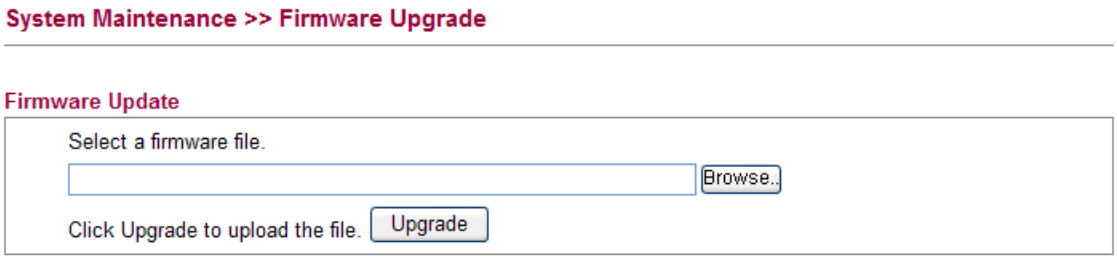
Click **OK** to save these settings.

3.6.4 Firmware Upgrade

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.draytek.com (or local DrayTek's web site) and FTP site is ftp.draytek.com.

Click **System Maintenance>> Firmware Upgrade** to launch the Firmware Upgrade Utility.

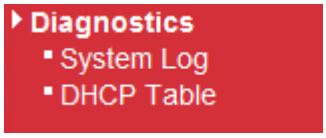


Click **Browse..** to locate the newest firmware and click **Upgrade**. During the process of upgrade, do not turn off your router.

3.7 Diagnostics

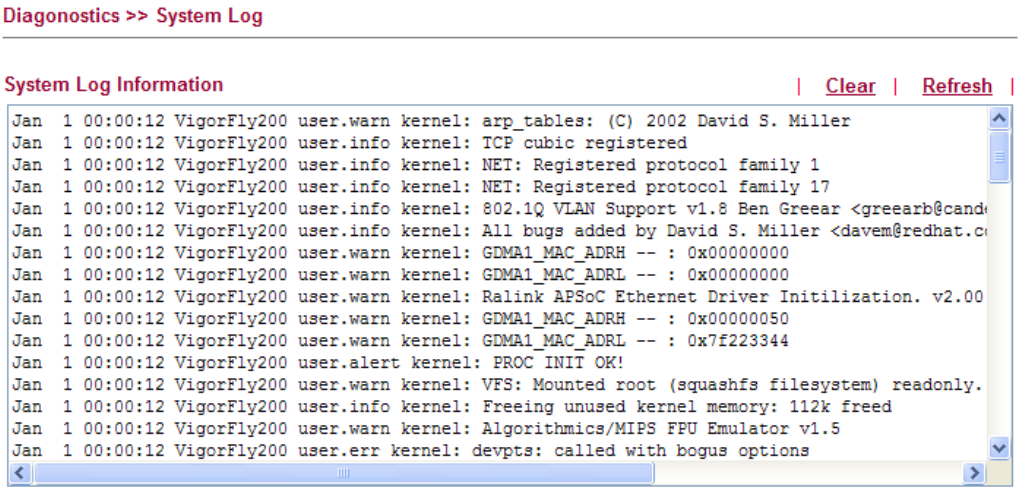
Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router.

Below shows the menu items for Diagnostics.



3.7.1 System Log

Click **Diagnostics** and click **System Log** to open the web page.

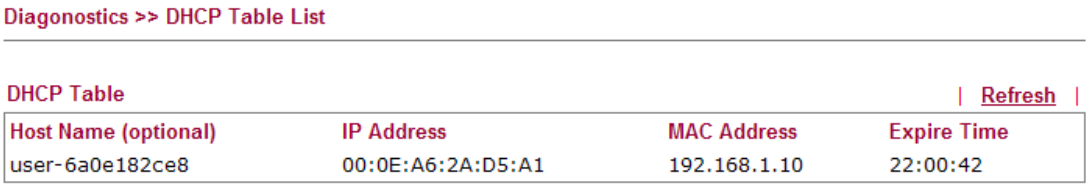


Clear	Click it to clear this page.
Refresh	Click it to reload the page.

3.7.2 DHCP Table

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **DHCP Table** to open the web page.

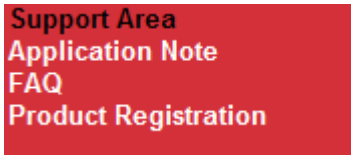


Host name	Display the name of the computer accepted the assigned IP address by this router.
IP Address	Display the IP address assigned by this router for specified PC.
MAC Address	Display the MAC address for the specified PC that DHCP assigned IP address for it.
Expire Time	Display the leased time of the specified PC.

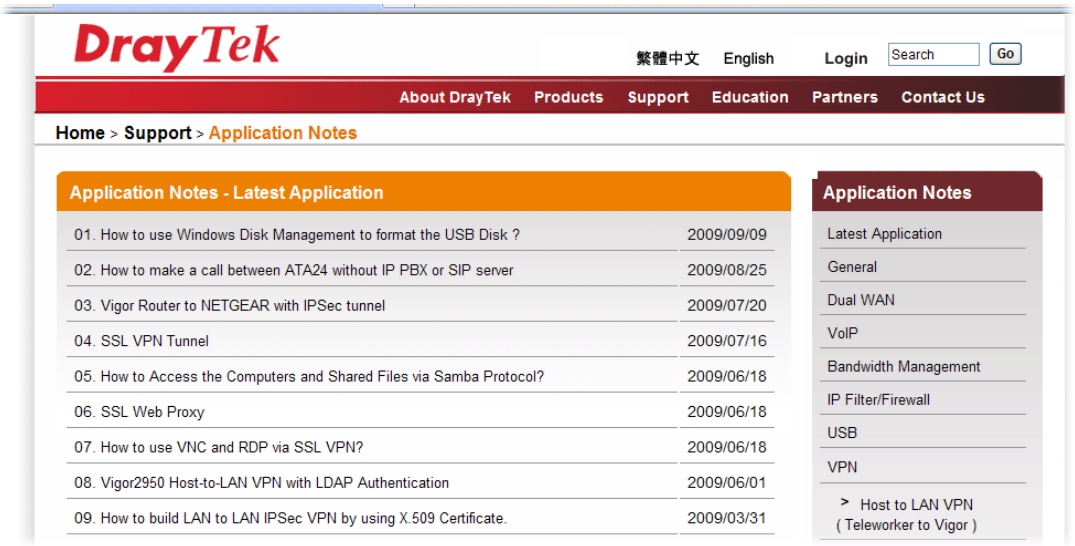
Refresh	Click it to reload the page.

3.8 Support Area

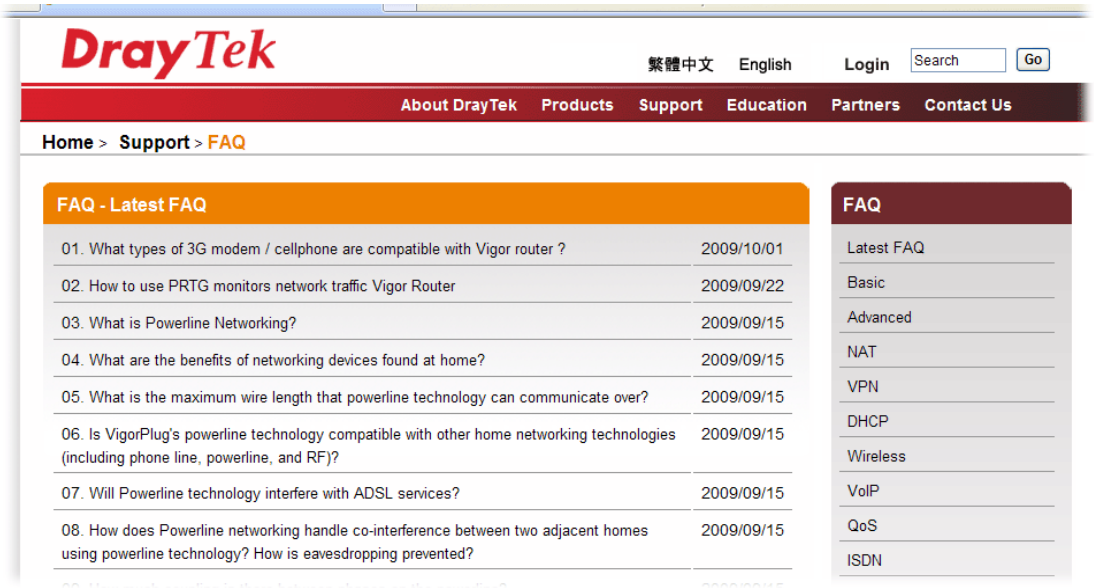
When you click the menu item under **Support Area**, you will be guided to visit www.draytek.com and open the corresponding pages directly.



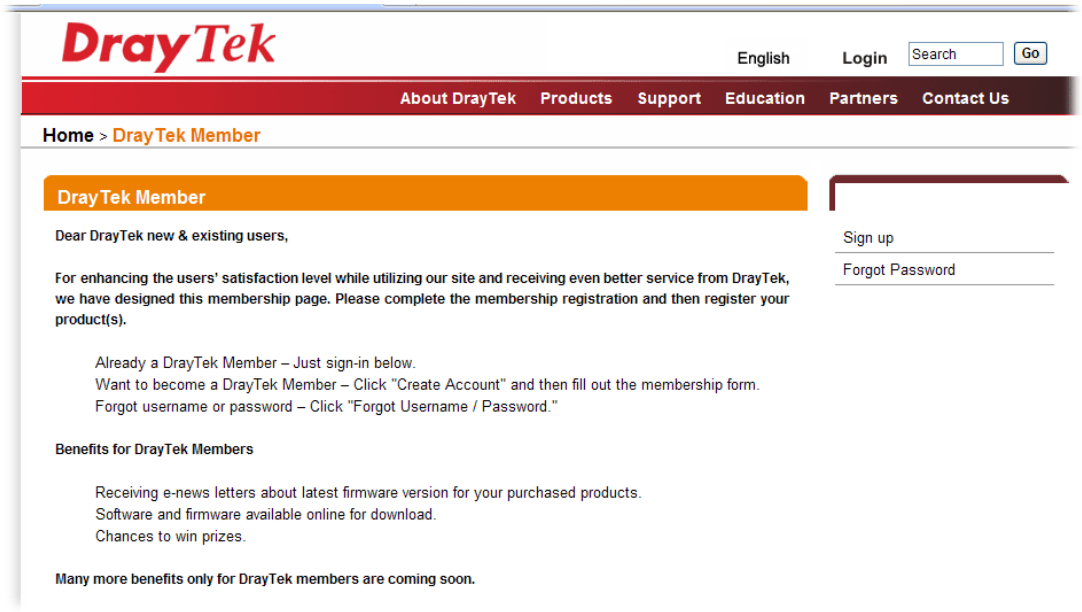
Click **Support Area>>Application Note**, the following web page will be displayed.



Click **Support Area>>FAQ**, the following web page will be displayed.



Click **Support Area>>Product Registration**, the following web page will be displayed.

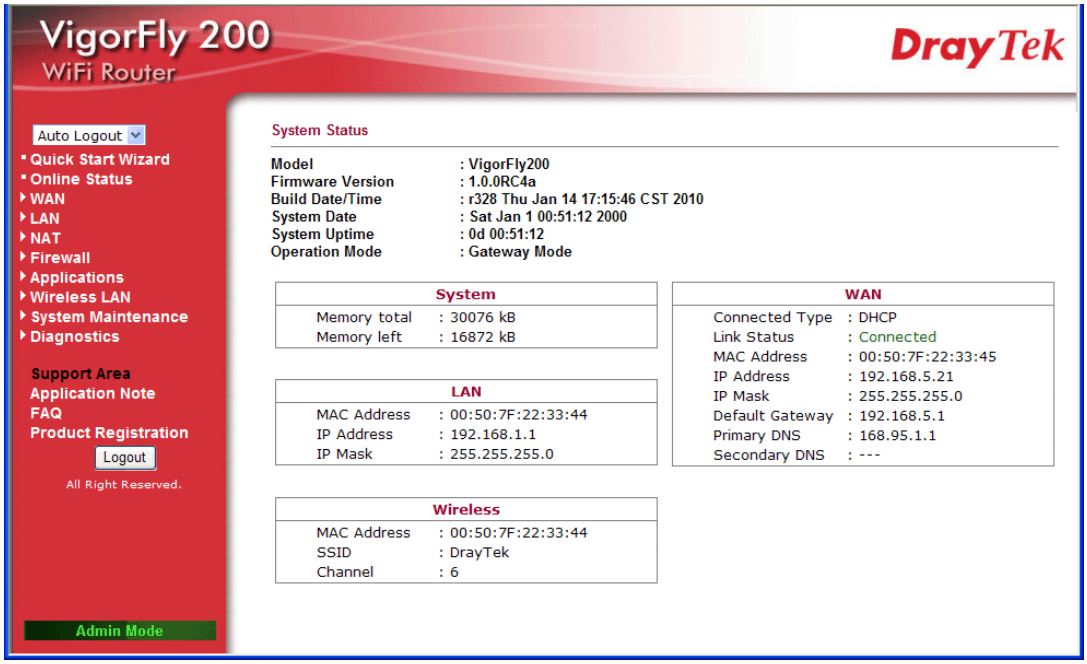


4 Admin Mode Operation

This chapter will guide users to execute advanced (full) configuration through admin mode operation.

1. Open a web browser on your PC and type **http://192.168.1.1.** The window will ask for typing username and password.
2. Please type "**admin/admin**" on Username/Password for administration operation.

Now, the **Main Screen** will appear. Be aware that "Admin mode" will be displayed on the bottom left side.



4.1 WAN

Quick Start Wizard offers user an easy method to quick setup the connection mode for the router. Moreover, if you want to adjust more settings for different WAN modes, please go to **Internet Access** group.

Basics of Internet Protocol (IP) Network

IP means Internet Protocol. Every device in an IP-based Network including routers, print server, and host PCs, needs an IP address to identify its location on the network. To avoid address conflicts, IP addresses are publicly registered with the Network Information Centre (NIC). Having a unique IP address is mandatory for those devices participated in the public network but not in the private TCP/IP local area networks (LANs), such as host PCs under the management of a router since they do not need to be accessed by the public. Hence, the NIC has reserved certain addresses that will never be registered publicly. These are known as ***private*** IP addresses, and are listed in the following ranges:

From 10.0.0.0 to 10.255.255.255
From 172.16.0.0 to 172.31.255.255
From 192.168.0.0 to 192.168.255.255

What are Public IP Address and Private IP Address

As the router plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor router. The router itself will also use the default **private IP** address: 192.168.1.1 to communicate with the local hosts. Meanwhile, Vigor router will communicate with other network devices through a **public IP** address. When the data flow passing through, the Network Address Translation (NAT) function of the router will dedicate to translate public/private addresses, and the packets will be delivered to the correct host PC in the local area network. Thus, all the host PCs can share a common Internet connection.

Get Your Public IP Address from ISP

In ADSL deployment, the PPP (Point to Point)-style authentication and authorization is required for bridging customer premises equipment (CPE). Point to Point Protocol over Ethernet (PPPoE) connects a network of hosts via an access device to a remote access concentrator or aggregation concentrator. This implementation provides users with significant ease of use. Meanwhile it provides access control, billing, and type of service according to user requirement.

When a router begins to connect to your ISP, a serial of discovery process will occur to ask for a connection. Then a session will be created. Your user ID and password is authenticated via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information will usually be assigned by your ISP.

Network Connection by 3G USB Modem

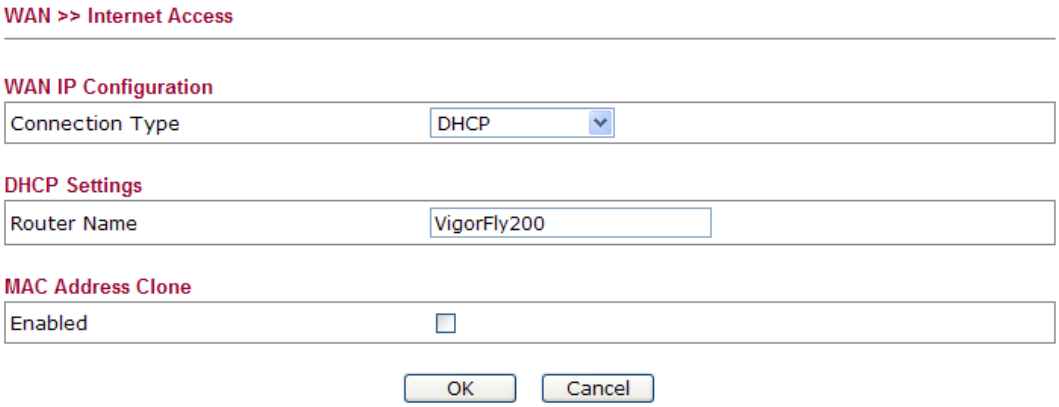
For 3G mobile communication through Access Point is popular more and more, Vigor router adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor router, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor router with 3G USB Modem allows you to receive 3G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use four LAN ports on the router to access Internet. Also, they can access Internet via wireless function of Vigor router, and enjoy the powerful firewall, bandwidth management features of Vigor router.

3G USB Modem can be used as backup device. Therefore, when WAN is not available, the router will use 3G USB Modem for supporting automatically. The supported 3G USB Modem will be listed on DrayTek web site. Please visit www.draytek.com for more detailed information.

Below shows the menu items for **WAN**.

4.1.1 Internet Access

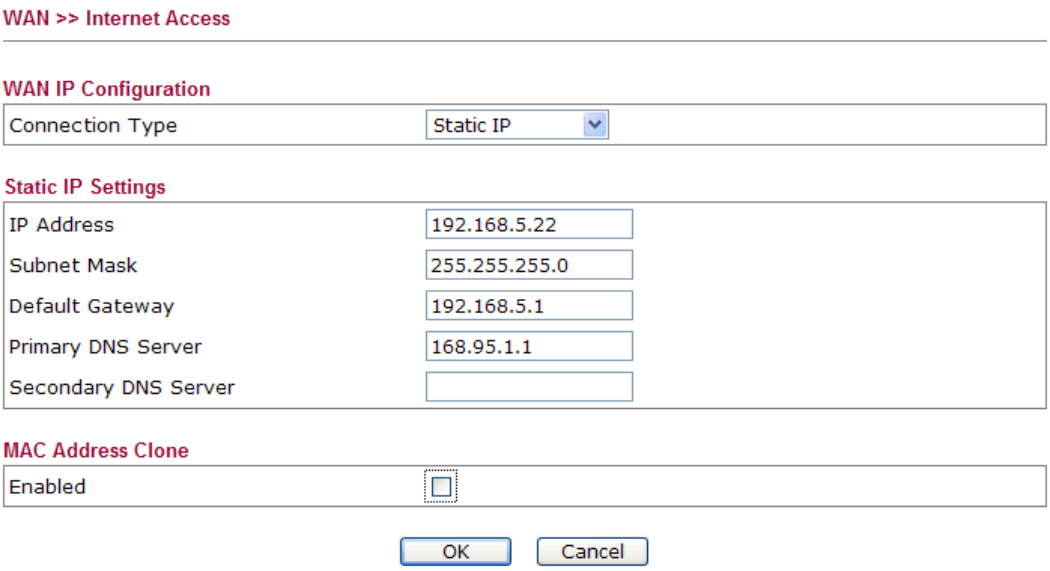
This page allows you to set WAN configuration with different modes. Use the Connection Type drop down list to choose one of the WAN modes. The corresponding page will be displayed.



Static IP

For static IP mode, you usually receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your DSL or Cable ISP service providers. In most cases, a Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you have a public subnet, you could assign an IP address or many IP address to the WAN interface.

To use **Static IP** as the accessing protocol of the internet, please choose **Static** mode from **Connection Type** drop down menu. The following web page will be shown.



IP Address	Type the IP address.
Subnet Mask	Type the subnet mask.
Default Gateway	Type the gateway IP address.
Primary DNS Server	You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will

automatically apply default DNS Server IP address: 198.95.1.1 to this field.

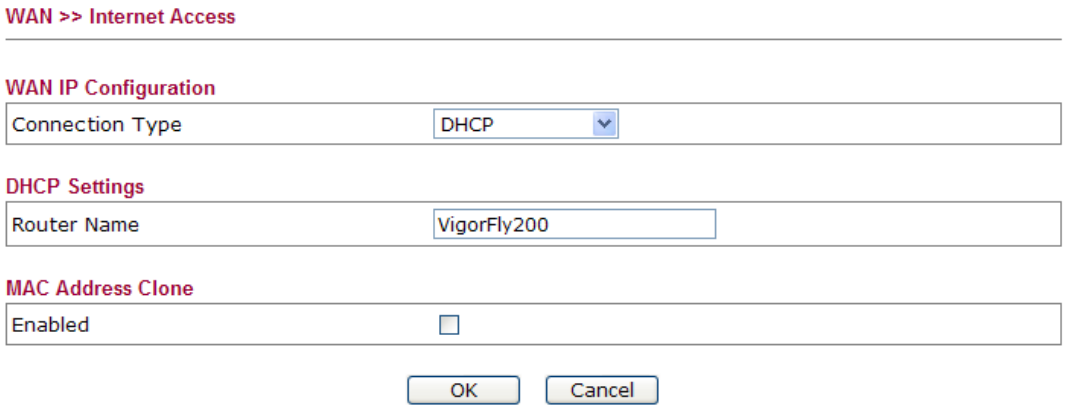
Secondary DNS Server — You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address.

MAC Address Clone — **MAC Address Clone** is available when the box of **Enable** is checked. The router will detect the MAC address automatically. The result will be displayed in the field of MAC Address.

After finishing all the settings here, please click **OK** to activate them.

DHCP

DHCP allows a user to obtain an IP address automatically from a DHCP server on the Internet. If you choose **DHCP** mode, the DHCP server of your ISP will assign a dynamic IP address for your router automatically. It is not necessary for you to assign any setting,



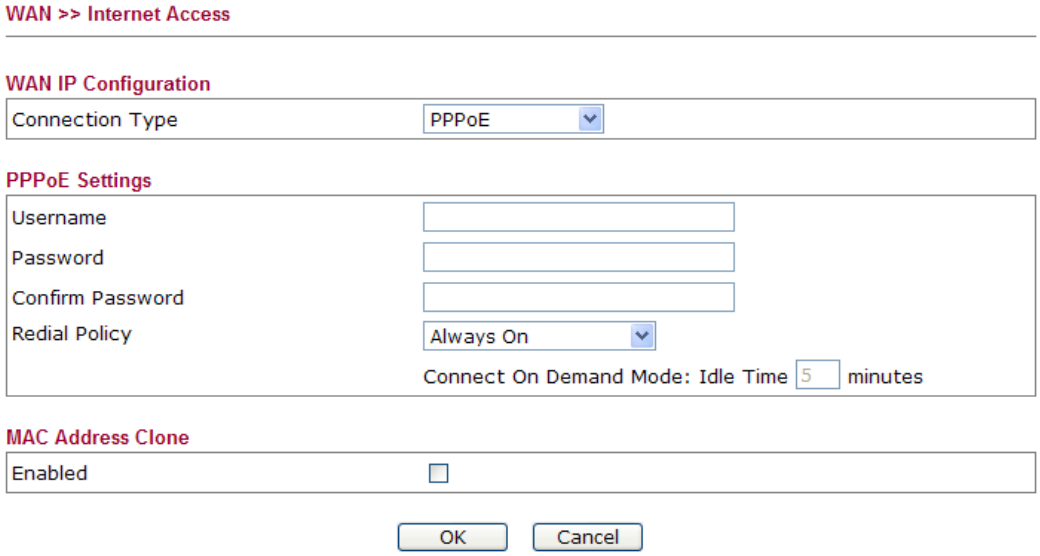
Router Name — Type in a name for the router. It must be the same as the name used in Syslog.

MAC Address Clone — **MAC Address Clone** is available when the box of **Enable** is checked. The router will detect the MAC address automatically. The result will be displayed in the field of MAC Address.

After finishing all the settings here, please click **OK** to activate them.

PPPoE

To choose PPPoE as the accessing protocol of the internet, please select **PPPoE** from the **Internet Access** menu. The following web page will be shown.

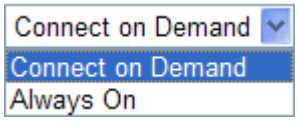


Username Type in the username provided by ISP in this field.

Password Type in the password provided by ISP in this field.

Confirm Password Re-enter the password for confirmation.

Redial Policy If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, choose **Connect on Demand**.



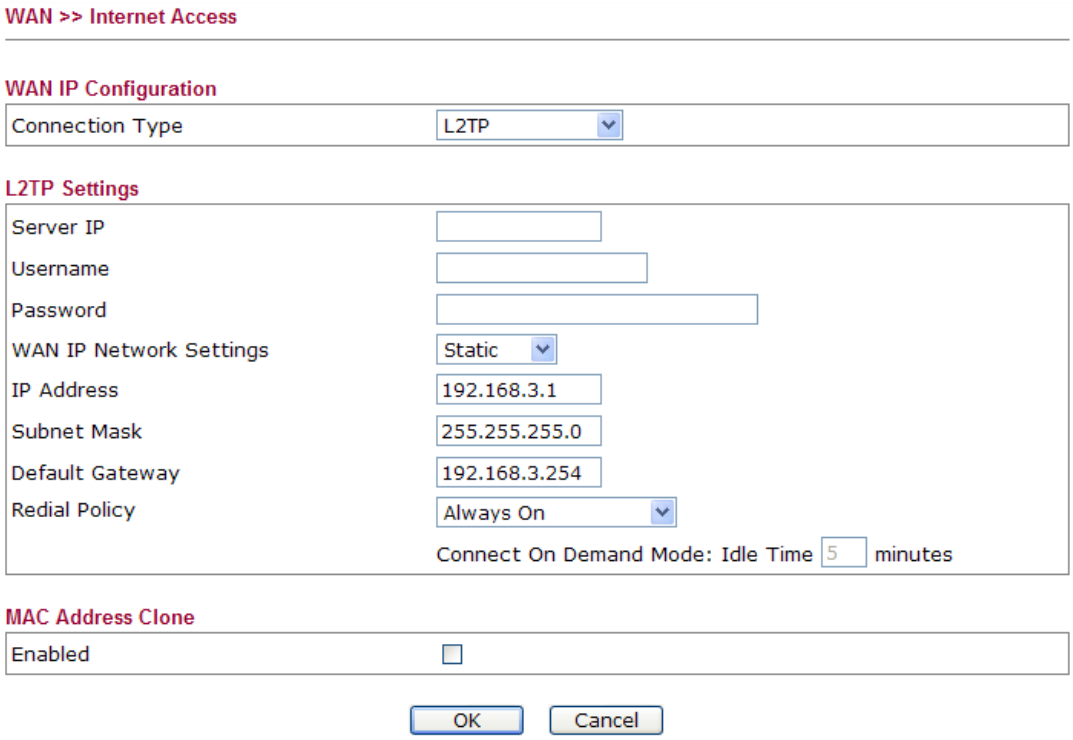
Idle Time - Set the timeout for breaking down the Internet after passing through the time without any action. When you choose **Connect on Demand,** you have to type value here.

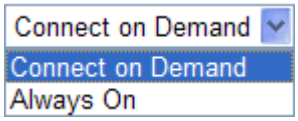
MAC Address Clone **MAC Address Clone** is available when the box of **Enable** is checked. The router will detect the MAC address automatically. The result will be displayed in the field of MAC Address.

After finishing all the settings here, please click **OK** to activate them.

PPTP/L2TP

To use **PPTP/L2TP** as the accessing protocol of the internet, please choose **PPTP/L2TP** from **Connection Type** drop down menu. The following web page will be shown.

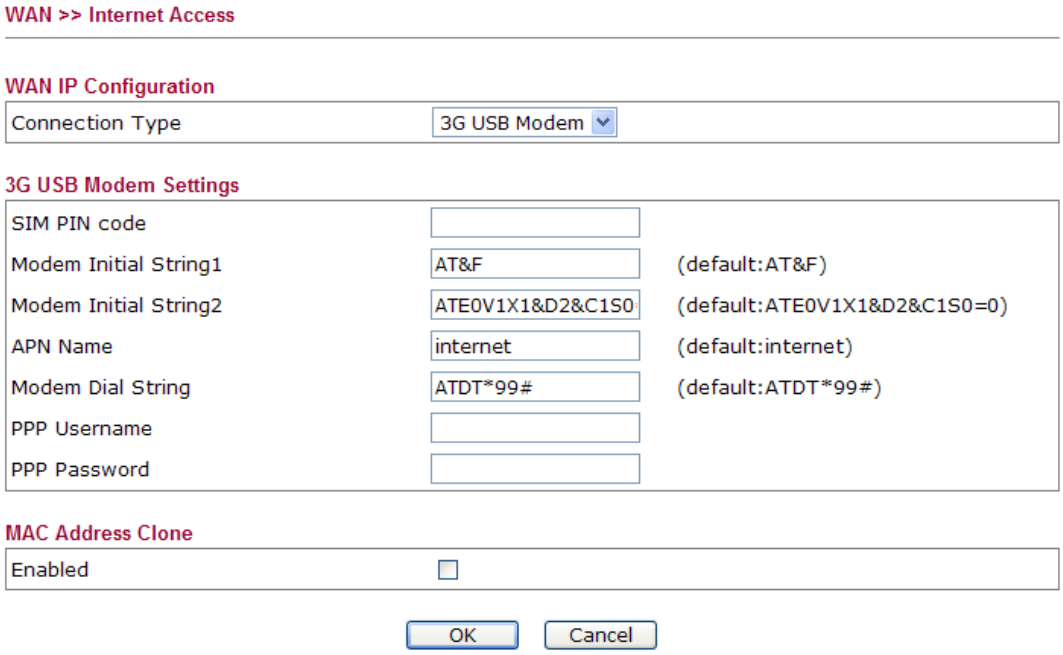


Server IP	Type in the IP address of the PPTP/L2TP server.
User Name	Type in the username provided by ISP in this field.
Password	Type in the password provided by ISP in this field.
Address Mode	You can choose **Static IP** or **DHCP** as WAN IP network setting.
IP Address	Type the IP address if you choose Static IP as the WAN IP network setting.
Subnet Mask	Type the subnet mask if you chose Static IP as the WAN IP.
Default Gateway	Type the gateway address for this router.
Redial Policy	If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, choose **Connect on Demand**.  **Idle Time -** Set the timeout for breaking down the Internet after passing through the time without any action. When you choose **Connect on Demand,** you have to type value here.
MAC Address Clone	**MAC Address Clone** is available when the box of **Enable** is checked. The router will detect the MAC address automatically. The result will be displayed in the field of MAC Address.

After finishing all the settings here, please click **OK** to activate them.

3G USB Modem

If your router connects to a 3G modem and you want to access Internet via 3G modem, choose 3G as connection type and type the required information in this web page.



SIM PIN code — Type PIN code of the SIM card that will be used to access Internet.

Modem Initial String1/2 — Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.

APN Name — APN means Access Point Name which is provided and required by some ISPs.

Modem Dial String — Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.

PPP Username — Type the PPP username (optional).

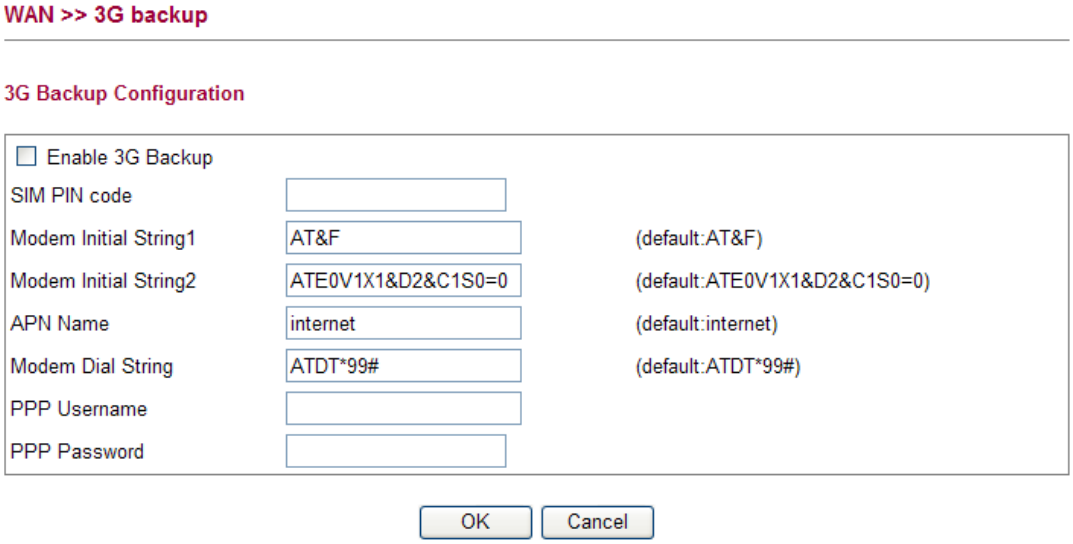
PPP Password — Type the PPP password (optional).

MAC Address Clone — **MAC Address Clone** is available when the box of **Enable** is checked. The router will detect the MAC address automatically. The result will be displayed in the field of MAC Address.

After finishing all the settings here, please click **OK** to activate them.

4.1.2 3G Backup

This page is used to setup 3G backup function. If you enable 3G backup, make sure your WAN connection type is not in 3G mode. When the WAN connection is broken, router will try to keep the connection with 3G mode. After WAN connection is recovered, router will disconnect the 3G connection automatically.



Enable 3G Backup — Check this box to enable the 3G backup feature.

SIM PIN code — Type PIN code of the SIM card that will be used to access Internet.

Modem Initial String1/2 — Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.

APN Name — APN means Access Point Name which is provided and required by some ISPs.

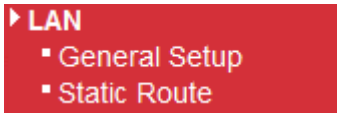
Modem Dial String — Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.

PPP Username — Type the PPP username (optional).

PPP Password — Type the PPP password (optional).

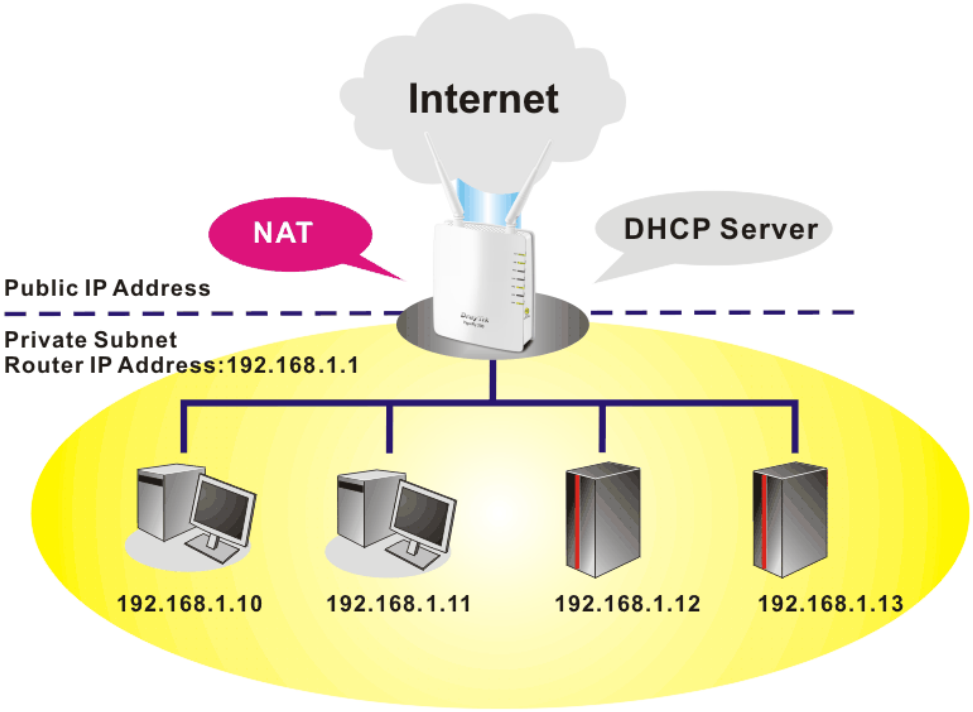
4.2 LAN

Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

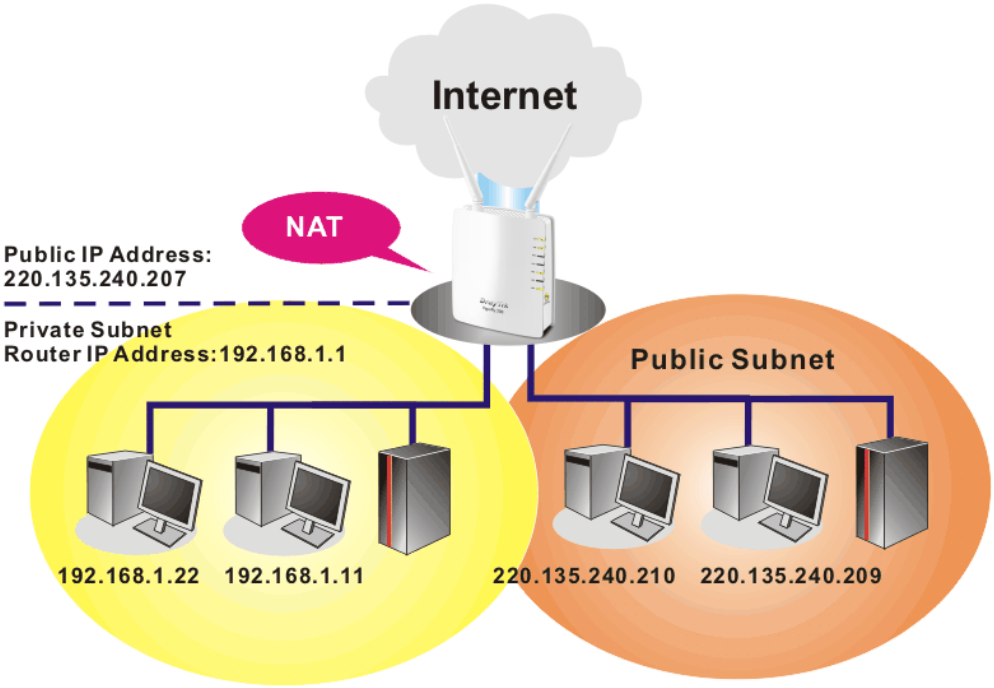


Basics of LAN

The most generic function of Vigor router is NAT. It creates a private subnet of your own. As mentioned previously, the router will talk to other public hosts on the Internet by using public IP address and talking to local hosts by using its private IP address. What NAT does is to translate the packets from public IP address to private IP address to forward the right packets to the right host and vice versa. Besides, Vigor router has a built-in DHCP server that assigns private IP address to each local host. See the following diagram for a briefly understanding.



In some special case, you may have a public IP subnet from your ISP such as 220.135.240.0/24. This means that you can set up a public subnet or call second subnet that each host is equipped with a public IP address. As a part of the public subnet, the Vigor router will serve for IP routing to help hosts in the public subnet to communicate with other public hosts or servers outside. Therefore, the router should be set as the gateway for public hosts.



What is Routing Information Protocol (RIP)

Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

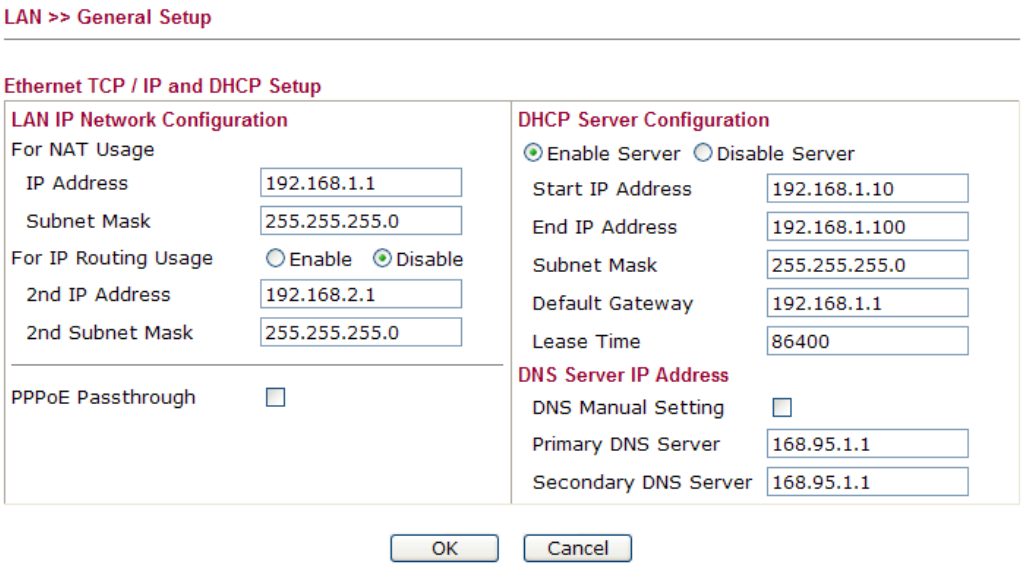
What is Static Route

When you have several subnets in your LAN, sometimes a more effective and quicker way for connection is the **Static routes** function rather than other method. You may simply set rules to forward data from one specified subnet to another specified subnet without the presence of RIP.

4.2.1 General Setup

This page provides you the general settings for LAN.

Click **LAN** to open the LAN settings page and choose **General Setup**.



IP Address	Type in private IP address for connecting to a local private network (Default: 192.168.1.1).
Subnet Mask	Type in an address code that determines the size of the network. (Default: 255.255.255.0)
For IP Routing Usage	Click **Enable** to invoke this function. The default setting is **Disable**.
2nd IP Address	Type in secondary IP address for connecting to a subnet. (Default: 192.168.2.1)
2nd Subnet Mask	An address code that determines the size of the network.
PPPoE Passthrough	If you want to use PPPoE server in the network via Vigor router, please check this box to redirect the PPPoE frames to the specified location.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network. If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
Enable Server	Let the router assign IP address to every host in the LAN.
Disable Server	Let you manually assign IP address to every host in the LAN.
Start IP Address	Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.
End IP Address	Enter a value of the IP address pool for the DHCP server to end with when issuing IP addresses.
Subnet Mask	Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
Default Gateway	Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.
Lease Time	It allows you to set the leased time for the specified PC.
DNS Manual Setting	If this function is enabled, LAN PCs use Primary DNS Server and Secondary DNS Server as their DNS servers. Otherwise, LAN PCs use the router as their DNS server and the router will do DNS proxy for them.
Primary DNS Address	You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
Secondary DNS Address	You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS

Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.

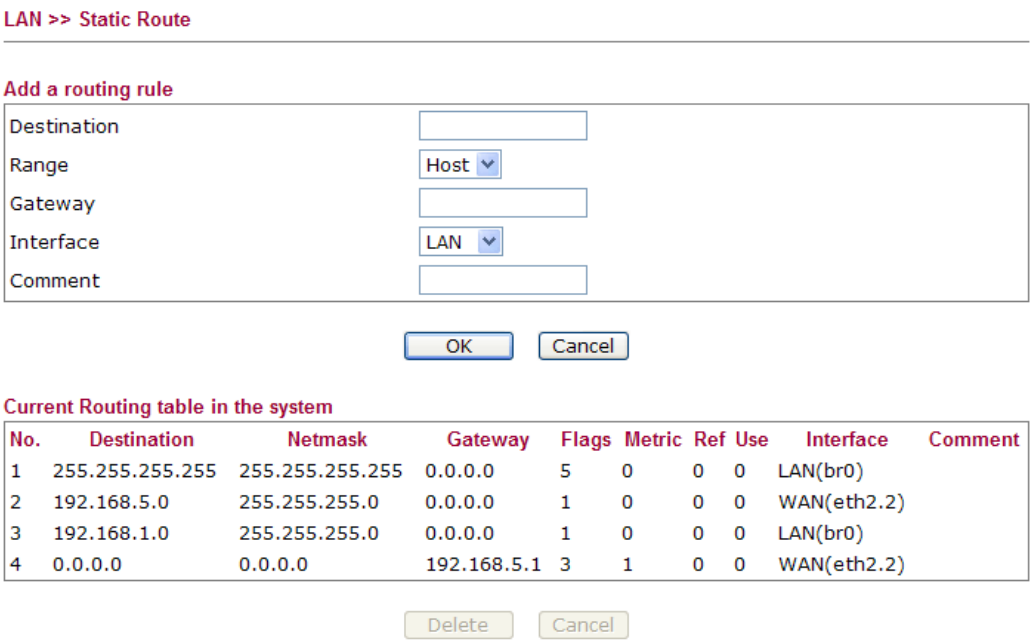
If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.

If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.

After finishing all the settings here, please click **OK** to activate them.

4.2.2 Static Route

Go to **LAN** to open setting page and choose **Static Route**. It can help to describe one way of configuring path selection of router in computer network.



Destination	Type the IP address for the routing rule applied to.
Range	Choose **Host** or **Net** for specifying gateway or netmask setting of such routing rule.
Netmask	Type the netmask for such routing rule if you choose **Net** as **Range** setting.
Gateway	Type the gateway address for such routing rule.
Interface	Choose **WAN** or **LAN** as the interface for such route.
Comment	Type words as notification for such routing.
OK	Click this button to save current configuration and display on the routing table below.
Cancel	Click this button to clear current configuration.

4.3 NAT

Usually, the router serves as an NAT (Network Address Translation) router. NAT is a mechanism that one or more private IP addresses can be mapped into a single public one. Public IP address is usually assigned by your ISP, for which you may get charged. Private IP addresses are recognized only among internal hosts.

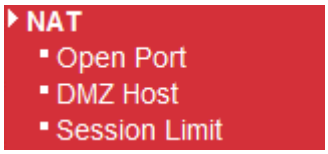
When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize this address/port-mapping relationship. When the public server response, the incoming traffic, of course, is destined to the router's public IP address and the router will do the inversion based on its table. Therefore, the internal host can communicate with external host smoothly.

The benefit of the NAT includes:

- **Save cost on applying public IP address and apply efficient usage of IP address.** NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- **Enhance security of the internal network by obscuring the IP address.** There are many attacks aiming victims based on the IP address. Since the attacker cannot be aware of any private IP addresses, the NAT function can protect the internal network.

On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by using port mapping methods.

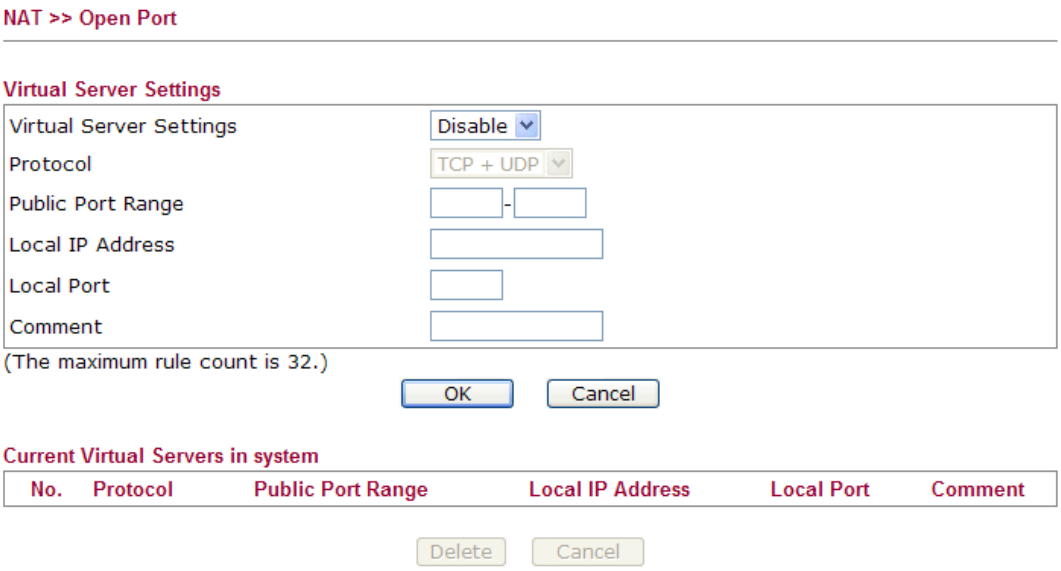
Below shows the menu items for NAT.

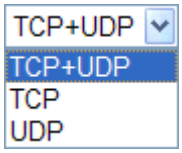


4.3.1 Open Ports

Open Ports allows you to open a range of ports for the traffic of special applications.

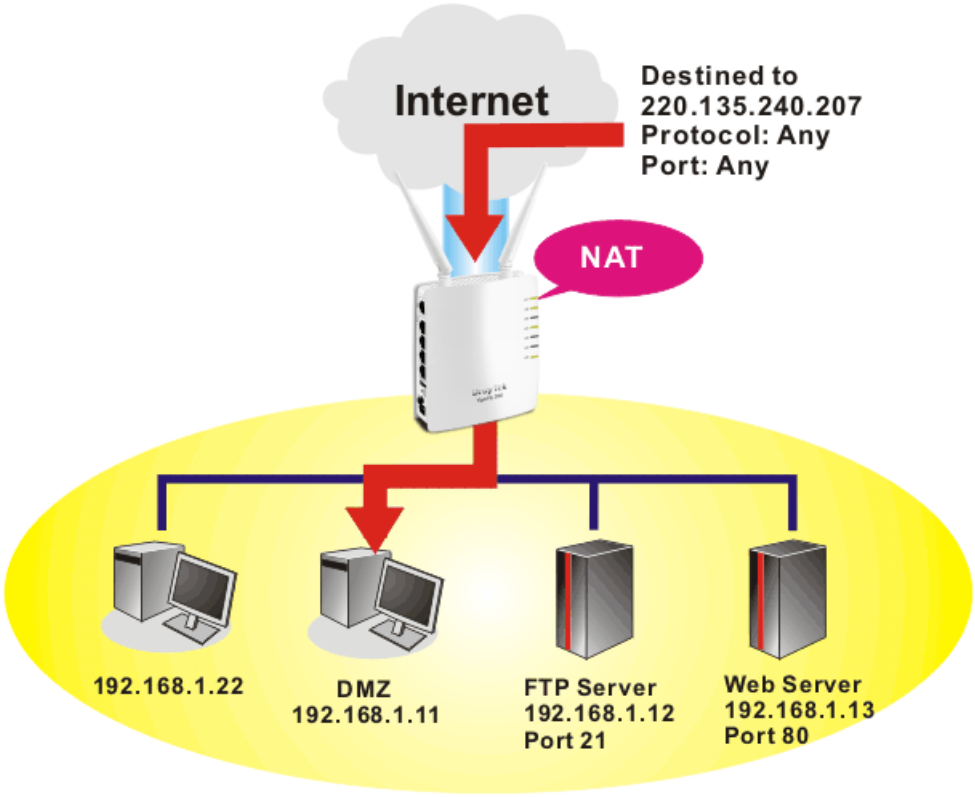
Common application of Open Ports includes P2P application (e.g., BT, KaZaA, Gnutella, WinMX, eMule and others), Internet Camera etc. Ensure that you keep the application involved up-to-date to avoid falling victim to any security exploits.



Virtual Server Settings	Choose **Enable** to invoke this setting.
Protocol	Specify the transport layer protocol. It could be **TCP**, **UDP** and **TCP+UDP**. 
Public Port Range	Specify the starting port number and ending port number of the service offered by the local host.
Local IP Address	Enter the private IP address of the local host.
Local Port	If it is configured, the forwarded traffic is mapped to this port on the local host.
Comment	Type words as notification for such virtual server.
OK	When you finish the above settings, simply click this button to save it and display on the field of **Current Virtual Servers in system**.
Cancel	Click this button to clear current configuration.
Delete	Click this button to remove the selected virtual server configuration.

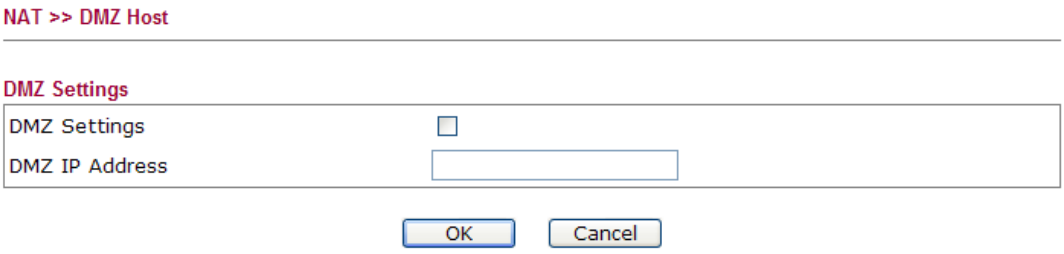
4.3.2 DMZ Host

As mentioned above, **Port Redirection** can redirect incoming TCP/UDP or other traffic on particular ports to the specific private IP address/port of host in the LAN. However, other IP protocols, for example Protocols 50 (ESP) and 51 (AH), do not travel on a fixed port. Vigor router provides a facility **DMZ Host** that maps ALL unsolicited data on any protocol to a single host in the LAN. Regular web surfing and other such Internet activities from other clients will continue to work without inappropriate interruption. **DMZ Host** allows a defined internal user to be totally exposed to the Internet, which usually helps some special applications such as Netmeeting or Internet Games etc.



Note: The security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

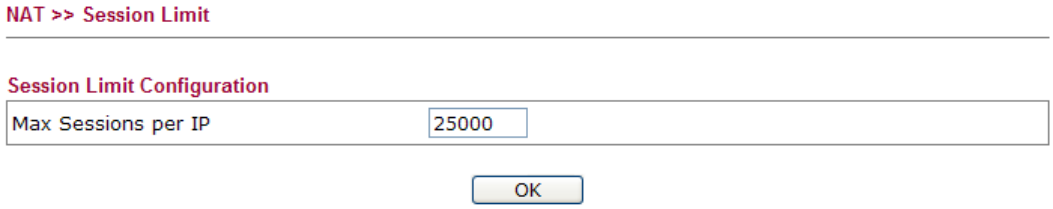
Click **DMZ Host** to open the following page:



DMZ Settings	Check this box to enable the DMZ Host function.
DMZ IP Address	Enter the private IP address of the DMZ host.
OK	Click this button to save such profile.
Cancel	Click this button to clear information on this page.

4.3.3 Session Limit

A PC with private IP address can access to the Internet via NAT router. The router will generate the records of NAT sessions for such connection. The P2P (Peer to Peer) applications (e.g., BitTorrent) always need many sessions for procession and also they will occupy over resources which might result in important accesses impacted. To solve the problem, you can use limit session to limit the session procession for specified Hosts.



Please define the available session number for the router. If you do not set the session number in this field, the system will use the default session limit (25000) for the specific limitation.

4.4 Firewall

Basics for Firewall

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of the Vigor router helps to protect your local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet. Furthermore, it can filter out specific packets that trigger the router to build an unwanted outgoing connection.

Denial of Service (DoS) Defense

The **DoS Defense** functionality helps you to detect and mitigate the DoS attack. The attacks are usually categorized into two types, the flooding-type attacks and the vulnerability attacks. The flooding-type attacks will attempt to exhaust all your system's resource while the vulnerability attacks will try to paralyze the system by offending the vulnerabilities of the protocol or operation system.

The **DoS Defense** function enables the Vigor router to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog server.

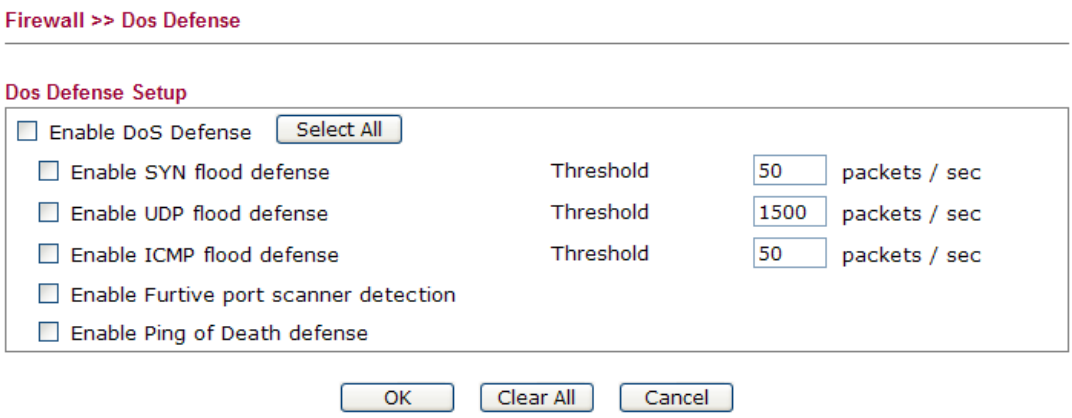
Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

Below shows the menu items for Firewall.

4.4.1 DoS Defense

As a sub-functionality of IP Filter/Firewall, there are 5 types of detect/ defense function in the **DoS Defense** setup. The DoS Defense functionality is disabled for default.

Click **Firewall** and click **DoS Defense** to open the setup page.

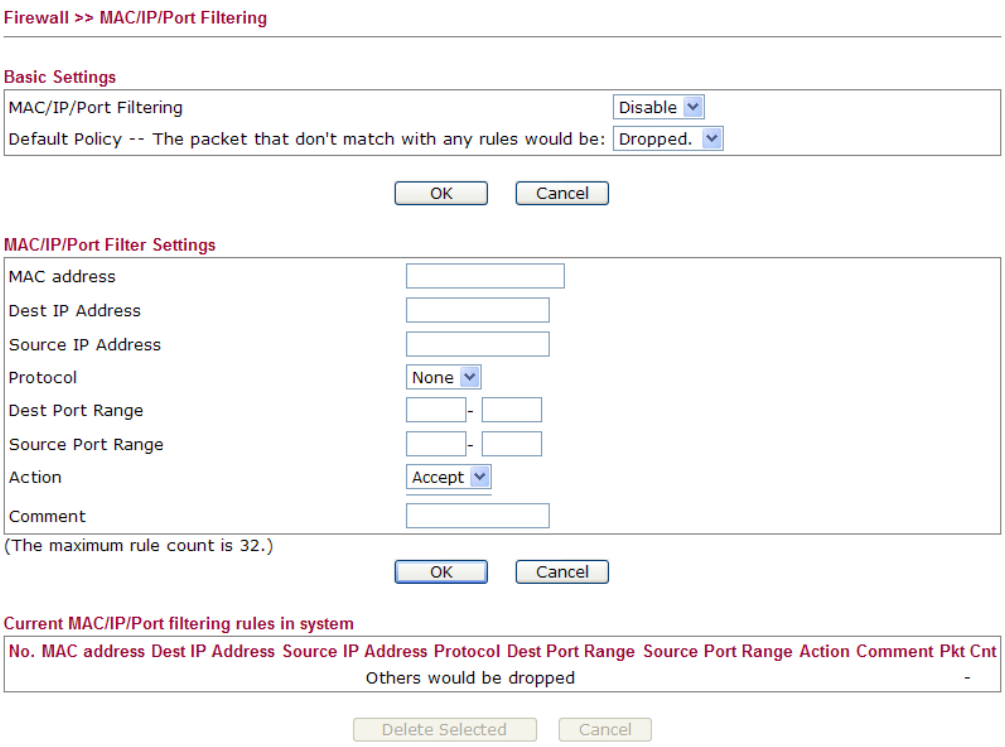


Enable Dos Defense	Check the box to activate the DoS Defense Functionality.
Enable SYN flood defense	Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router. By default, the threshold and timeout values are set to 50 packets per second and 10 seconds, respectively.
Enable UDP flood defense	Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout. The default setting for threshold and timeout are 150 packets per second and 10 seconds, respectively.
Enable ICMP flood defense	Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet. The default setting for threshold and timeout are 50 packets per second and 10 seconds, respectively.
Enable Furtive port scanner detection	Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior, the Vigor router will send out a warning.
Enable Ping of Death Defense	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers

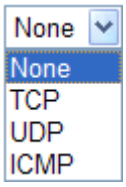
	will block any packets realizing this attacking activity.
OK	Click this button to save such profile.
Clear All	Click this button to clear all of the settings in this page.
Cancel	Click this button to cancel current operation

4.4.2 MAC/IP/Port Filtering

This page allows you to set up to 32 MAC/IP/Port Filtering rules. When you finish the filtering rule, simply click **OK**. The new rule will be displayed below in this page.



MAC/IP/Port Filtering	Choose **Enable** to activate MAC/IP/Port Filtering function.
Default Policy	**Accepted** – all the packets that do not match with any rule will be accepted. **Dropped** – all the packets that do not match with any rule will be blocked.
MAC Address	Type the MAC address for the router.
Dest IP Address	Type the destination IP address for applying such rule.
Source IP Address	Type the source IP address for applying such rule.
Protocol	Specify the protocol(s) which this filter rule will apply to.



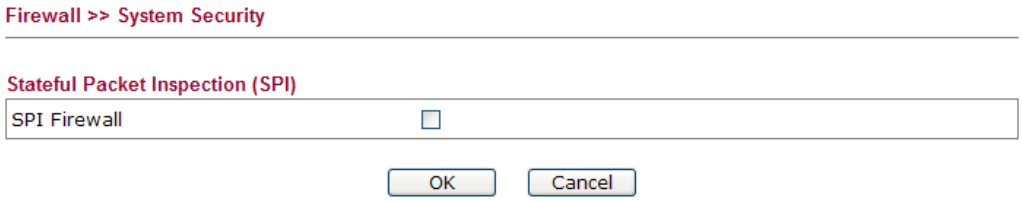
Dest Port Range	Determine the port range for the destination.

Source Port Range	Determine the port range for the source.
Action	**Accept** – the packets that match with such rule will be accepted. **Drop** – the packets that match with such rule will be blocked.
Comment	Enter filter set comments/description. Maximum length is 23–character long.
OK	Click this button to save such profile.
Cancel	Click this button to cancel current operation.

4.4.3 System Security

Stateful Packet Inspection (SPI) is a firewall architecture that works at the network layer. Unlike legacy static packet filtering, which examines a packet based on the information in its header, stateful inspection builds up a state machine to track each connection traversing all interfaces of the firewall and makes sure they are valid. The stateful firewall of Vigor router not just examine the header information also monitor the state of the connection.

The purpose of this is to enable the SPI firewall for the filtering incoming packets and outgoing packets. Simply check the box and click **OK**.



4.4.4 Content Filtering

Web Content Filter

We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary threats, such as productivity, legal liability, network and security threats. For parents, you can protect your children from viewing adult websites or chat rooms.

Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g.www.bbc.co.uk) will be checked against our server database. This database is updated as frequent as daily by a global team of Internet researchers. The server will look up the URL and return a category to your router. Your Vigor router will then decide whether to allow access to this site according to the categories you have selected. Please note that this action will not introduce any delay in your Web surfing because each of multiple load balanced database servers can handle millions of requests for categorization.

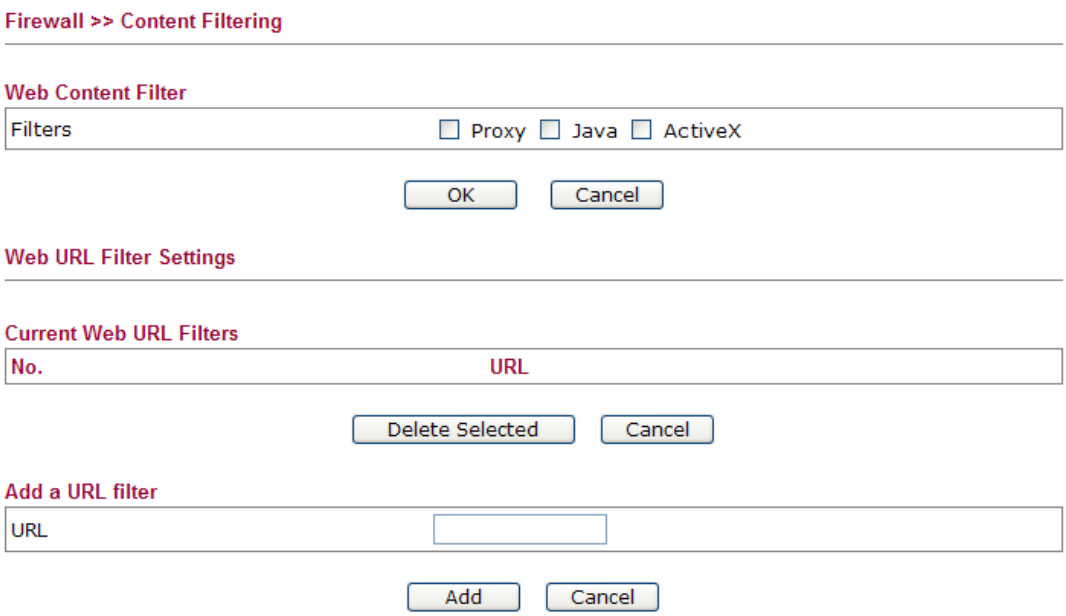
URL Content Filter

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

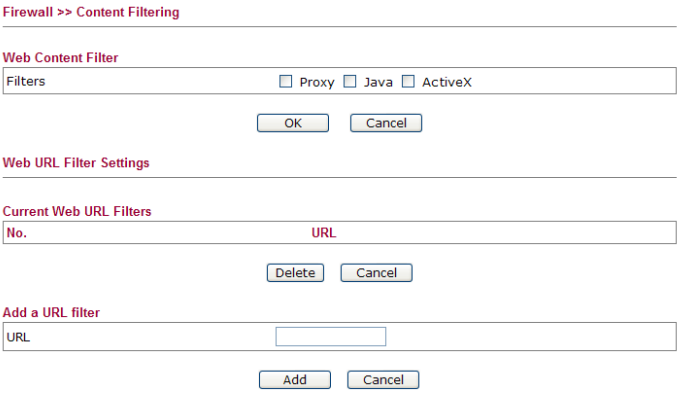
On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

Open **Firewall>>MAC/IP/Port Filtering** to access into the following page.

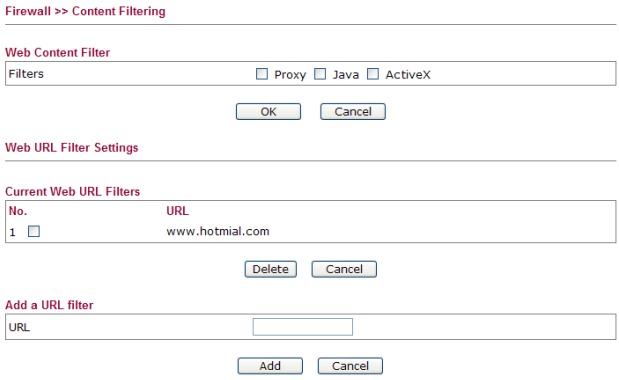


Web Content Filter — At present, there are three content filters offered here for you to choose. Check Proxy, Java or ActiveX and click **OK**. The system will filter and block the web pages according to the item you specified here.

Web URL Filter Settings — URL – type the URL of the web site in the field of URL and click **Add**. The new link with the URL you specified will be shown on this page. The system will filter and block the web pages according to the item you specified here.

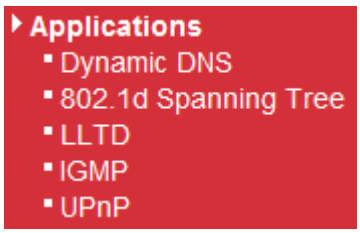


To delete the URL setting, simply click that one and click **Delete** to remove it.



4.5 Applications

Below shows the menu items for Applications.

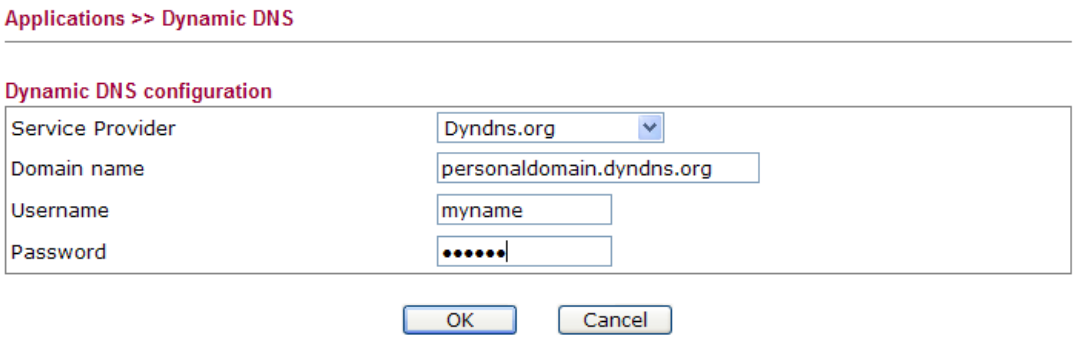


4.5.1 Dynamic DNS

The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router to update its online WAN IP address mappings on the specified Dynamic DNS server. Once the router is online, you will be able to use the registered domain name to access the router or internal virtual servers from the Internet. It is particularly helpful if you host a web server, FTP server, or other server behind the router.

Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The router provides up to three accounts from three different DDNS service providers. Basically, Vigor routers are compatible with the DDNS services supplied by most popular DDNS service providers such as **www.dyndns.org, www.no-ip.com,**

www.dtdns.com, www.changeip.com, www.dynamic- nameserver.com. You should visit their websites to register your own domain name for the router.

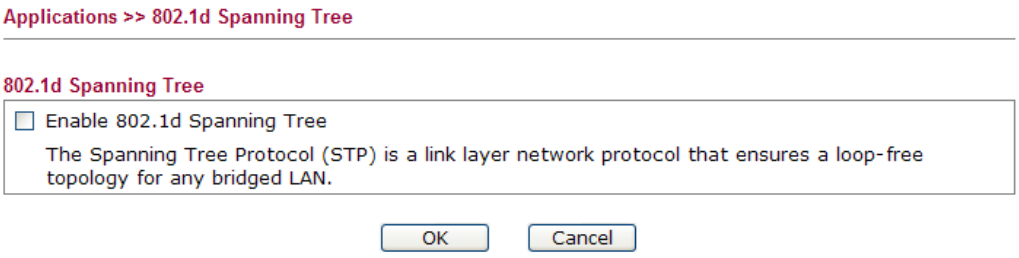


Service Provider	Select the service provider for the DDNS account. If you choose **None**, such function will be disabled.
Domain name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
Username	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.
OK	Click it to save and apply such setting.

Click **OK** button to activate the settings.

4.5.2 802.1d Spanning Tree

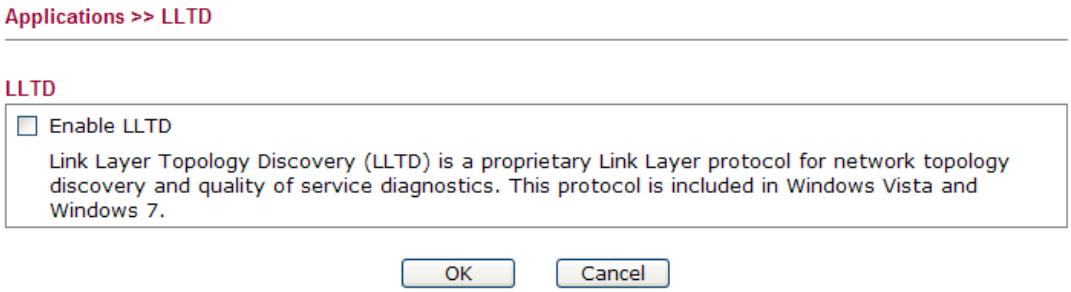
The Spanning Tree Protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN.



OK	Click it to save and apply such setting.

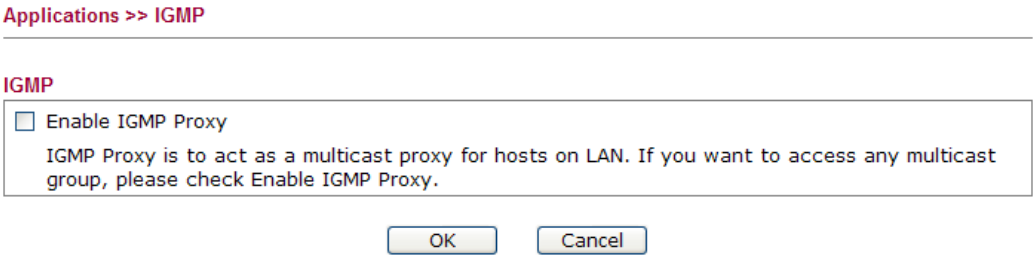
4.5.3 LLTD

Link Layer Topology Discovery (LLTD) is a proprietary Link Layer protocol for network topology discovery and quality of service diagnostics. This protocol is included in Windows Vista and Windows 7.



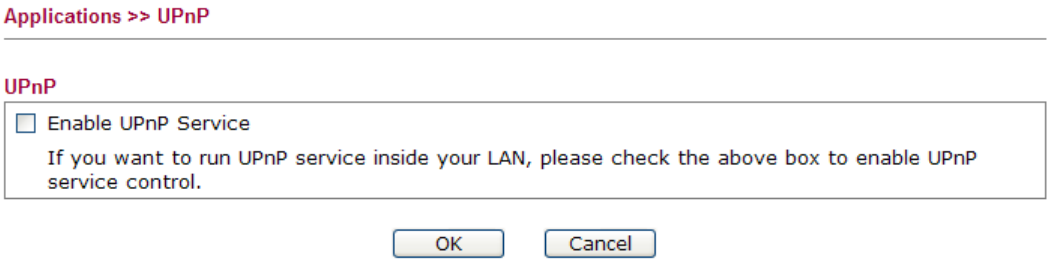
4.5.4 IGMP

IGMP is the abbreviation of *Internet Group Management Protocol*. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups.



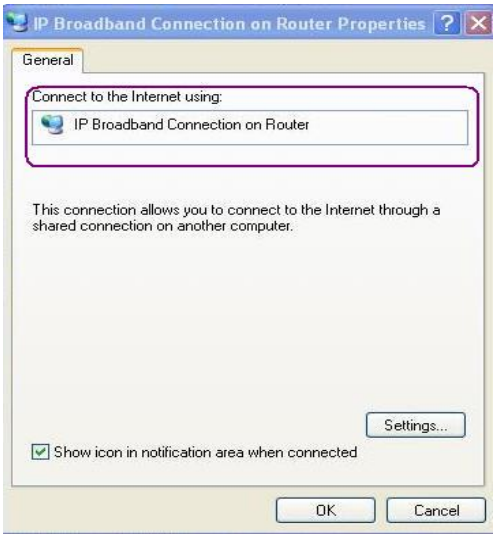
4.5.5 UPnP Configuration

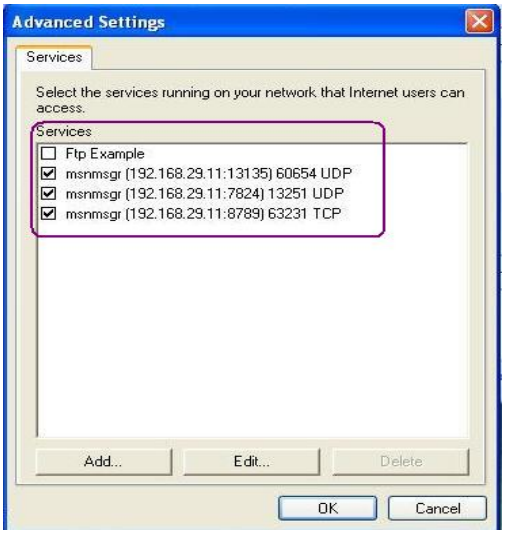
The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on the router is “NAT Traversal”. This enables applications inside the firewall to automatically open the ports that they need to pass through a router. It is more reliable than requiring a router to work out by itself which ports need to be opened. Further, the user does not have to manually set up port mappings or a DMZ. **UPnP is available on Windows XP** and the router provide the associated support for MSN Messenger to allow full use of the voice, video and messaging features.



After setting **Enable UPnP** setting, an icon of **IP Broadband Connection on Router** on Windows XP/Network Connections will appear. The connection status and control status will be able to be activated. The NAT Traversal of UPnP enables the multimedia features of your applications to operate. This has to manually set up port mappings or use other similar methods. The screenshots below show examples of this facility.

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





The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

Enabling firewall applications on your PC may cause the UPnP function not working properly. This is because these applications will block the accessing ability of some network ports.

Security Considerations

Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

- Some Microsoft operating systems have found out the UPnP weaknesses and hence you need to ensure that you have applied the latest service packs and patches.
- Non-privileged users can control some router functions, including removing and adding port mappings.

The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

4.6 Wireless LAN

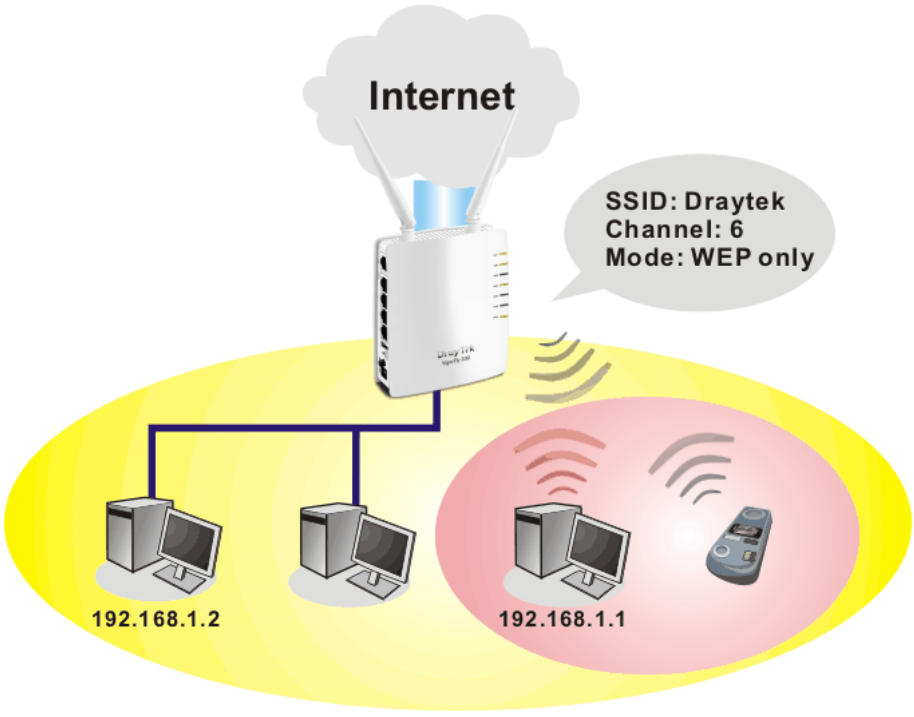
4.6.1 Basic Concepts

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor router is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps*. Hence, you can finally smoothly enjoy stream music and video.

Note: * The actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via Vigor wireless router. The **General Settings** will set up the information of this wireless network, including its SSID as identification, located channel etc.



Security Overview

Real-time Hardware Encryption: Vigor Router is equipped with a hardware AES encryption engine so it can apply the highest protection to your data without influencing user experience.

Complete Security Standard Selection: To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

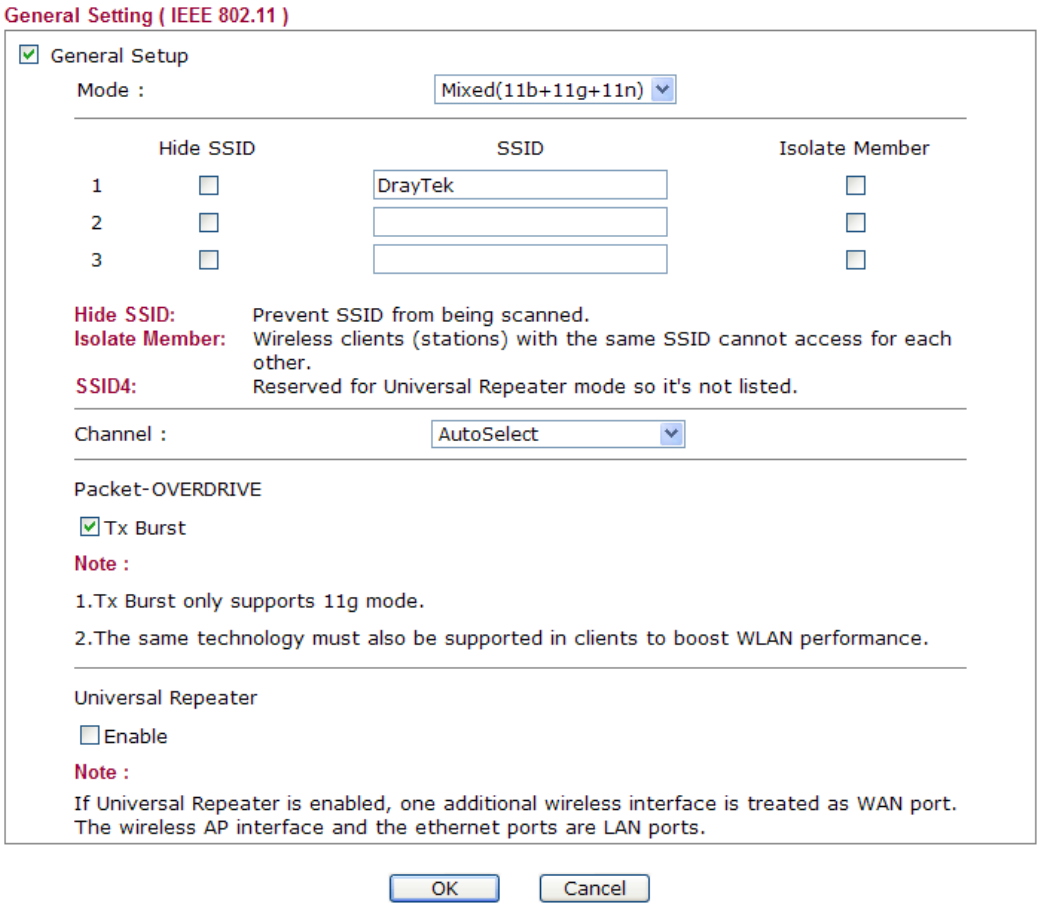
Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The Vigor wireless router is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

Below shows the menu items for Wireless LAN.

4.6.2 General Setup

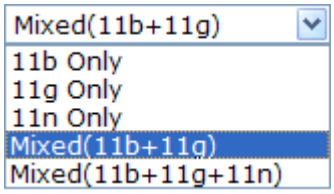
By clicking the **General Setup**, a new web page will appear so that you could configure the SSID and the wireless channel.

Please refer to the following figure for more information.



Enable Wireless LAN Check the box to enable wireless function.

Mode At present, the router can connect to Mixed (11b+11g), 11g Only, 11b Only, Mixed (11g+11n), 11n Only and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.



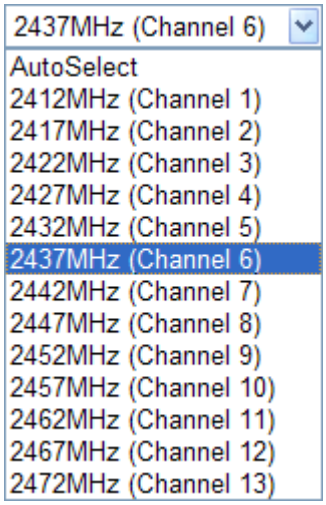
Hide SSID Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set three sets of SSID for different usage.

SSID Set a name for the router to be identified.

Isolate Member Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.

Channel Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of

choosing the frequency, please select AutoSelect to let system determine for you.



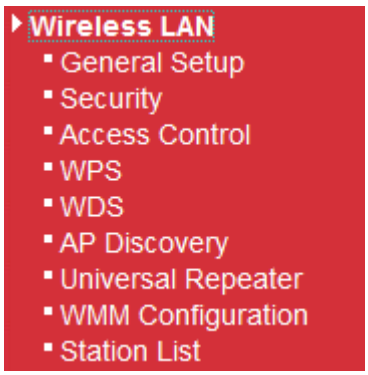
OK Click it to save and apply such setting.

Packet-OVERDRIVE This feature can enhance the performance in data transmission about 40%* more (by checking **Tx Burs**t). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.

Note: Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose **Enable** for **TxBURST** on the tab of **Option**).

Universal Repeater If such mode is enabled, the access point can act as a wireless repeater; it can be Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to service all wireless stations within its coverage.

Check this box to enable the function. Besides, it will be displayed on the Wireless LAN for you to access for detailed configuration.

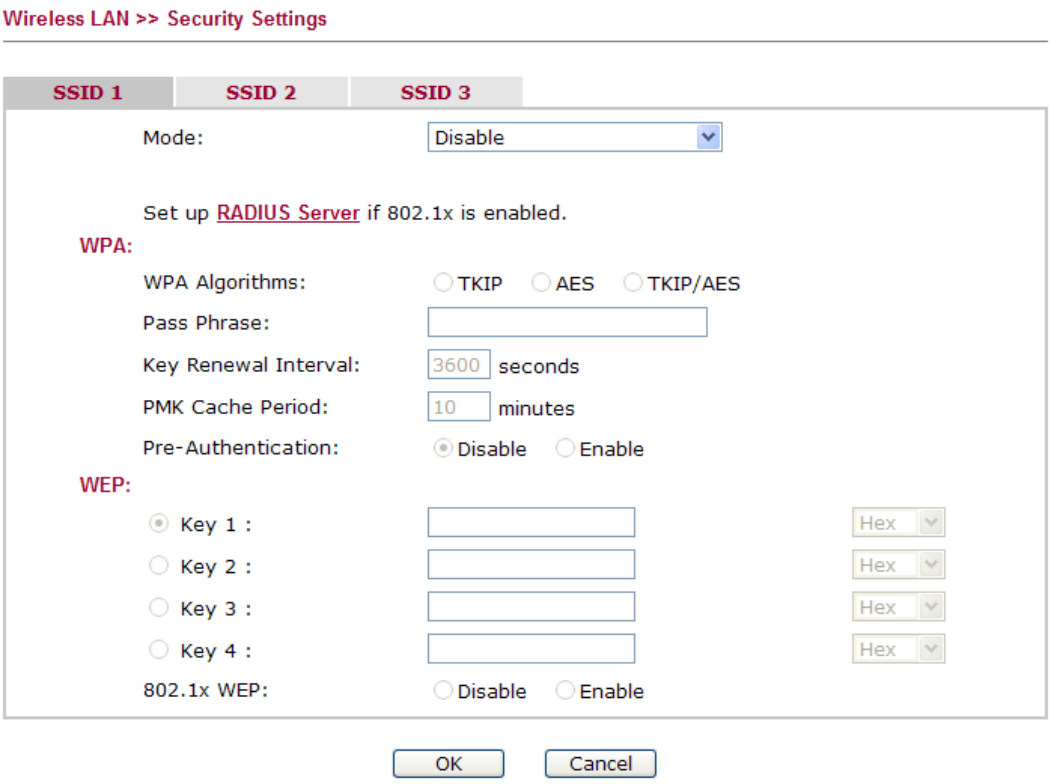


Open **Wireless LAN>>Universal Repeate**r. Please refer to the corresponding section for detailed information.

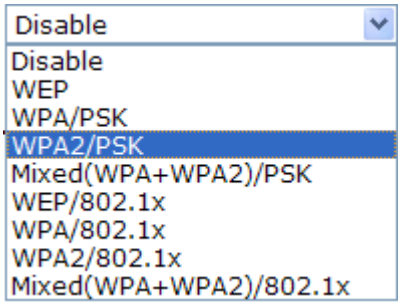
4.6.3 Security

This page allows you to set security with different modes for SSID 1, 2 and 3 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

By clicking the **Security Settings**, a new web page will appear so that you could configure the settings.



Mode There are several modes provided for you to choose.

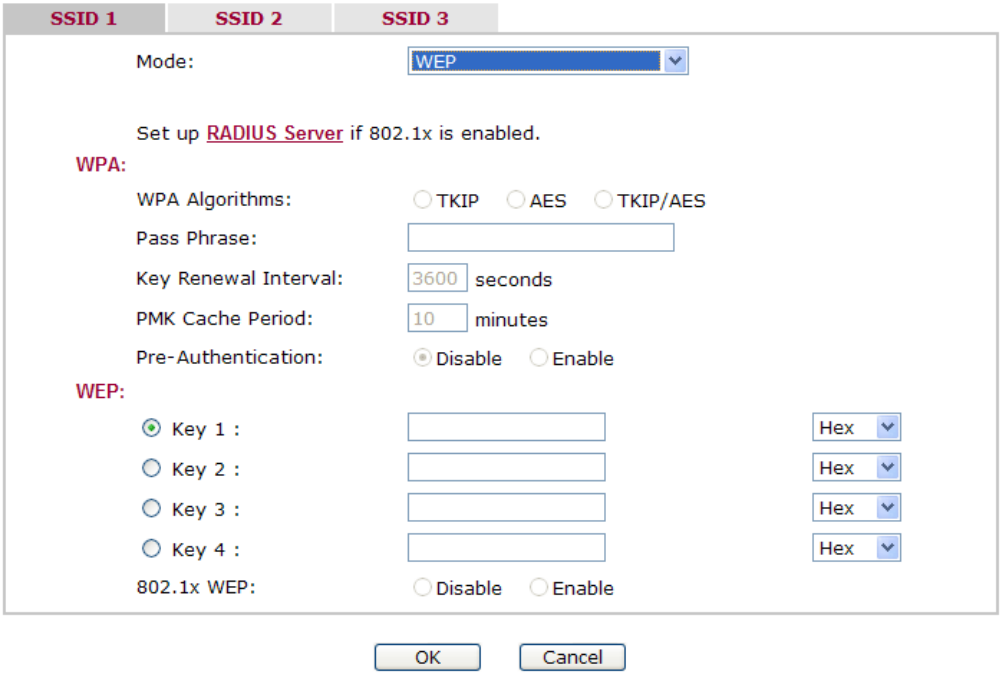


- **Disable**

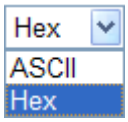
  The encryption mechanism is turned off.

- **WEP**

  Accepts only WEP clients and the encryption key should be entered in WEP Key.

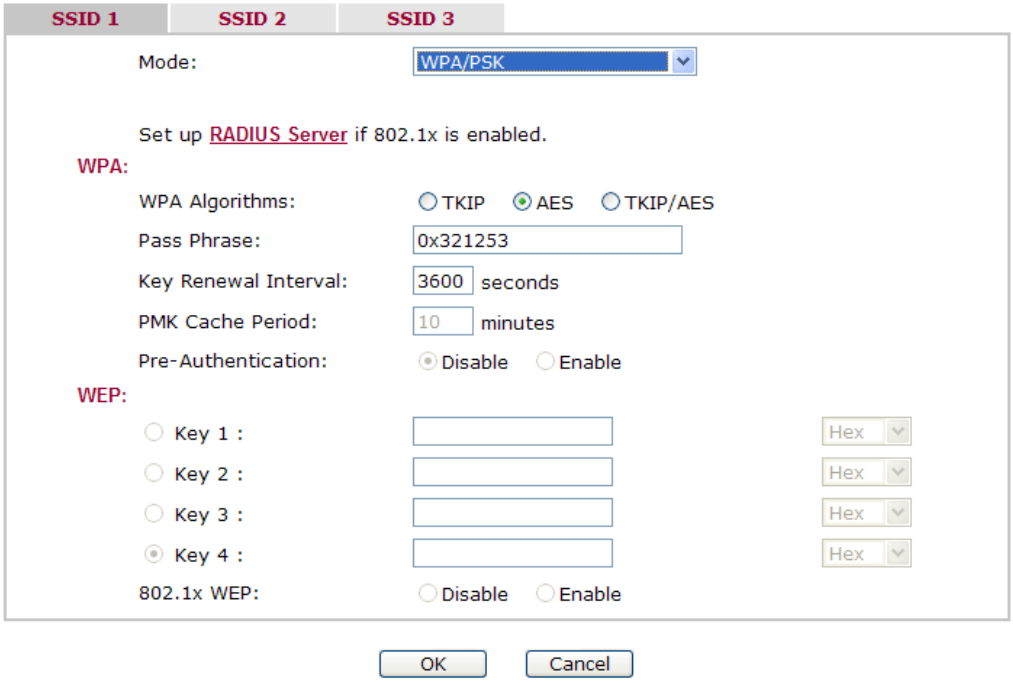


WEP Key1-Key4 Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','.



- **WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK**

  Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.

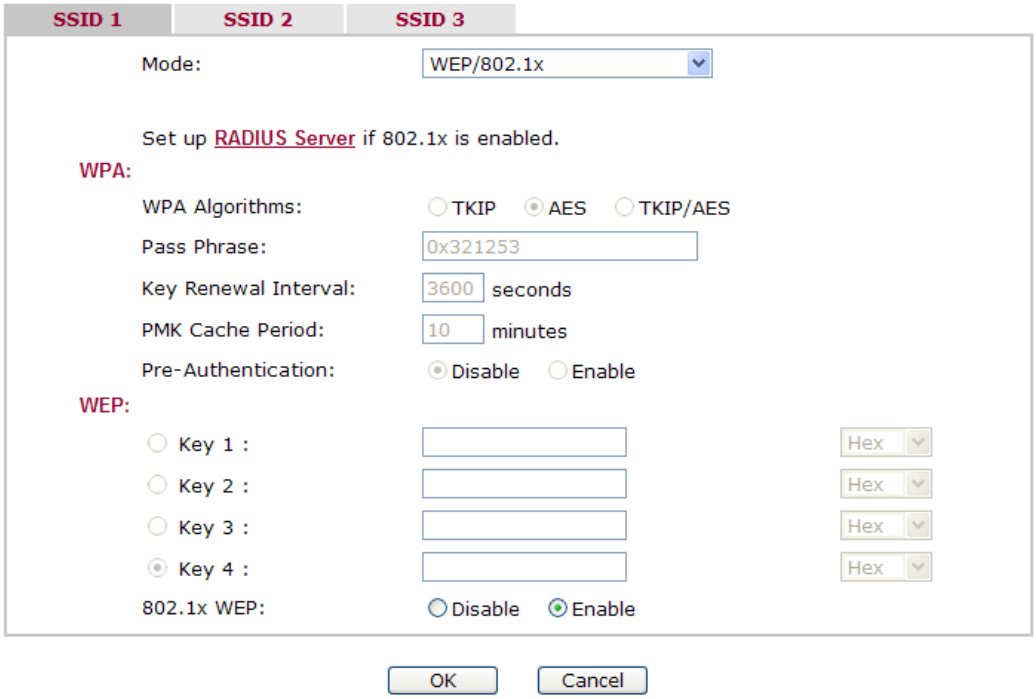


WPA Algorithm	Select TKIP, AES or TKIP/AES as the algorithm for WPA.
Pass Phrase	Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key.

- **WEP/802.1x**

  The built-in RADIUS client feature enables the router to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.

  The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode.

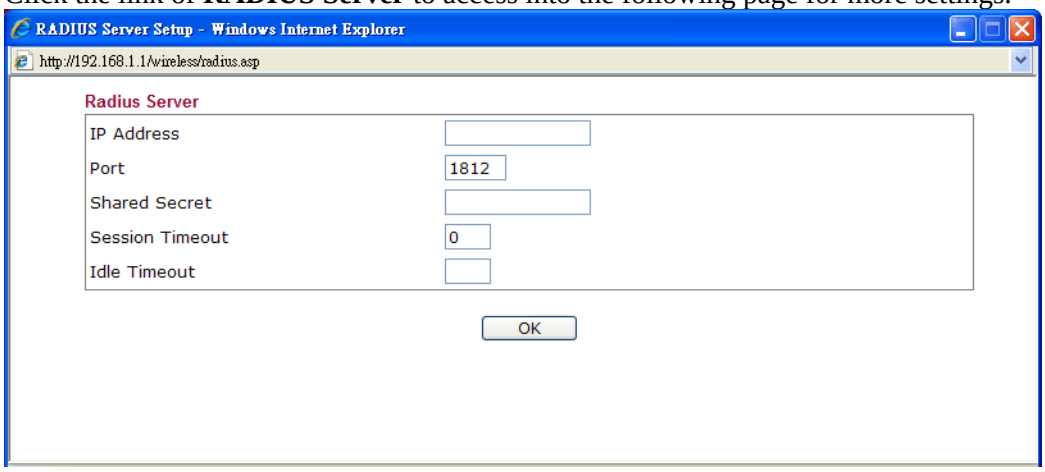


802.1x WEP

Disable - Disable the WEP Encryption. Data sent to the AP will not be encrypted.

Enable - Enable the WEP Encryption.

Click the link of **RADIUS Server** to access into the following page for more settings.



IP Address Enter the IP address of RADIUS server.

Port The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.

Shared Secret The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.

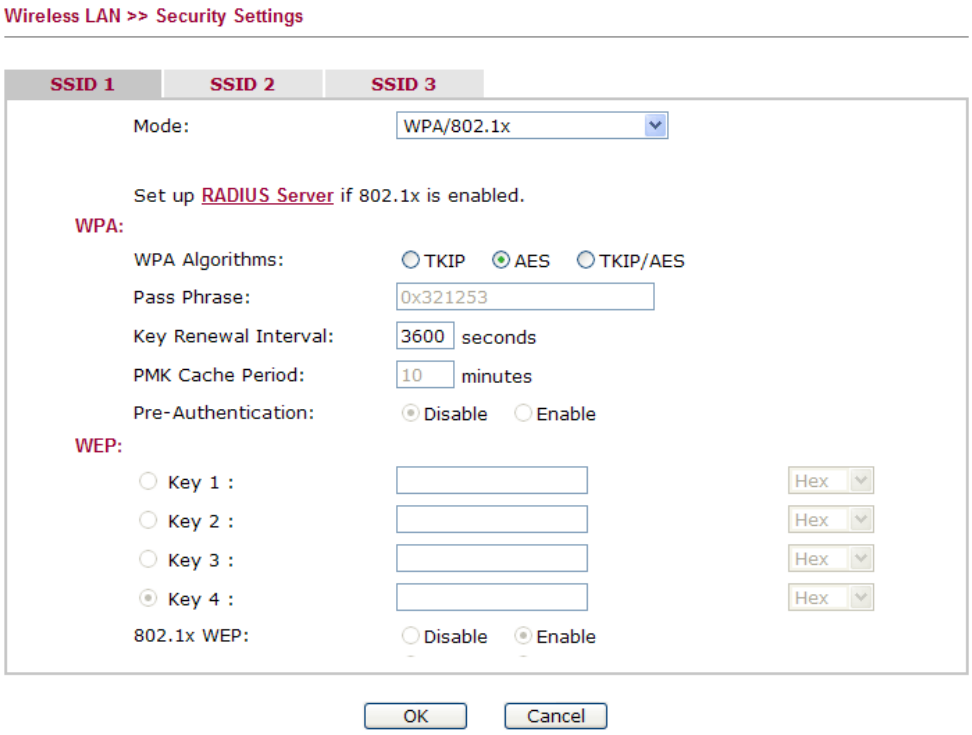
Session Timeout Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)

Idle Timeout Set the maximum time that a wireless device may remain

idle. (The unit is second.)

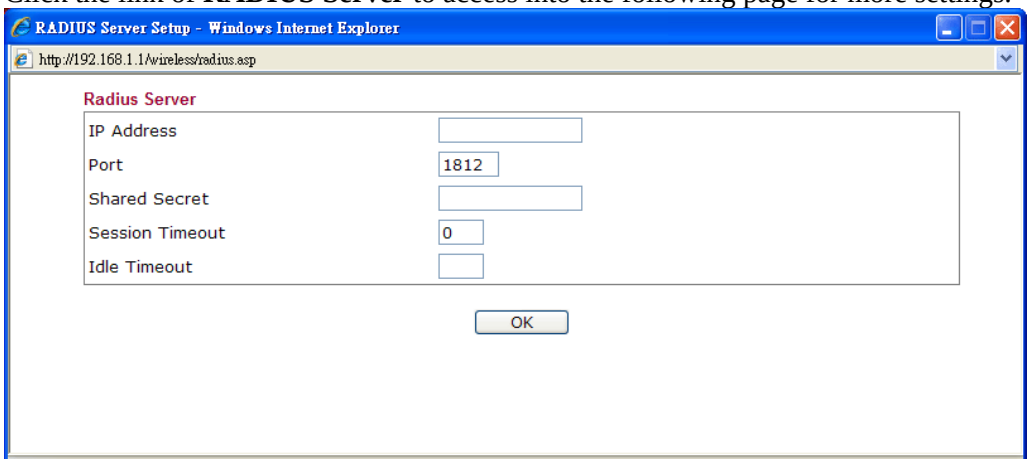
- **WPA/802.1x**

The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.



WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key.

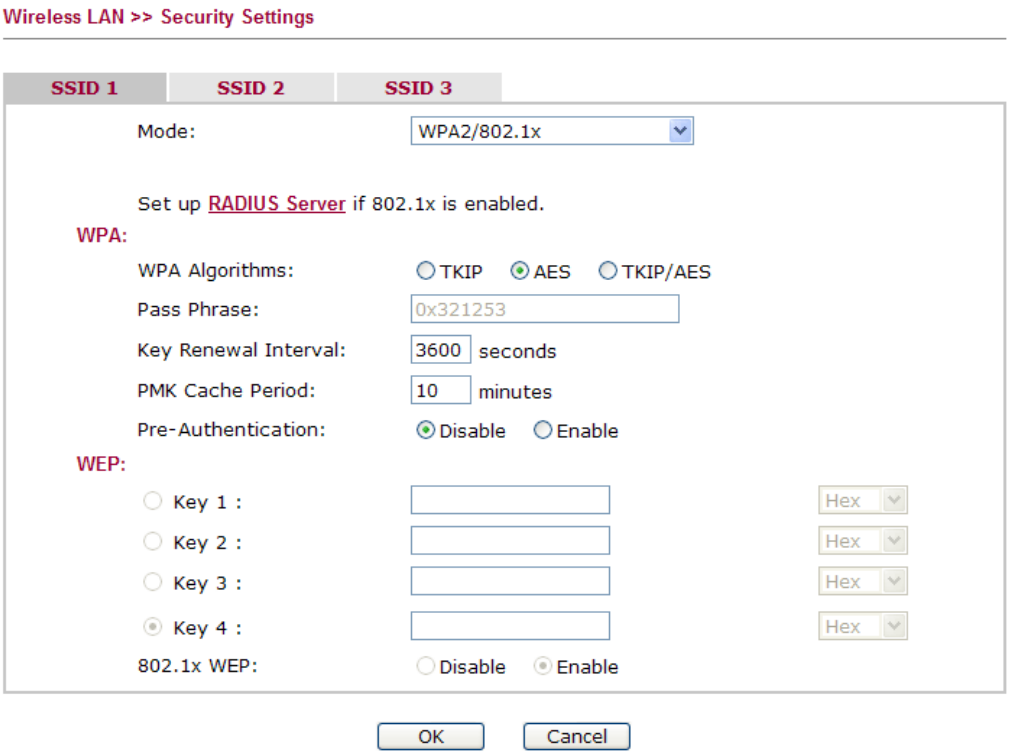
Click the link of **RADIUS Server** to access into the following page for more settings.



IP Address	Enter the IP address of RADIUS server.
Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)
Idle Timeout	Set the maximum time that a wireless device may remain idle. (The unit is second.)

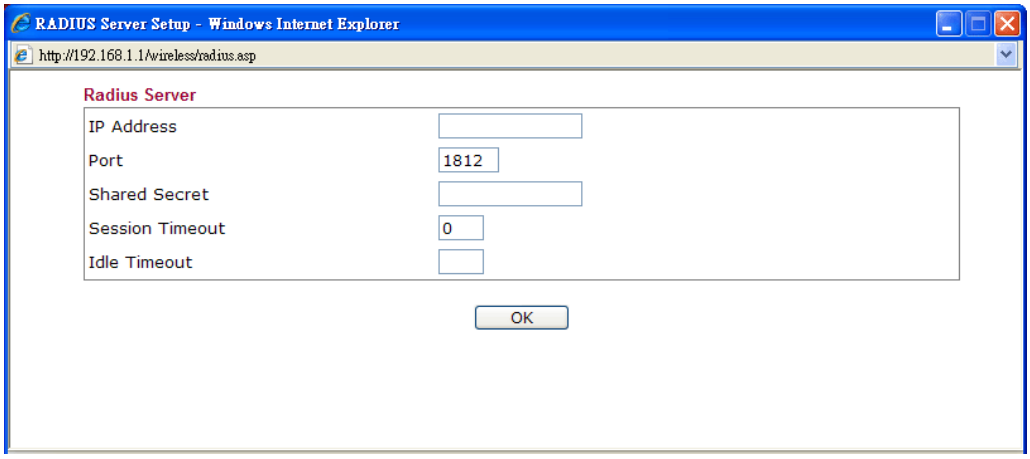
- **WPA2/802.1x**

The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.



WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key.
PMK Cache Period	Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated.
Pre-Authentication	Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2) **Enable** - Enable IEEE 802.1X Pre-Authentication. **Disable** - Disable IEEE 802.1X Pre-Authentication.

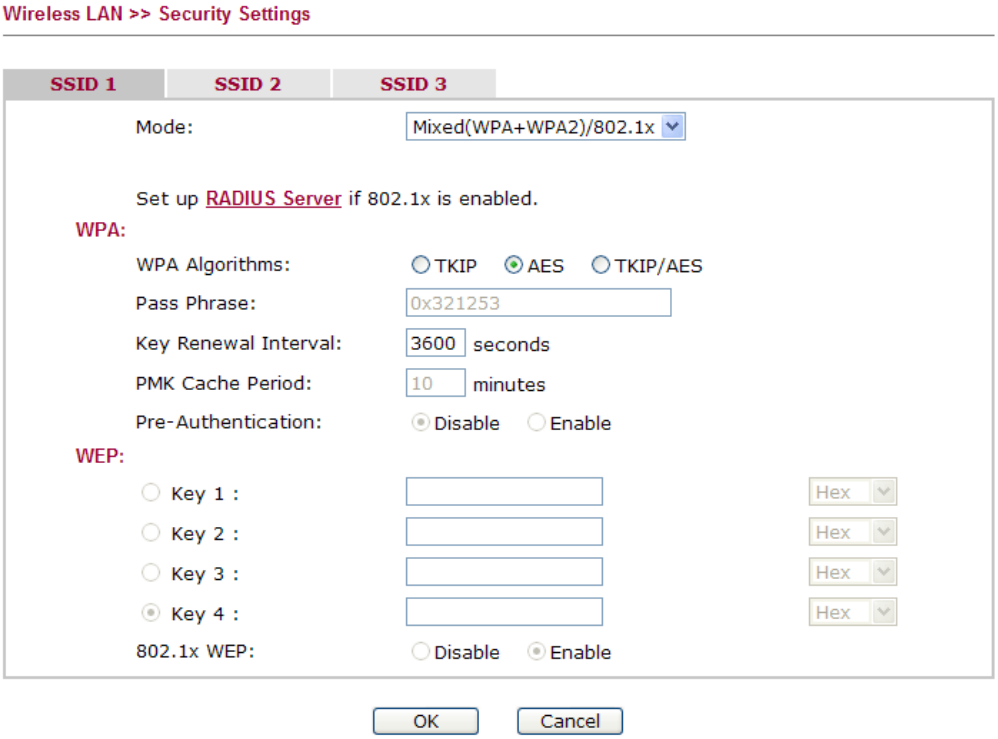
Click the link of **RADIUS Server** to access into the following page for more settings.



IP Address	Enter the IP address of RADIUS server.
Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)
Idle Timeout	Set the maximum time that a wireless device may remain idle. (The unit is second.)

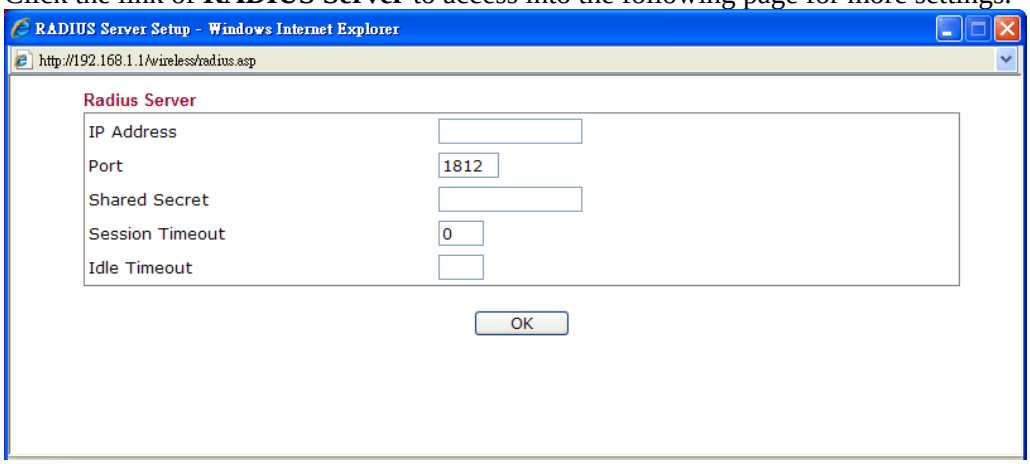
- **Mixed (WPA+WPA2)/802.1x**

  The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.



WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key.?

Click the link of **RADIUS Server** to access into the following page for more settings.

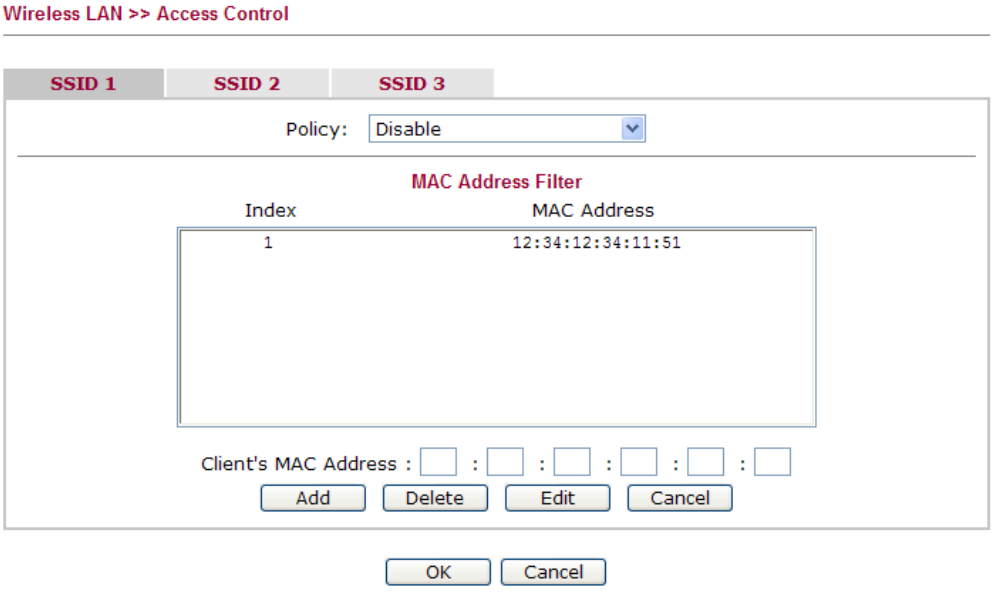


IP Address	Enter the IP address of RADIUS server.
Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.

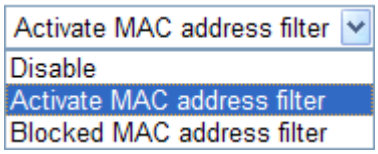
Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)
Idle Timeout	Set the maximum time that a wireless device may remain idle. (The unit is second.)

4.6.4 Access Control

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**, a new web page will appear, as depicted below, so that you could edit the clients' MAC addresses to control their access rights (deny or allow).



Policy	Select to enable any one of the following policy or disable the policy. Choose **Activate MAC address filter** to type in the MAC addresses for other clients in the network manually. Choose **Isolate WLAN from LAN** will separate all the WLAN stations from LAN based on the MAC Address list.



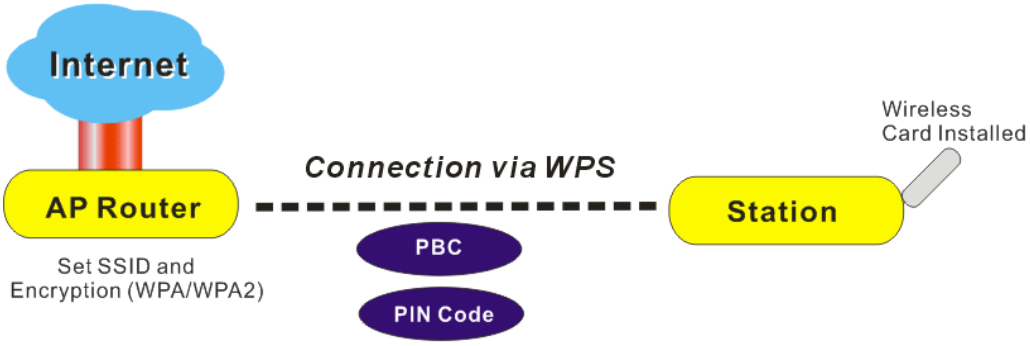
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.

OK	Click it to save the access control list.
Cancel	Clean all entries in the MAC address list.

4.6.5 WPS

WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.

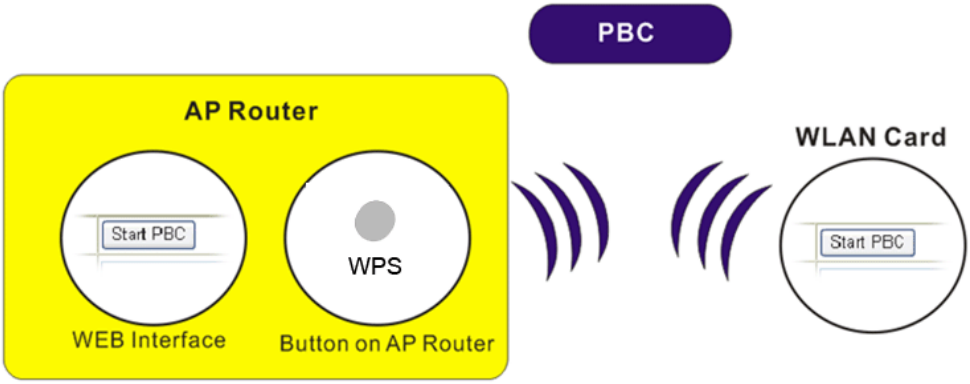
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and router automatically.



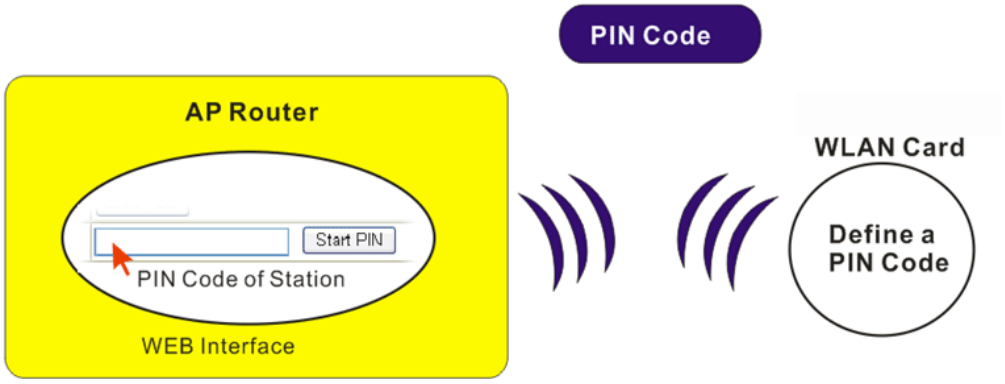
Note: Such function is available for the wireless station with WPS supported.

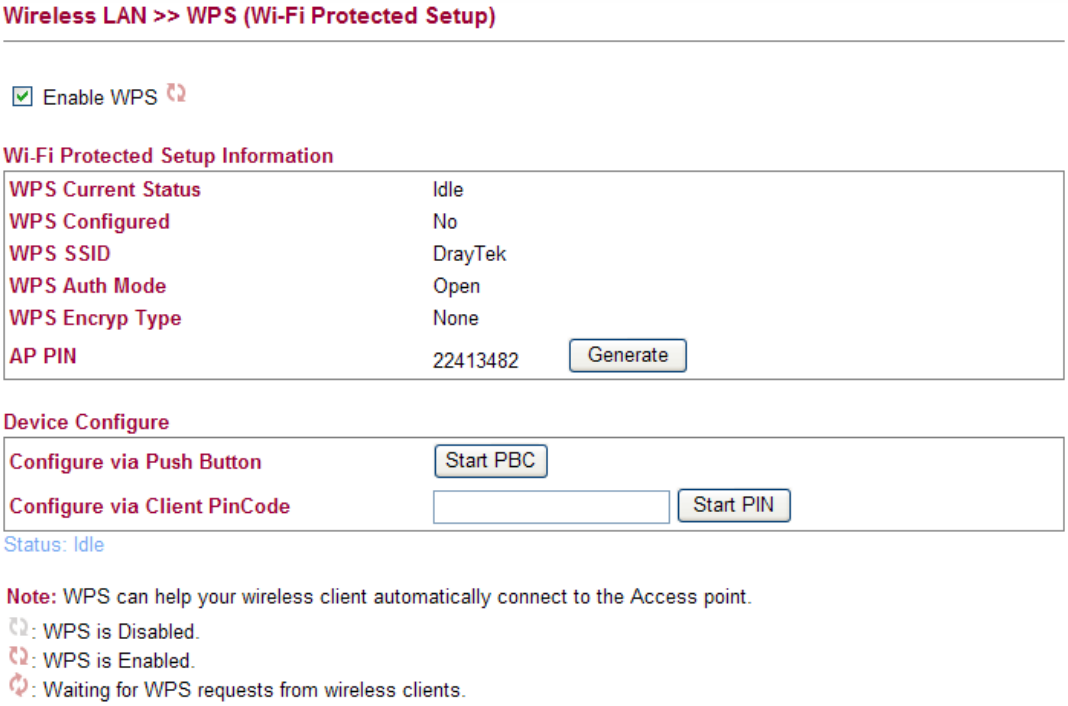
There are two methods to do network connection through WPS between AP and Stations: pressing the ***Start PBC*** button or using ***PIN Code***.

On the side of VigorFly 200 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the vigor router.





Enable WPS	Check this box to enable WPS setting.
WPS Current Status	Display related system information for WPS. If the wireless security (encryption) function of the router is properly configured, you can see 'Configured' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encryp Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of the router.
AP PIN	The number displayed here is used for remote client entering the registrar's PIN code in remote station to make a network connection.
Configure via Push Button	Click **Start PBC** to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return

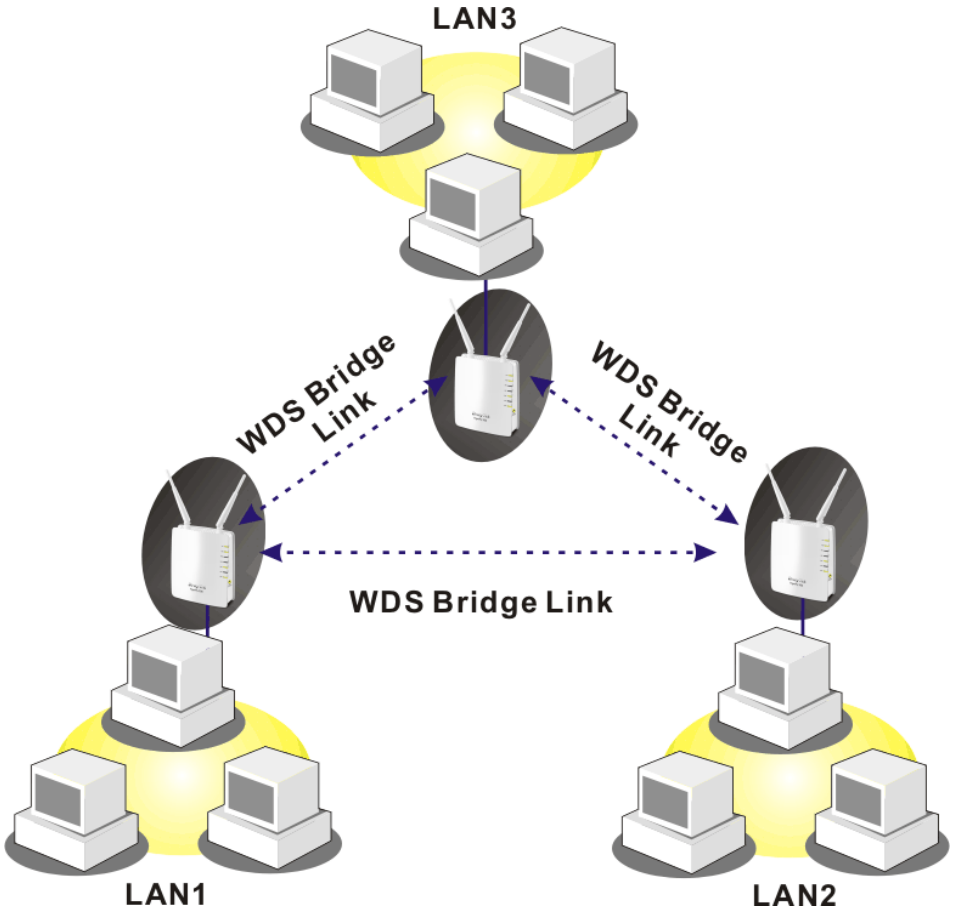
	to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Type the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. The WLAN LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes.

4.6.6 WDS

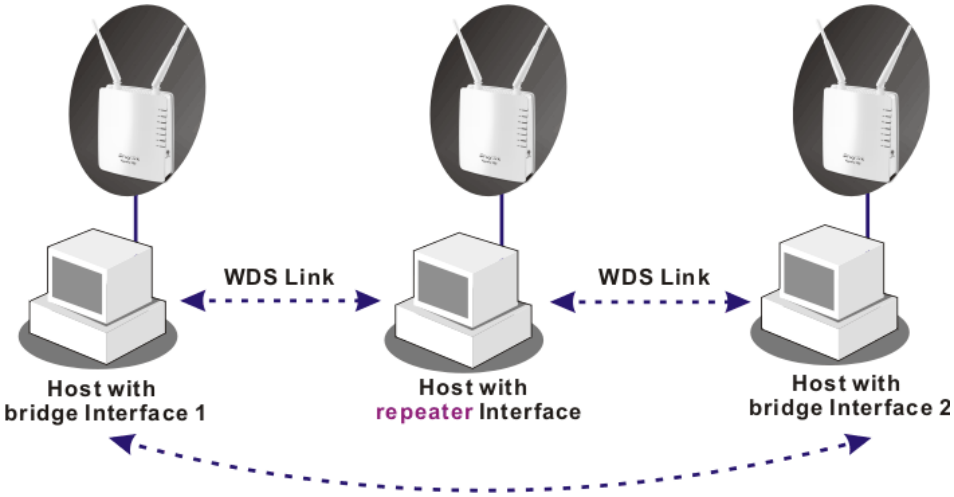
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.

To meet the above requirement, two WDS modes are implemented in Vigor router. One is **Bridge**, the other is **Repeater**. Below shows the function of WDS-bridge interface:

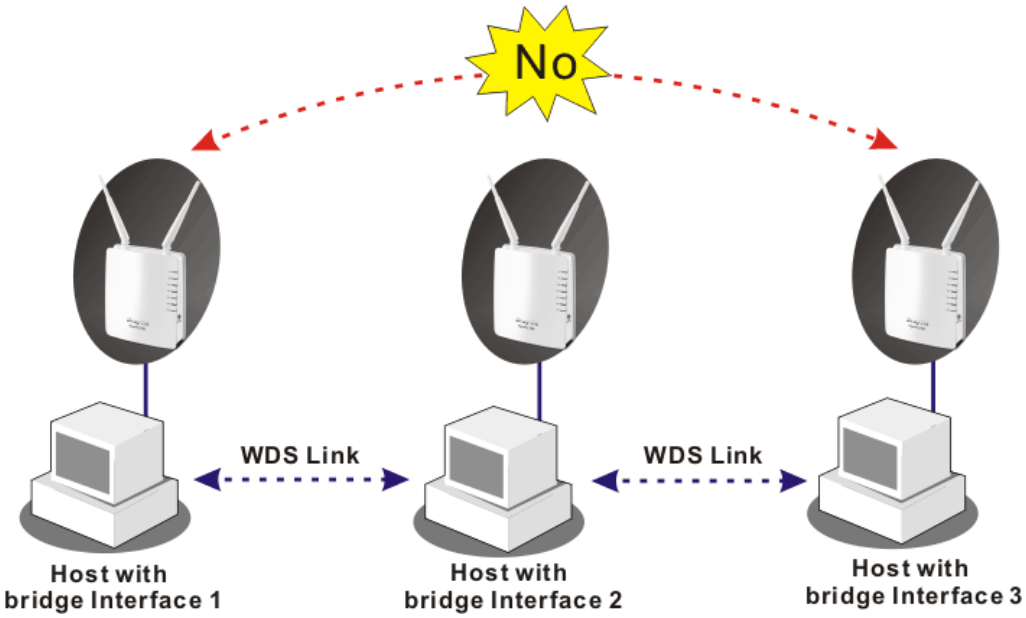


The application for the WDS-Repeater mode is depicted as below:

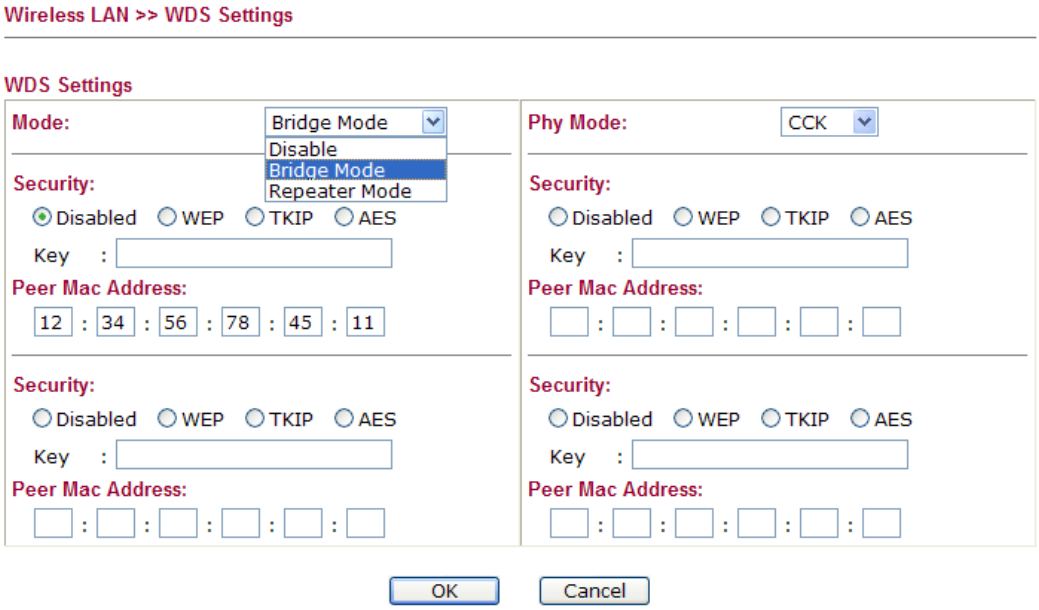


The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words, only Repeater mode can do WDS-to-WDS packet forwarding.

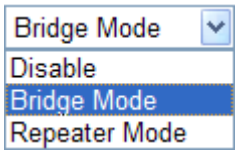
In the following examples, hosts connected to Bridge 1 or 3 can communicate with hosts connected to Bridge 2 through WDS links. However, hosts connected to Bridge 1 CANNOT communicate with hosts connected to Bridge 3 through Bridge 2.



Click **WDS** from **Wireless LAN** menu. The following page will be shown.



Mode Choose the mode for WDS setting. **Disable** mode will not invoke any WDS setting. **Bridge Mode** is designed to fulfill the first type of application. **Repeater Mode** is for the second one.



Security There are four types for security, **Disabled**, **WEP**, **TKIP** and **Key** or **Peer Mac Address** field valid or not. Choose one of the types for the router. Please disable the unused link to get better performance.

Key Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by “0x”.

Peer Mac Address Four peer MAC addresses are allowed to be entered in this page at one time.

Phy Mode There are three types of transmission rates developed by different techniques for **Phy Mode**. Data will be transmitted via communication channel.

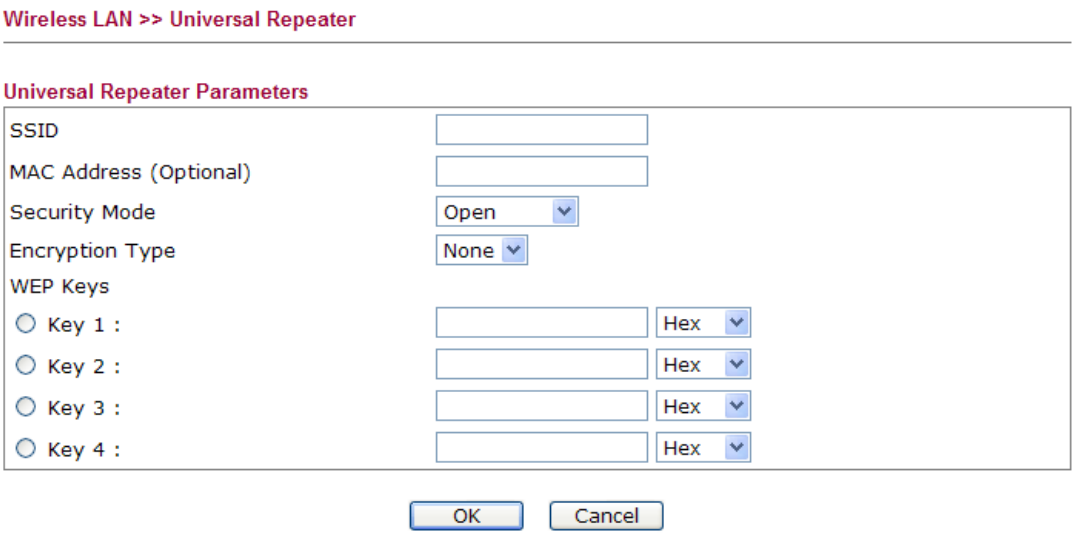
OK Click this button to save the configuration.

4.6.7 Universal Repeater

This menu is available only when it is enabled in **Wireless LAN>>General Setup**. It allows you to specify which AP that remote client can connect to.

The access point can act as a wireless repeater; it can be Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to serve all wireless stations within its coverage.

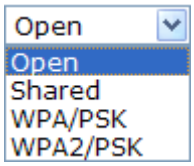
> **Note:** While using Universal Repeater Mode, the access point will demodulate the received signal. Please check if this signal is noise for the operating network, then have the signal modulated and amplified again. The output power of this mode is the same as that of WDS and normal AP mode.



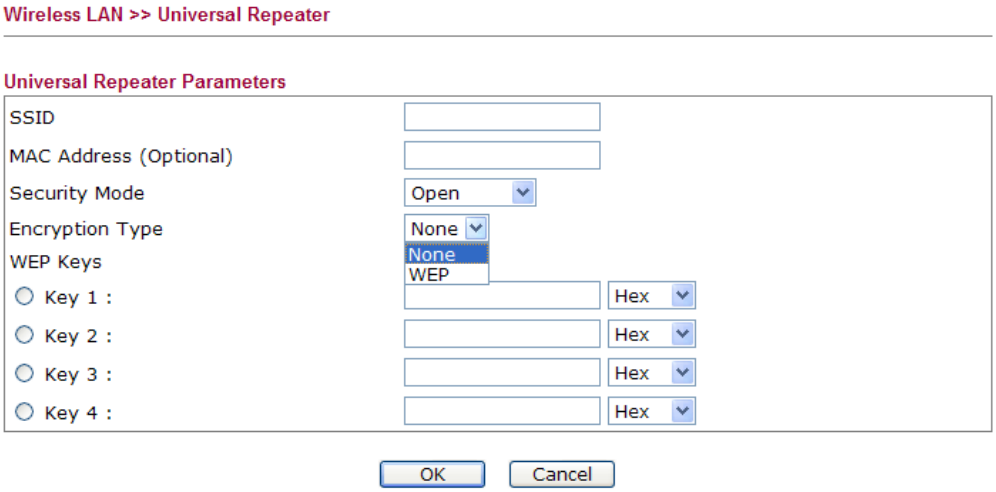
SSID Set a name for the router to be identified.

MAC Address (Optional) Type the MAC address of the Access Point that VigorFly 200 wants to connect to.

Security Mode There are several modes provided for you to choose. Each mode will bring up different parameters (e.g., WEP keys, Pass Phrase) for you to configure.

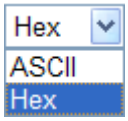


- **Open / Shared Mode**

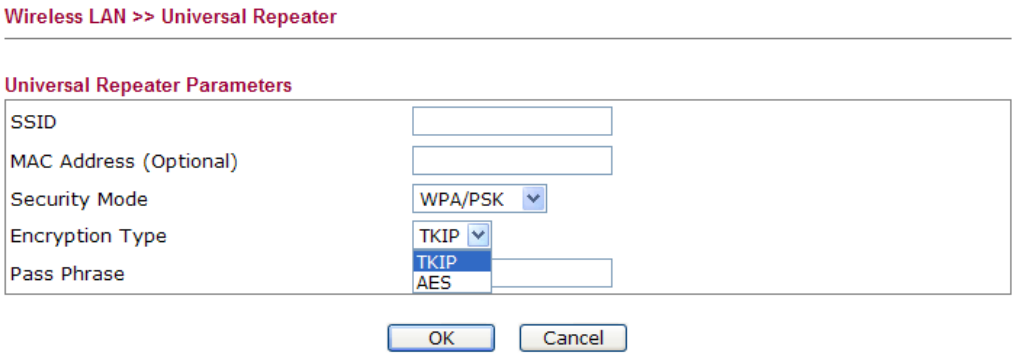


Encryption Type — Choose **None** to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose **WEP**.

WEP Keys — Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','.



- **WPA/PSK Mode and WPA2/PSK Mode**



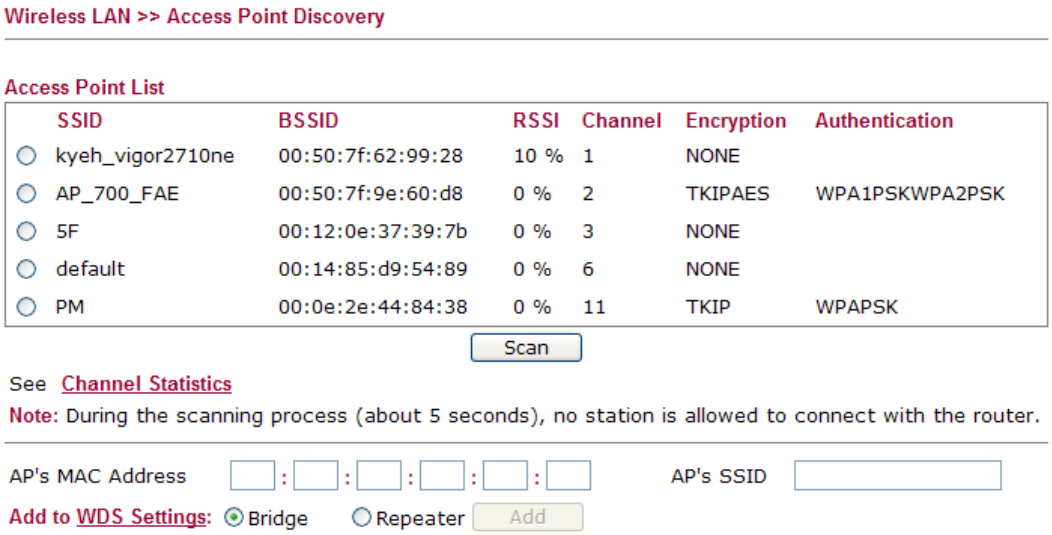
Encryption Type — Select TKIP or AES as the algorithm for WPA.

Pass Phrase — Either **8~63** ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

4.6.8 AP Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover all the connected APs.

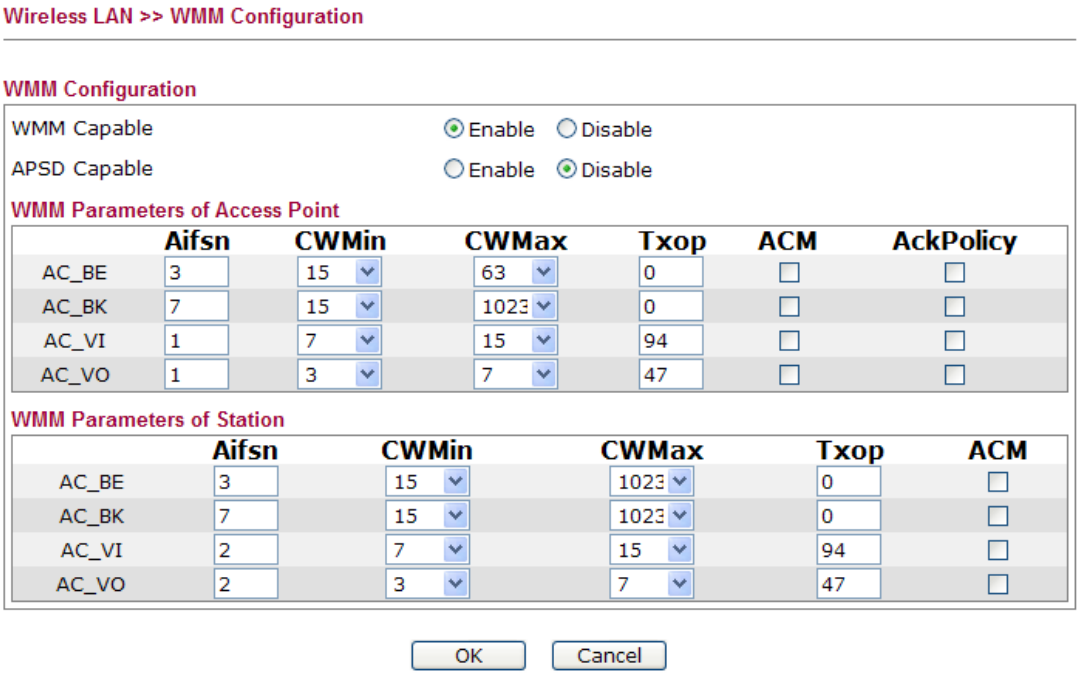


SSID	Display the SSID of the AP scanned by this router.
BSSID	Display the MAC address of the AP scanned by this router.
RSSI	Display the signal strength. RSSI is the abbreviation of Receive Signal Strength Indication.
Channel	Display the wireless channel used for the AP that is scanned by this router.
Encryption	Display the encryption mode for the scanned AP.
Authentication	Display the authentication type that the scanned AP applied.
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button
Statistics	It displays the statistics for the channels used by APs.
AP's MAC Address	If you want the found AP applying the WDS settings, please type in the AP's MAC address.
AP's SSID	To specify an AP to be applied with WDS settings, you can specify MAC address or SSID for the AP. Here is the place that you can type the SSID of the AP.
Add	Click **Bridge** or **Repeater** for the specified AP. Next, click **Add**. Later, the MAC address of the AP will be added and be shown on WDS settings page.

4.6.9 WMM Configuration

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC_BE , AC_BK, AC_VI and AC_VO for WMM.

APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency. Such function is designed for mobile and cordless phones that support VoIP mostly.



WMM Capable — To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.

APSD Capable — The default setting is **Disable**. Click **Enable** to enable the function of automatic power-save delivery (APSD).

Aifsn — It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories. As to the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.

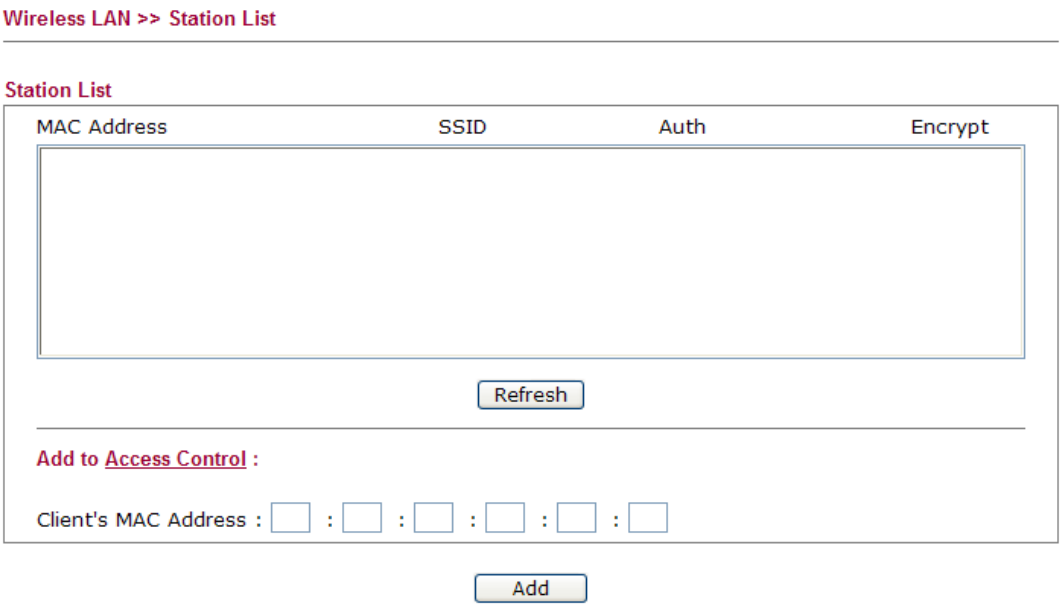
CWMin/CWMax — **CWMin** means contention Window-Min and **CWMax** means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.

Txop — It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data

	transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
ACM	It is an abbreviation of Admission Control Mandatory. It can restrict stations from using specific category class if it is checked.
AckPolicy	"Uncheck" (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets.
OK	Click this button to save the configuration.

4.6.10 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code.

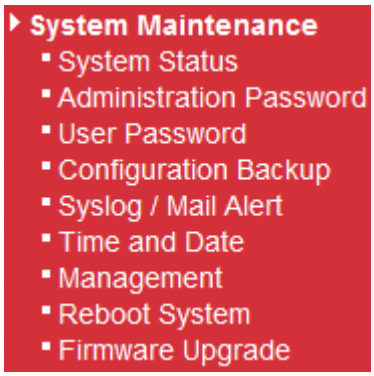


MAC Address	Display the MAC Address for the connecting client.
SSID	Display the SSID that the wireless client connects to.
Auth	Display the authentication that the wireless client uses for connection with such AP.
Encrypt	Display the encryption mode used by the wireless client.
Refresh	Click this button to refresh the status of station list.
Add to Access Control	**Client's MAC Address** - For additional security of wireless access, the Access Control facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface.
Add	Click this button to add current typed MAC address into **Access Contro**l.

4.7 System Maintenance

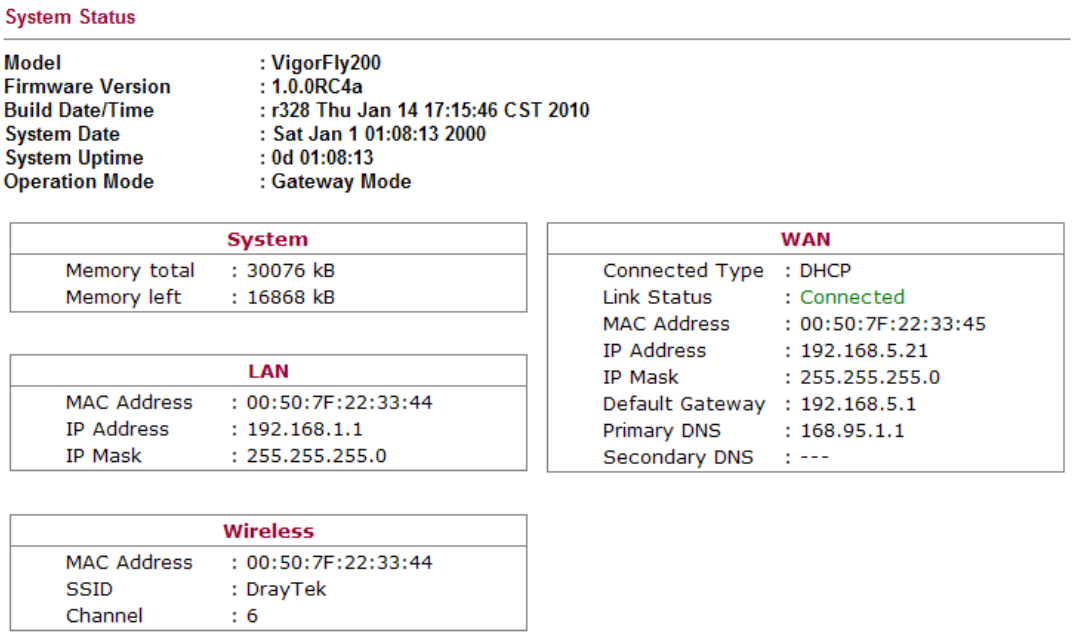
For the system setup, there are several items that you have to know the way of configuration: System Status, Administrator Password, Configuration Backup, Syslog/Mail Alert, Time and Date, Management, Reboot System, and Firmware Upgrade.

Below shows the menu items for System Maintenance.



4.7.1 System Status

The **System Status** provides basic network settings of Vigor router. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.

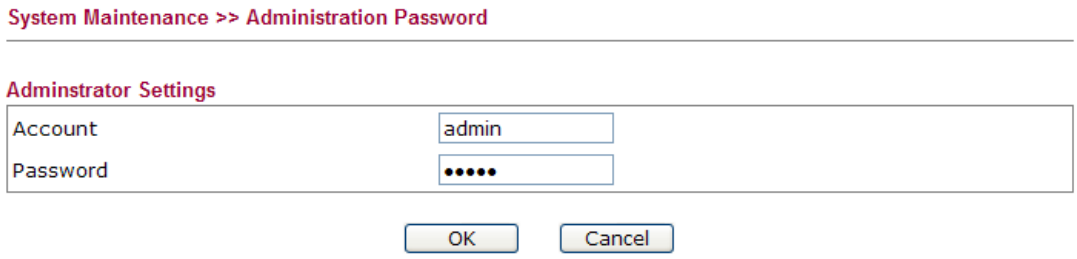


Model	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
System Date	Display current time and date for the system server.
System Uptime	Display the connection time for the system server.
Operation Mode	Display the connection mode for the router.
Memory total	Display the total dynamic RAM size for the whole system.
Memory left	Display the remaining RAM size for the whole system.

MAC Address	Display the MAC address of the LAN or WAN or WLAN Interface.
IP Address	Display the MAC address of the LAN or WAN Interface.
IP Mask	Display the subnet mask address of the LAN or WAN interface.
Device Type	Display the device type used for wireless LAN.
SSID	Display the SSID of this router.
Channel	Display the channel that wireless LAN used.
Connected Type	Display the network connection type for this router.
Link Status	Display if current network is connected or not.
Default Gateway	Display the gateway address of the WAN interface.
Primary DNS	Display the specified primary DNS setting.
Secondary DNS	Display the specified secondary DNS setting.

4.7.2 Administration Password

This page allows you to set new password for admin operation.

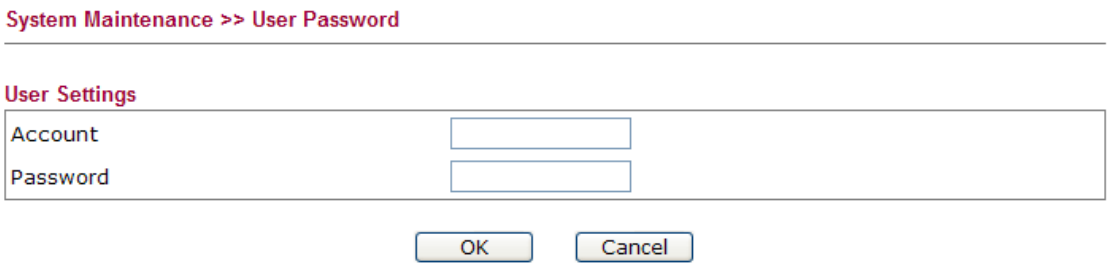


Account	Type in the name for login.
Password	Type in new password in this filed.

When you click **OK**, the login window will appear. Please use the new login name and password to access into the web configurator for admin operation again.

4.7.3 User Password

This page allows you to set new password for user operation.



Account	Type in the name for login.
Password	Type in new password in this filed.

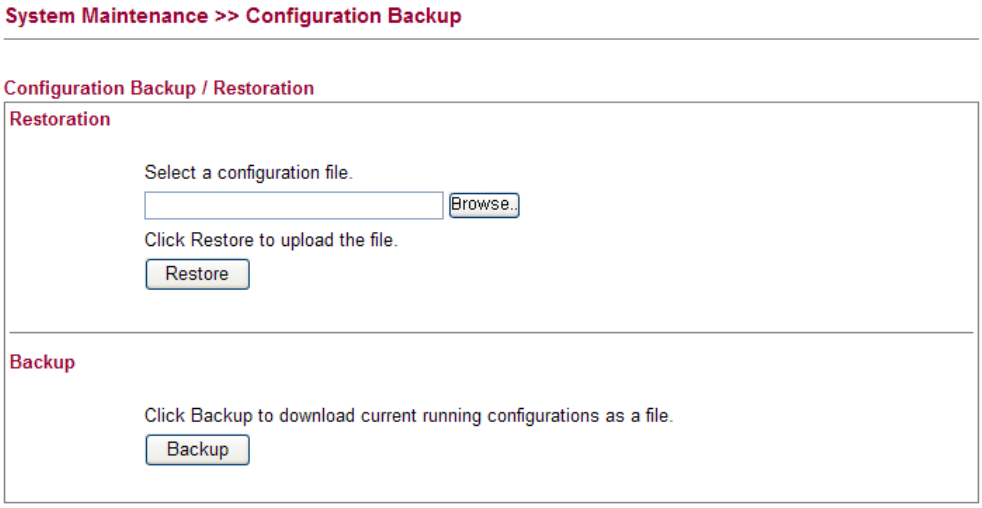
When you click **OK**, the login window will appear. Please use the new password to access into the web configurator for user operation again.

4.7.4 Configuration Backup

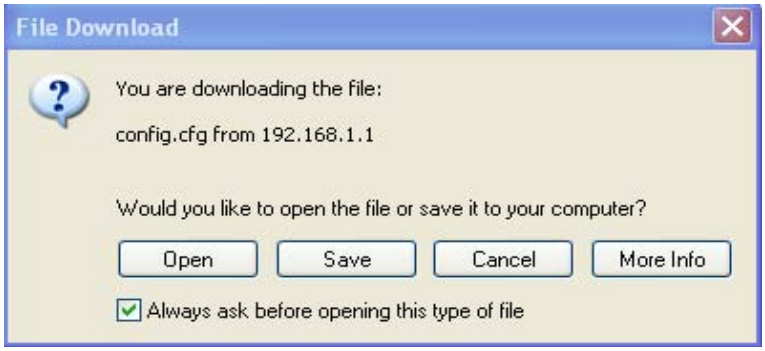
Backup the Configuration

Follow the steps below to backup your configuration.

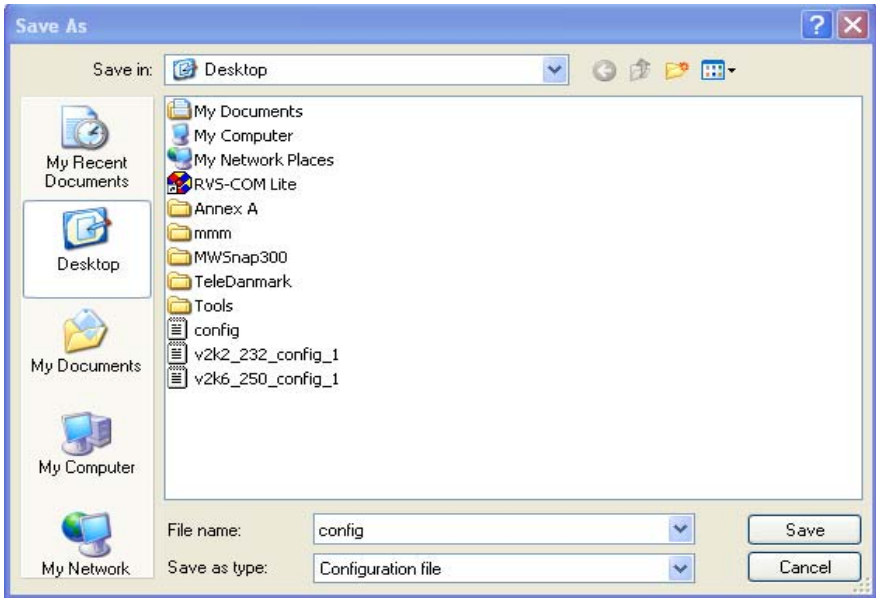
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.



2. Type a key arbitrarily for encrypting the file. Keep the key in mind. You will need it whenever you want to restore such file. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.



3. In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.



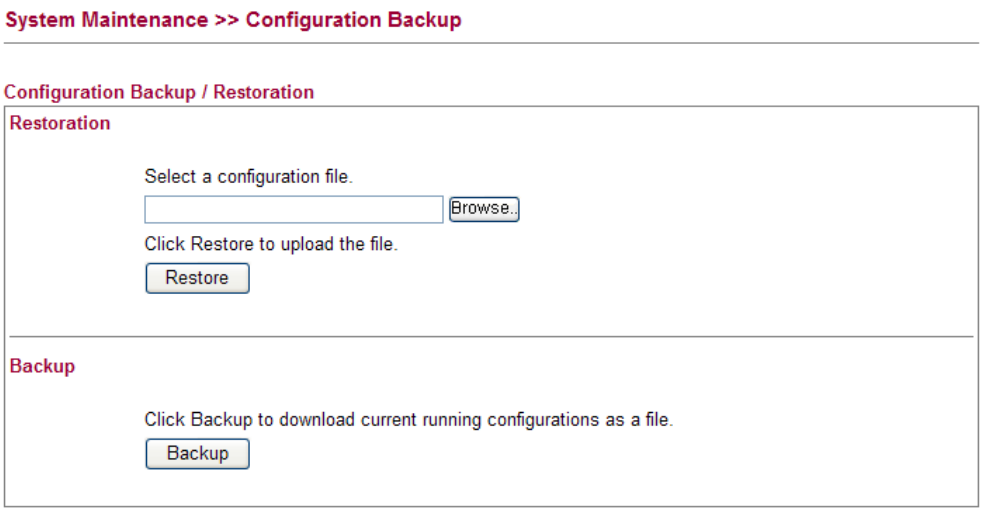
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.

> **Note:** Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

Restore Configuration

1. Go to **System Maintenance** >> **Configuration Backup**. The following screen will be shown as below.

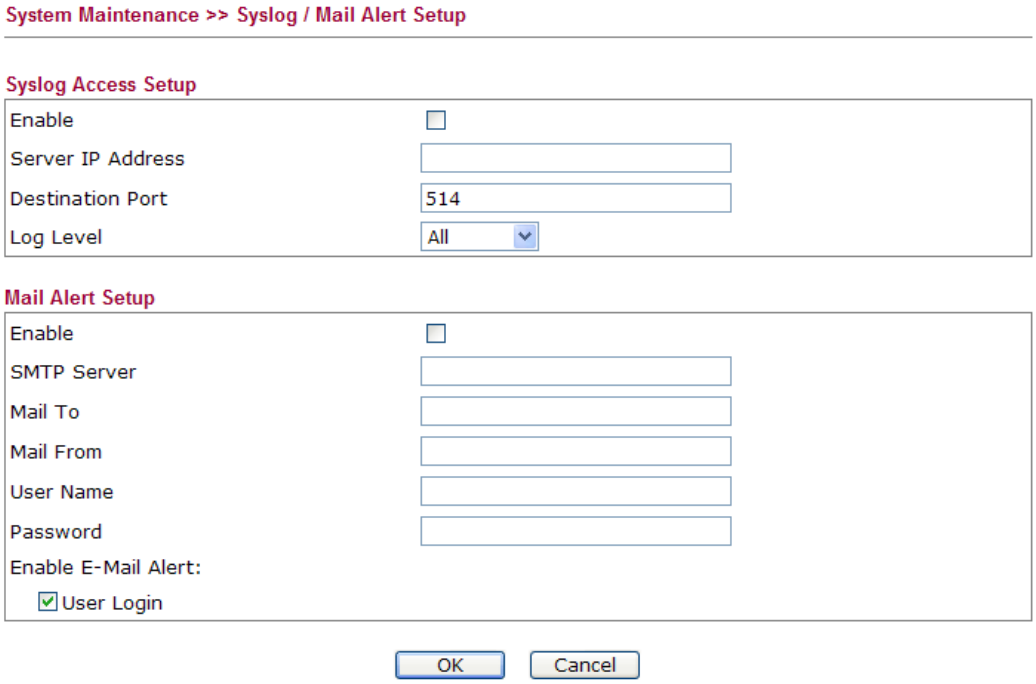


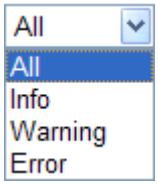
2. Click **Browse** button to choose the correct configuration file for uploading to the router.
3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

> **Note:** If the file you want to restore has been encrypted, you will be asked to type the encrypted key before clicking **Restore**.

4.7.5 Syslog/Mail Alert

SysLog function is provided for users to monitor router. There is no bother to directly get into the Web Configurator of the router or borrow debug equipments.

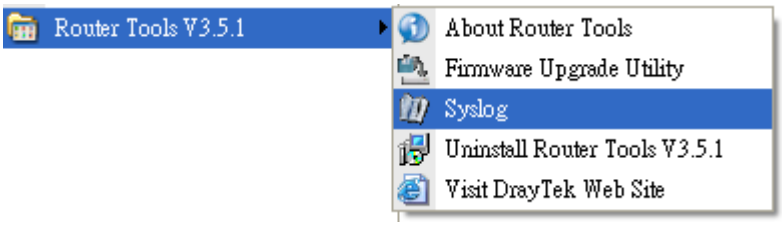


Enable (for Syslog Access Setup)	Check **Enable** to activate function of syslog.
Server IP Address	The IP address of the Syslog server.
Destination Port	Assign a port for the Syslog protocol.
Log Level	Choose the severity level for the system log entry. 
Enable (for Mail Alert Setup)	Check "**Enable**" to activate function of mail alert.
SMTP Server	The IP address of the SMTP server.
Mail To	Assign a mail address for sending mails out.
Mail From	Assign a path for receiving the mail from outside.
User Name	Type the user name for authentication.
Password	Type the password for authentication.
Enable E-mail Alert	Check the box of **User Login** to send alert message to the e-mail box while the router detecting the item(s) you specify here.

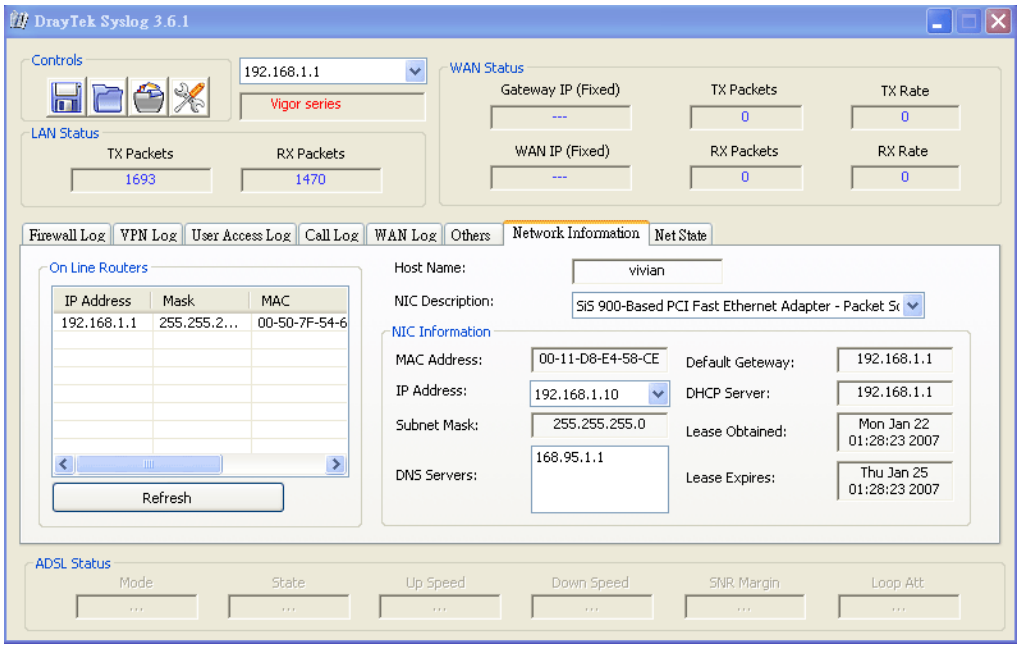
Click **OK** to save these settings.

For viewing the Syslog, please do the following:

1. Just set your monitor PC's IP address in the field of Server IP Address
2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.

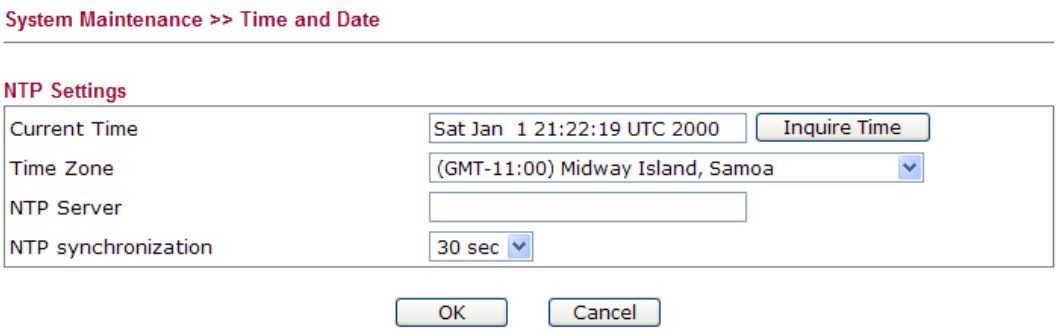


3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.



4.7.6 Time and Date

It allows you to specify where the time of the router should be inquired from.

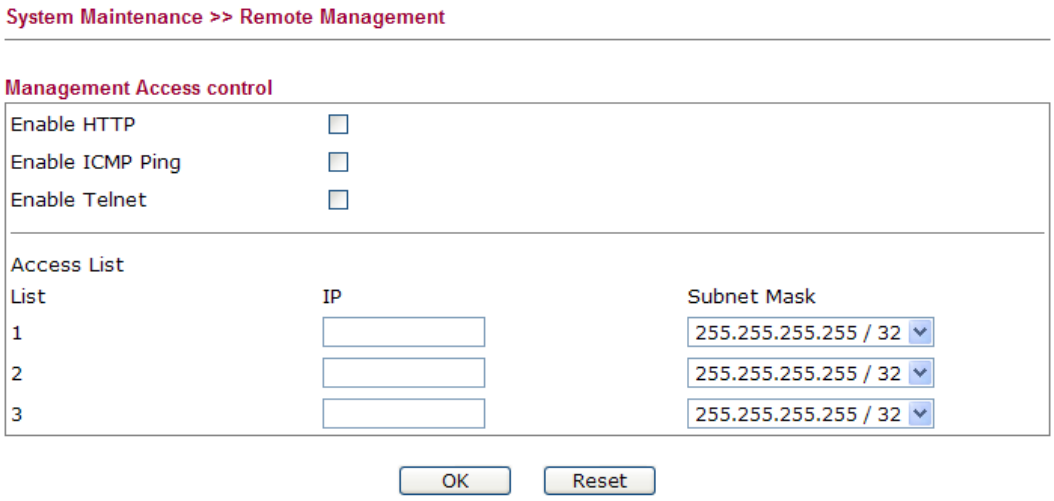


Current Time	Click **Inquire Time** to get the current time.
Time Zone	Select the time zone where the router is located.
NTP Server	Type a new NTP server.
NTP synchronization	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

4.7.7 Management

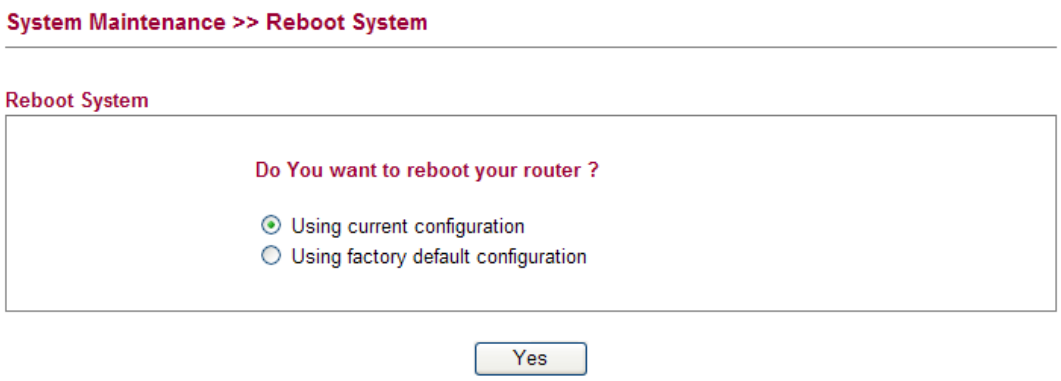
This page allows you to manage the settings for access control, access list, port setup, and SMP setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session.



Enable HTTP/ICMP Ping/Telnet	Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
Access List	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed. **List IP** - Indicate an IP address allowed to login to the router. **Subnet Mask** - Represent a subnet mask allowed to login to the router.

4.7.8 Reboot System

The Web Configurator may be used to restart your router for using current configuration. Click **Reboot System** from **System Maintenance** to open the following page.



Click **Yes**. The router will take 5 seconds to reboot the system.

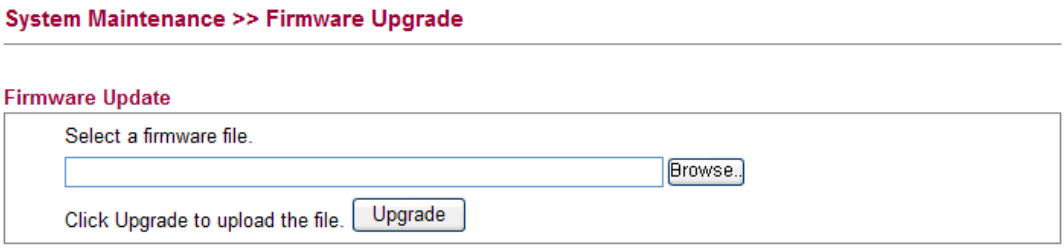
Note: When the system pops up Reboot System web page after you configure web settings, please click **Yes** to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

4.7.9 Firmware Upgrade

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.draytek.com (or local DrayTek's web site) and FTP site is ftp.draytek.com.

Click **Maintenance>> Firmware Upgrade** to launch the Firmware Upgrade Utility.

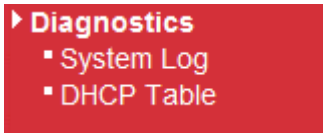


Click **Browse..** to locate the newest firmware and click **Upgrade**. During the process of upgrade, do not turn off your router.

4.8 Diagnostics

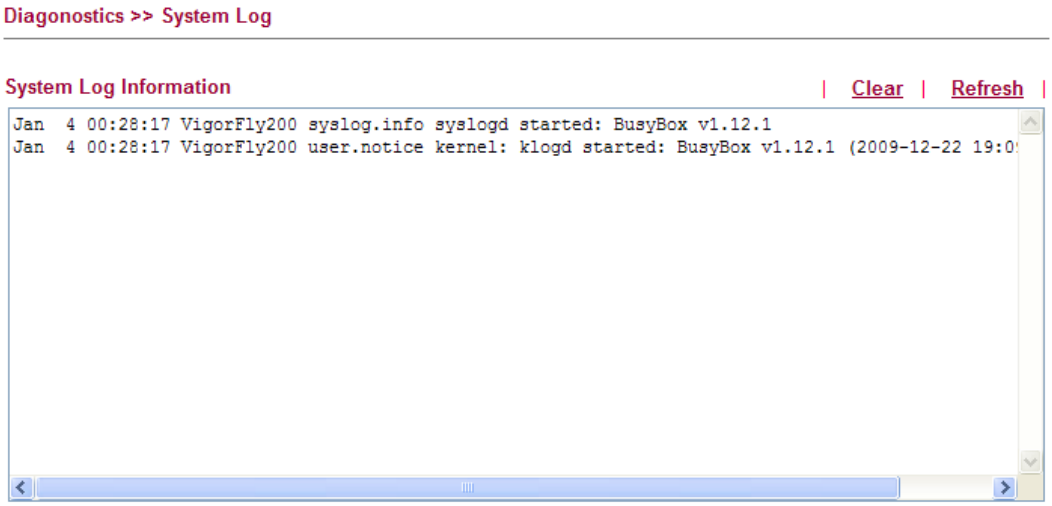
Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router.

Below shows the menu items for Diagnostics.



4.8.1 System Log

Click **Diagnostics** and click **System Log** to open the web page.

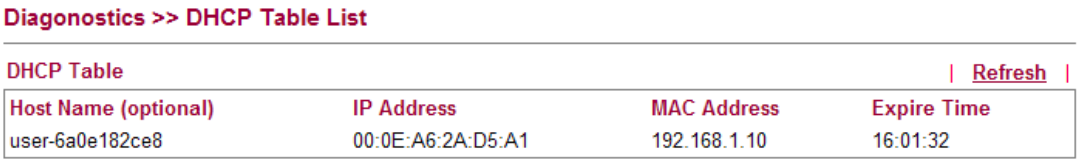


Clear	Click it to clear this page.
Refresh	Click it to reload the page.

4.8.2 DHCP Table

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

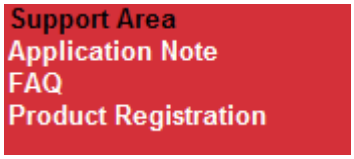
Click **Diagnostics** and click **DHCP Table** to open the web page.



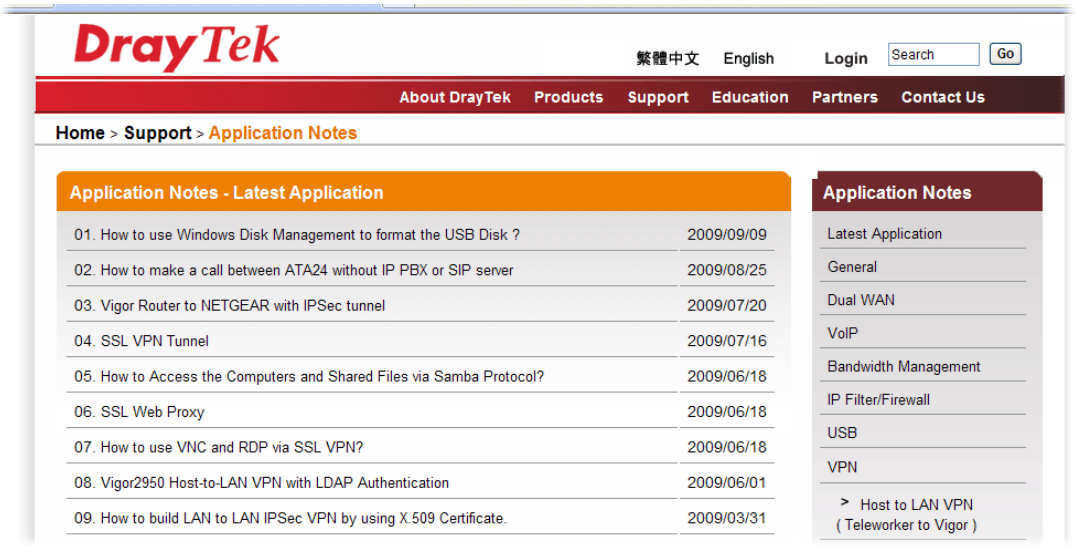
Host name	Display the name of the computer accepted the assigned IP address by this router.
IP Address	Display the IP address assigned by this router for specified PC.
MAC Address	Display the MAC address for the specified PC that DHCP assigned IP address for it.
Expire Time	Display the leased time of the specified PC.
Refresh	Click it to reload the page.

4.9 Support Area

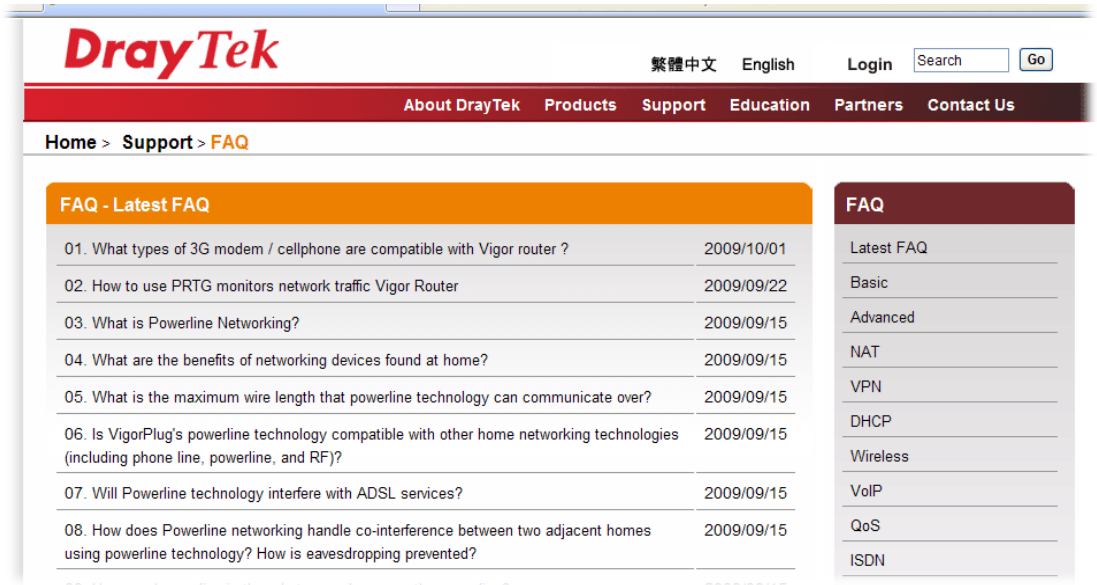
When you click the menu item under **Support Area**, you will be guided to visit www.draytek.com and open the corresponding pages directly.



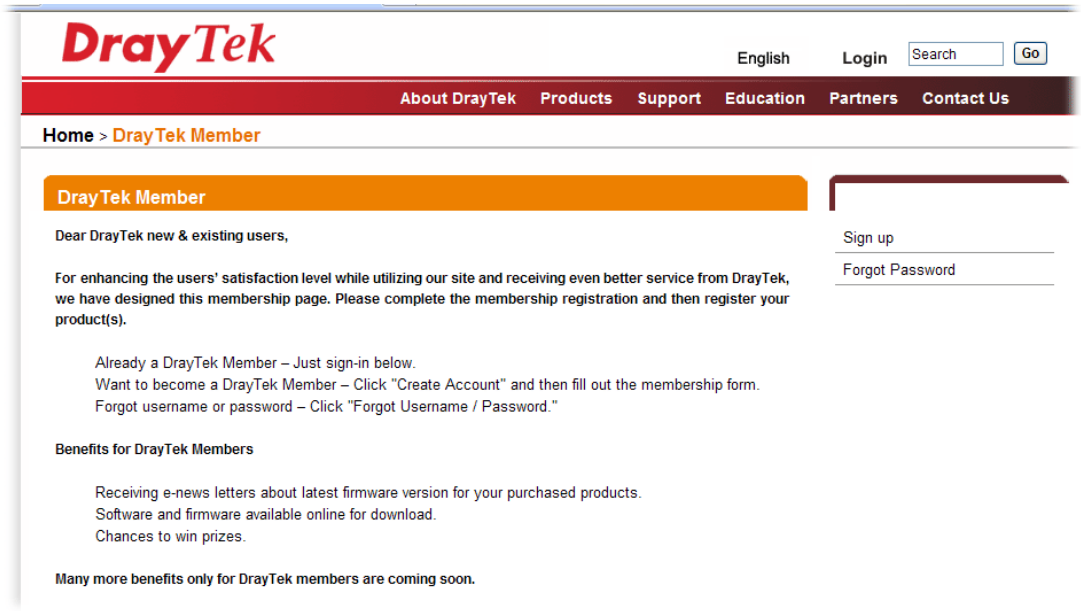
Click **Support Area>>Application Note**, the following web page will be displayed.



Click **Support Area>>FAQ**, the following web page will be displayed.



Click **Support Area>>Product Registration**, the following web page will be displayed.



This page is left blank.

5 Trouble Shooting

This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer for advanced help.

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check the power line and WLAN/LAN cable connections.
   Refer to "**1.3 Hardware Installation"** for details.
2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.

3. If not, it means that there is something wrong with the hardware status. Simply back to **"1.3 Hardware Installation"** to execute the hardware installation again. And then, try again.

5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

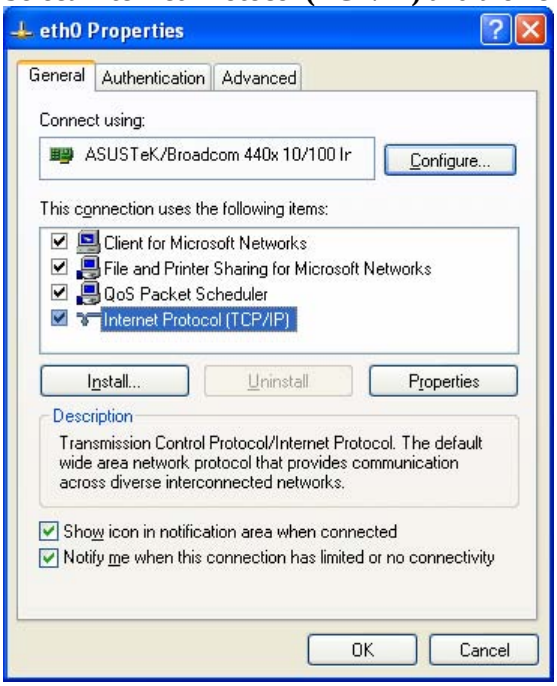
For Windows

> The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

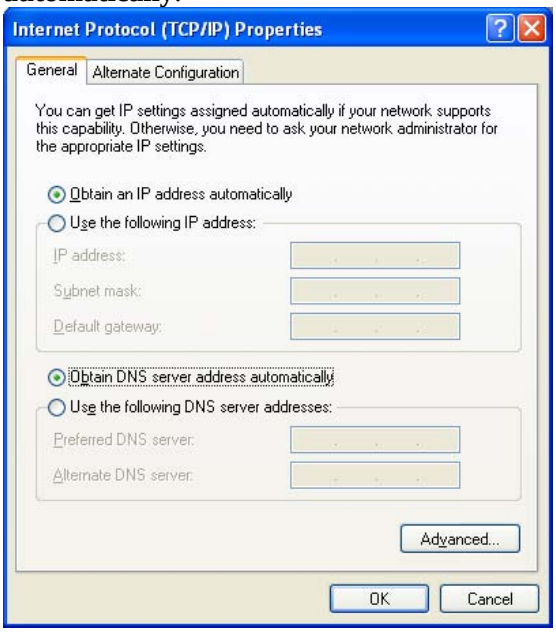
1. Go to **Control Panel** and then double-click on **Network Connections**.

2. Right-click on **Local Area Connection** and click on **Properties**.

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

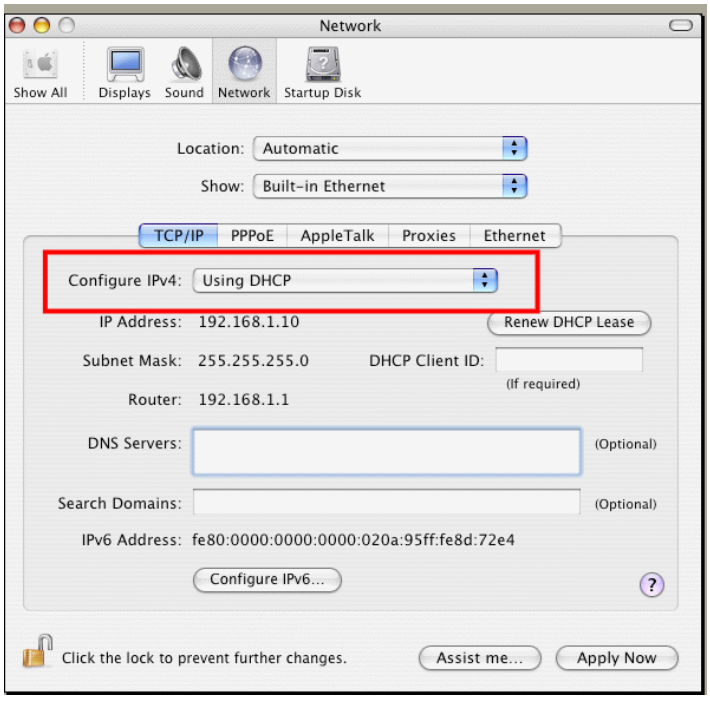


4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



For MacOs

1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Network**.
3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.



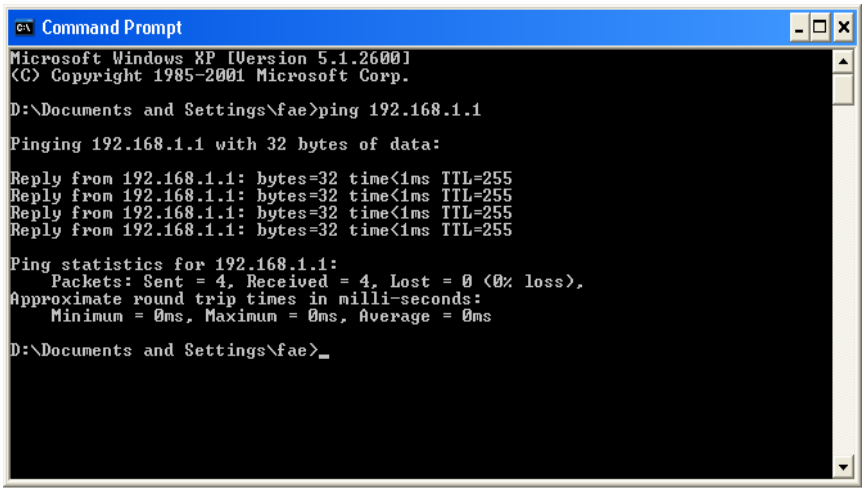
5.3 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 5.2)

Please follow the steps below to ping the router correctly.

For Windows

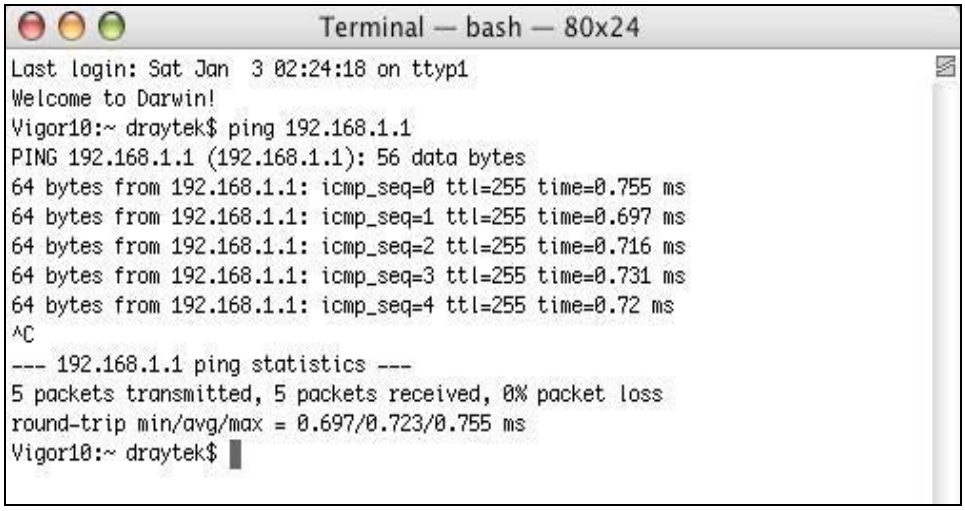
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista). The DOS command dialog will appear.



3. Type ping 192.168.1.1 and press [Enter]. If the link is **OK**, the line of **"Reply from 192.168.1.1:bytes=32 time<1ms TTL=255"** will appear.
4. If the line does not appear, please check the IP address setting of your computer.

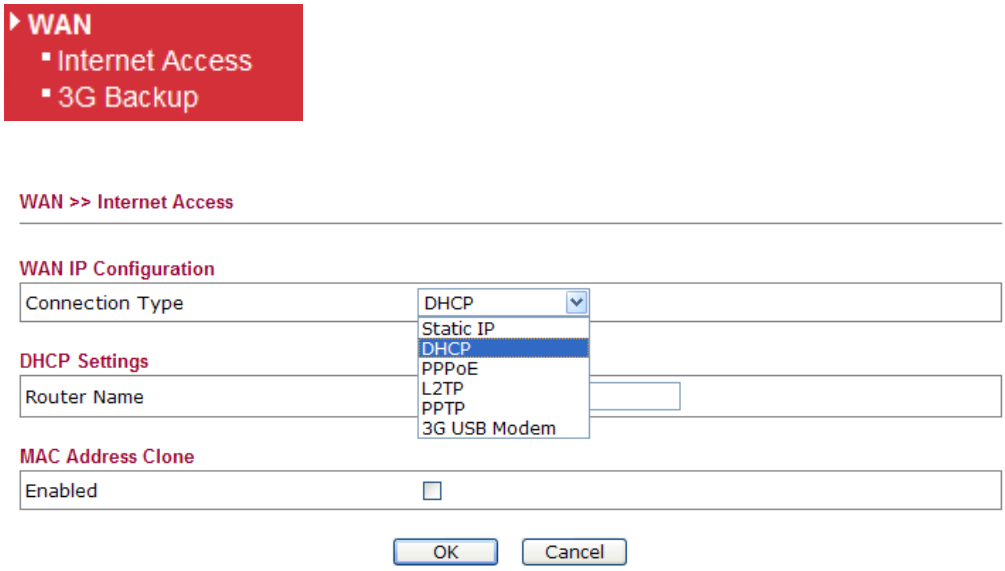
For MacOs (Terminal)

1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. If the link is **OK**, the line of **"64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**" will appear.



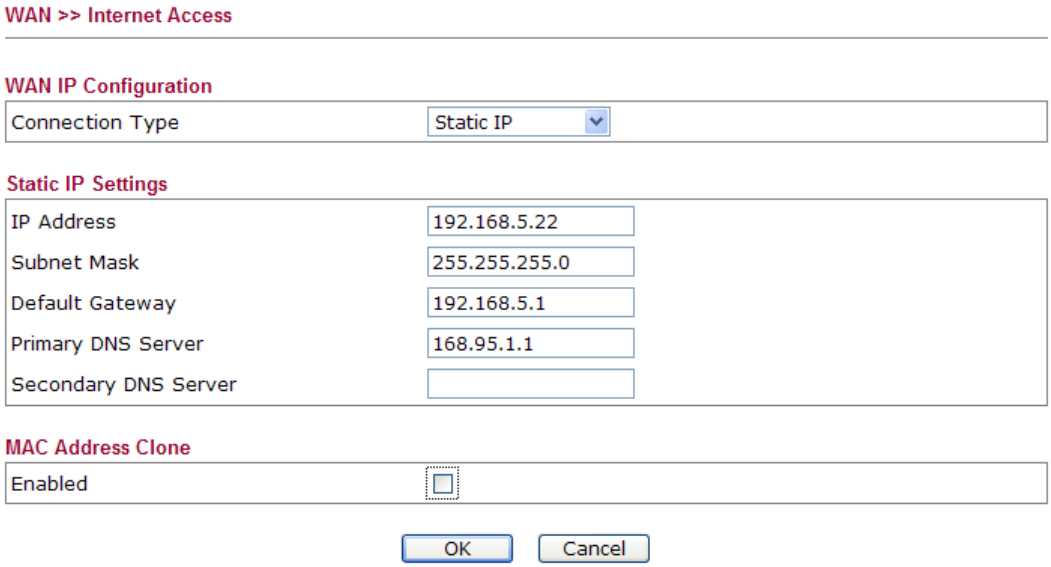
5.4 Checking If the ISP Settings are OK or Not

Open **WAN>>Internet Access** page and then check whether the ISP settings are set correctly. Use the Connection Type drop down list to choose Static IP/DHCP/PPPoE/PPTP/L2TP for reviewing the settings that you configured previously.



For Static Users

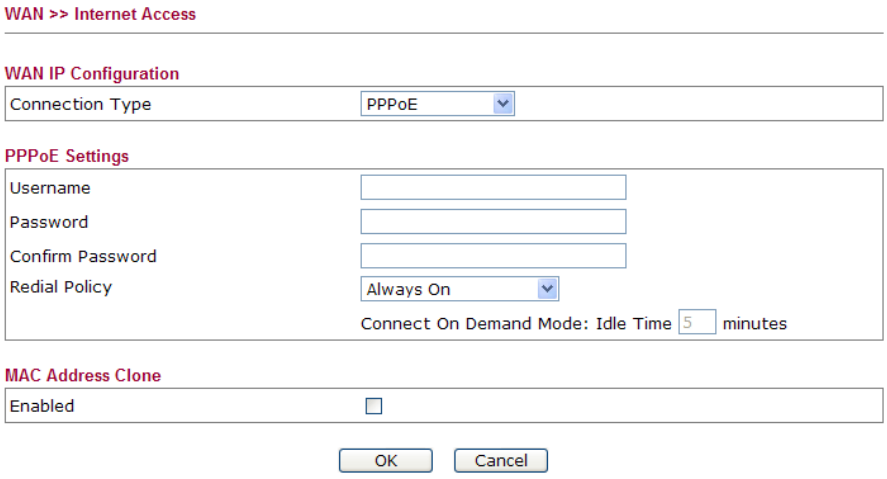
1. Choose **Static IP** as the connection type.



2. Check if **IP Address, IP Mask** and **IP Router** are set correctly (must identify with the values from your ISP).

For PPPoE Users

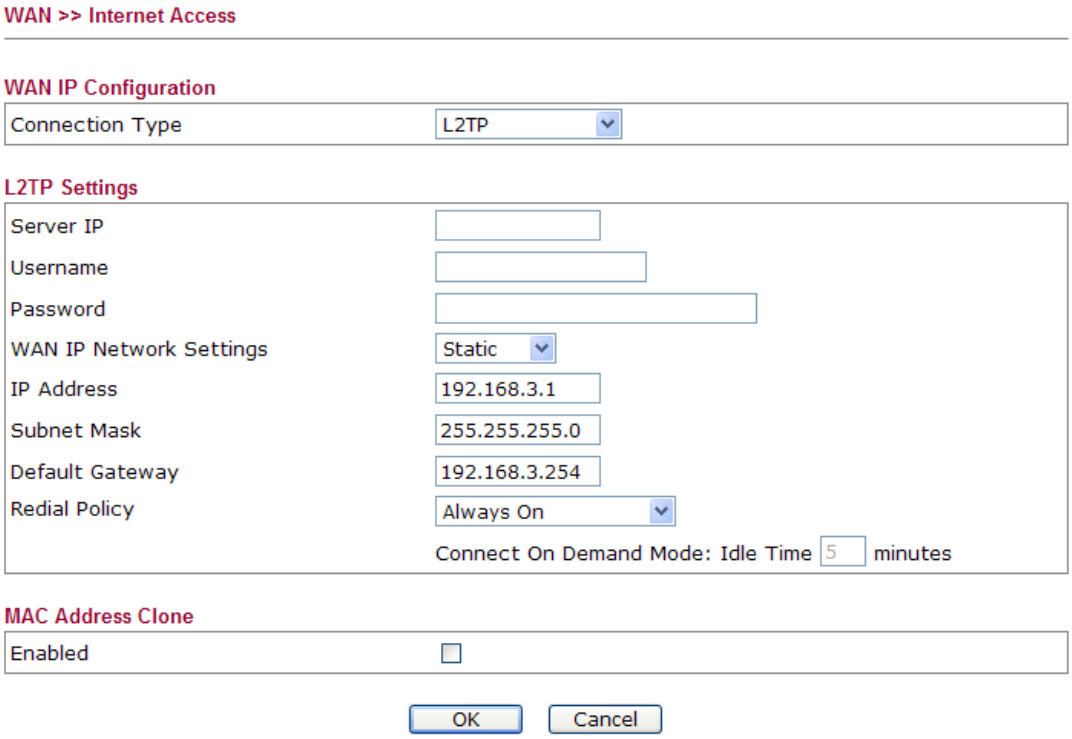
1. Choose **PPPoE** as the connection type.



2. Check if **Username** and **Password** are set correctly (must identify with the values from your ISP).

For PPTP/L2TP Users

1. Choose **PPTP/L2TP** as the connection type.



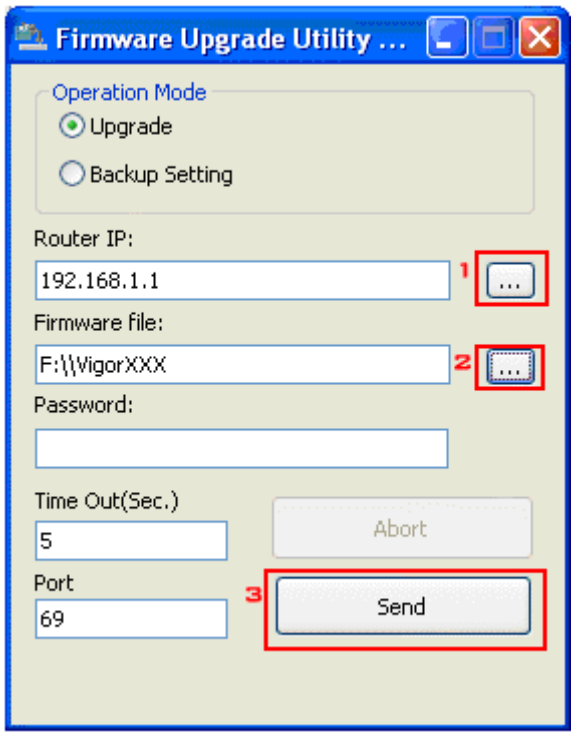
2. Check if **Username**, **Password, IP address, Subnet Mask** are entered with correct values that you **get from** your **ISP**.

5.5 Forcing Vigor Router into TFTP Mode for Performing the Firmware Upgrade

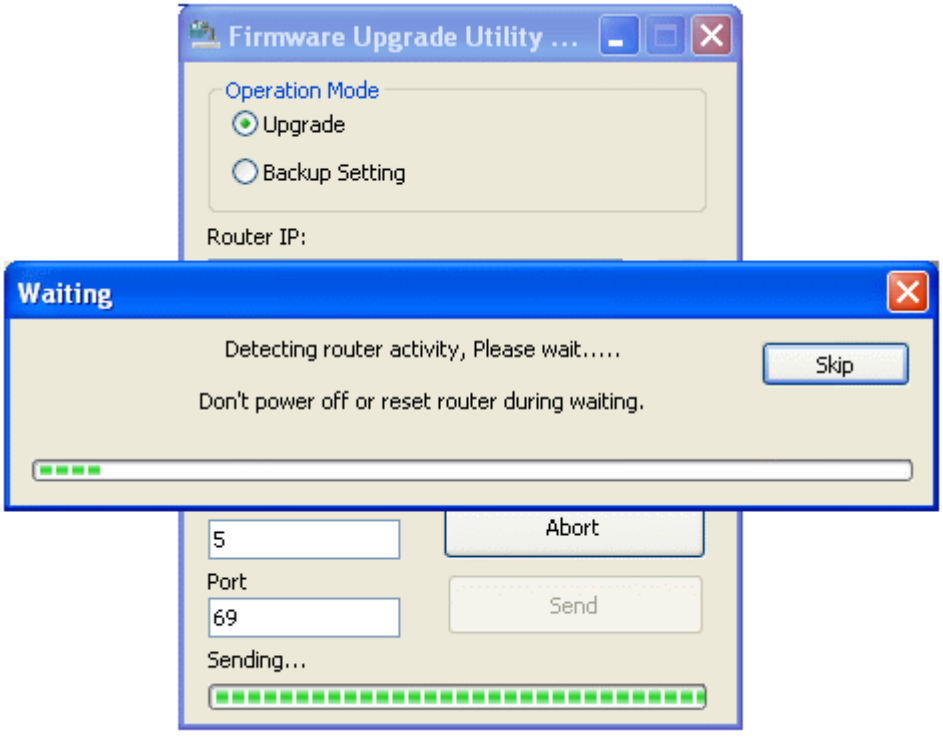
1. Press and hold the **Factory Reset** button. The system will power off and power on the Vigor Router.
2. Release the **Factory Reset** button when the ACT LED and its neighbor LED blink simultaneously.
3. Change your PC IP address to 192.168.1.10.
4. Open **Firmware Upgrade Utility** and key in Router IP 192.168.1.1 manually.
5. Install **Router Tools** on one computer that connects to Vigor Router's LAN port.
6. Make sure the computer can ping Vigor's LAN IP. (Default IP is 192.168.1.1)
7. Run **Router Tools >> Firmware Upgrade Utility**.
8. Input Vigor's LAN IP manually or use the **. . .**button to select.
9. Indicate the firmware location.

> **Note:** There are two firmware types. The *.rst* firmware format will make the configurations be back to default settings after upgrading firmware. The *.all* firmware format will remain the former configurations after upgrading firmware.

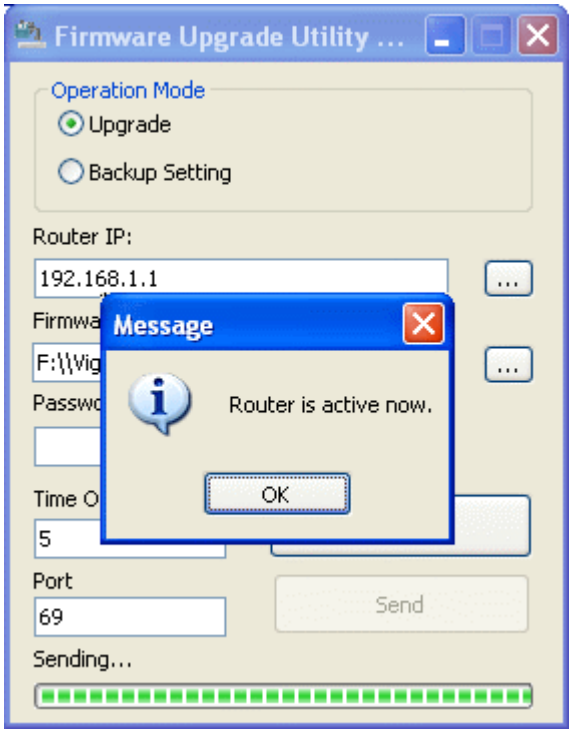
10. Input the Password if you have set one, then click **Send**.



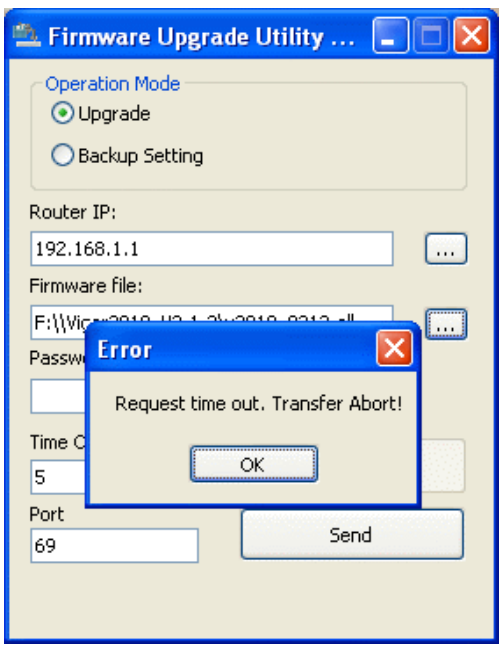
11. There is a bar showing the upgrading process.

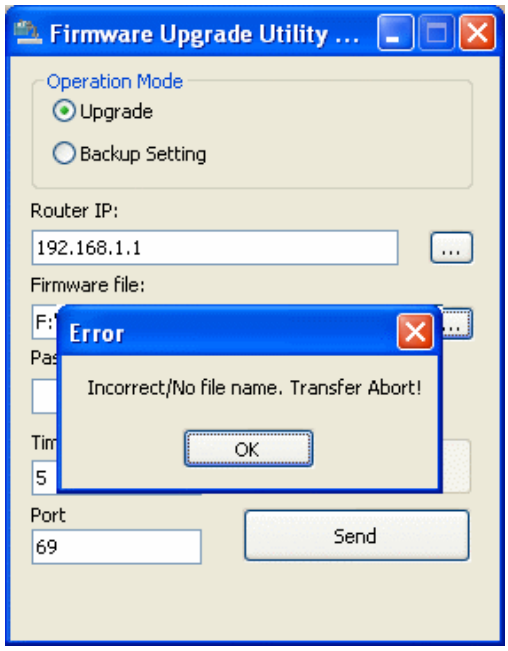


12. When the firmware upgrade is successful, the following window will pop up.



If the message of **Request Timeout. Transfer Abort !** appears, please check if the connection between the computer and the Vigor is active or not. And, if the message of **Incorrect/No file name. Transfer Abort !** appears, please check if the firmware you download is correct for your Vigor router.





Note: Please turn off the Firewall protection while upgrading the firmware with Windows Vista. The Firewall function can be turned off via **Control Panel** >> **Security Center** >> **Firewall**.

5.6 Backing to Factory Default Setting If Necessary

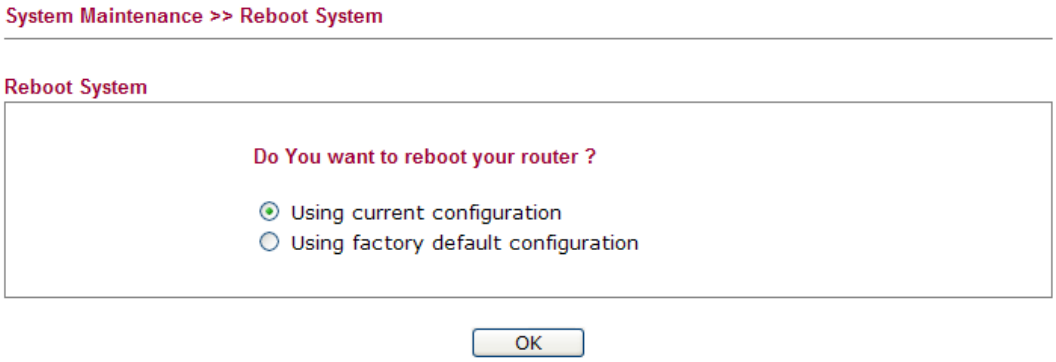
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

Warning: After pressing **factory default setting**, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing.

Software Reset

You can reset the router to factory default via Web page.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **OK**. After few seconds, the router will return all the settings to the factory settings.



Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the router will restart with the default configuration.

After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

5.7 Contacting Your Dealer

If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@draytek.com.