DrayTek

VigorFly 210

WiFi Router

Your reliable networking solutions partner

User's Guide

V1.1

VigorFly 210
Wi-Fi Router
User's Guide

Version: 1.1

Firmware Version :V1.3.5

Date: July 18, 2014

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 210 Series Router

DrayTek Corp. declares that VigorFly 210 is in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EC.

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.

The antenna/transmitter should be kept at least 20 cm away from human body.

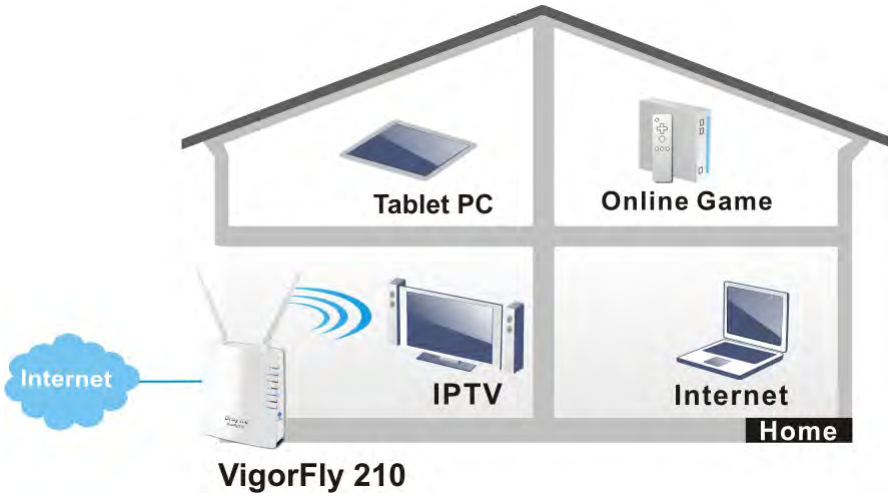
Please visit http://www.draytek.com/user/SupportDLRTTECE.php

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 Introduction

VigorFly 210 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/WiMAX/LTE USB** modem to USB port on VigorFly 210. The sharing **3.5G/WiMAX/LTE** 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

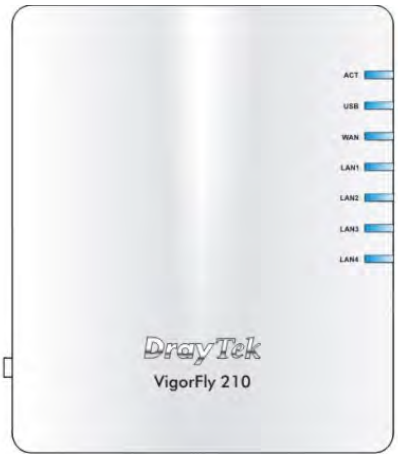
Several main buttons appeared on the web pages are defined as the following:

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

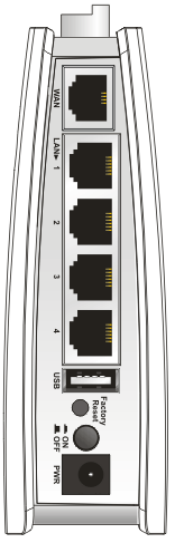
Note: For the other buttons shown on the web pages, please refer to the following chapters for detailed explanation.

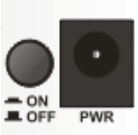
1.2 LED Indicators and Connectors

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 (Blue LED) on WLAN button	On	Wireless access point is ready.
	Off	Wireless access point is not ready.
	Blinking (Blue)	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.

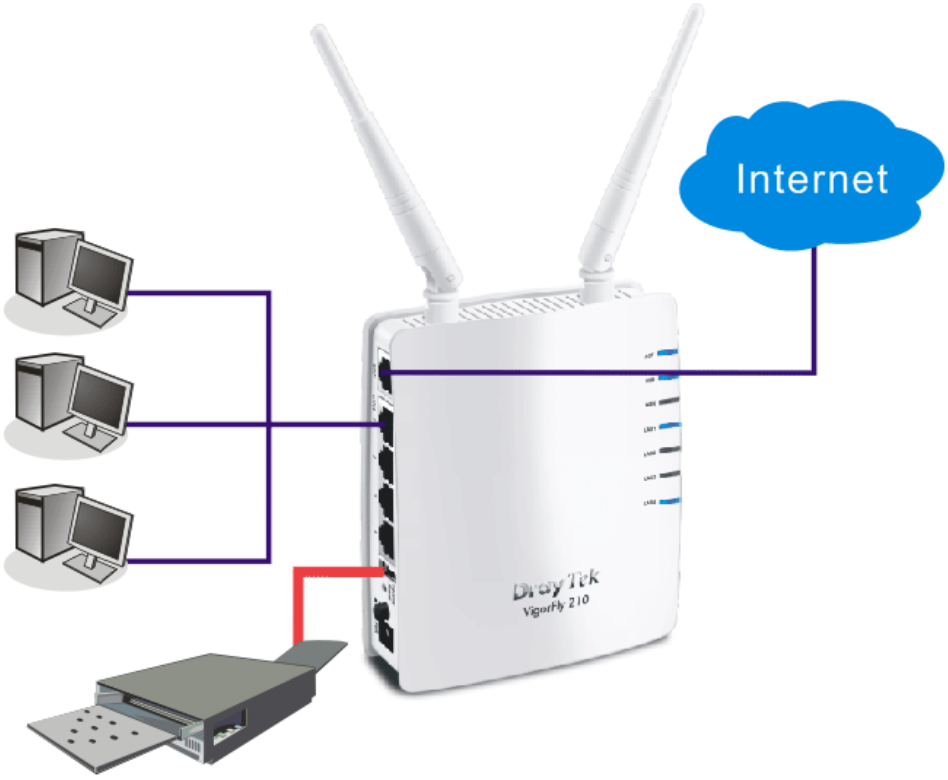
1. Connect this device to a modem with an Ethernet cable.
2. Connect the LAN port to your computer with a RJ-45 cable.
3. Connect one end of the power adapter to the Power port of this device. Connect the other end to the wall outlet of electricity.
4. Power on the router.
5. Check the **ACT, WAN** and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

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

Note: To get a better WiMAX signal, please use a USB extension cable to connect USB WiMAX dongle to Vigor router for increasing the distance between Vigor router and the dongle.

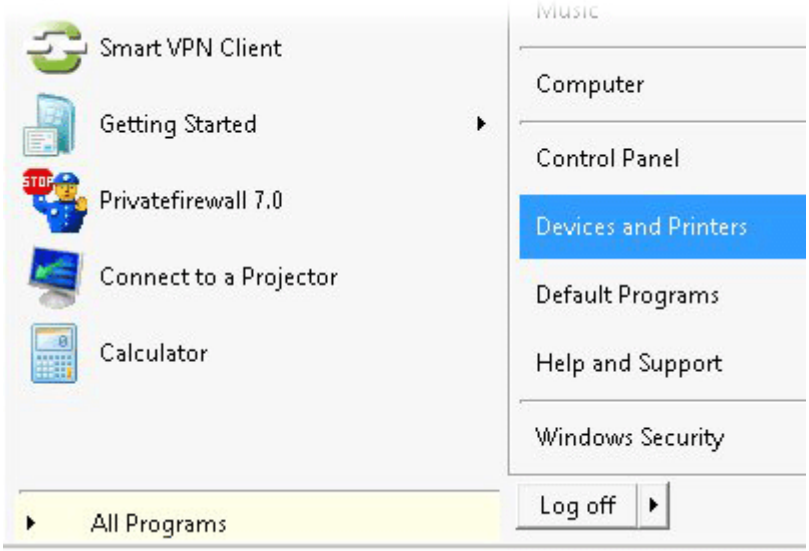
1.4 Printer Installation

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 7. For other Windows system, please visit **www.draytek.com**.

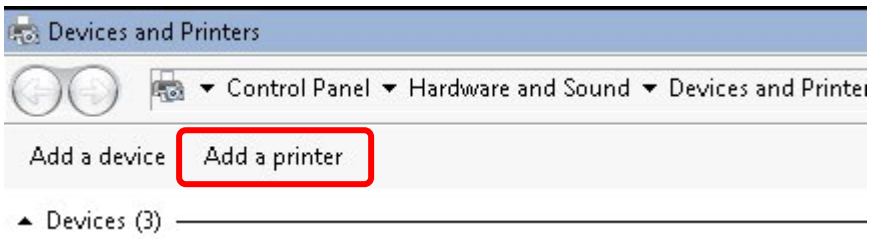


Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

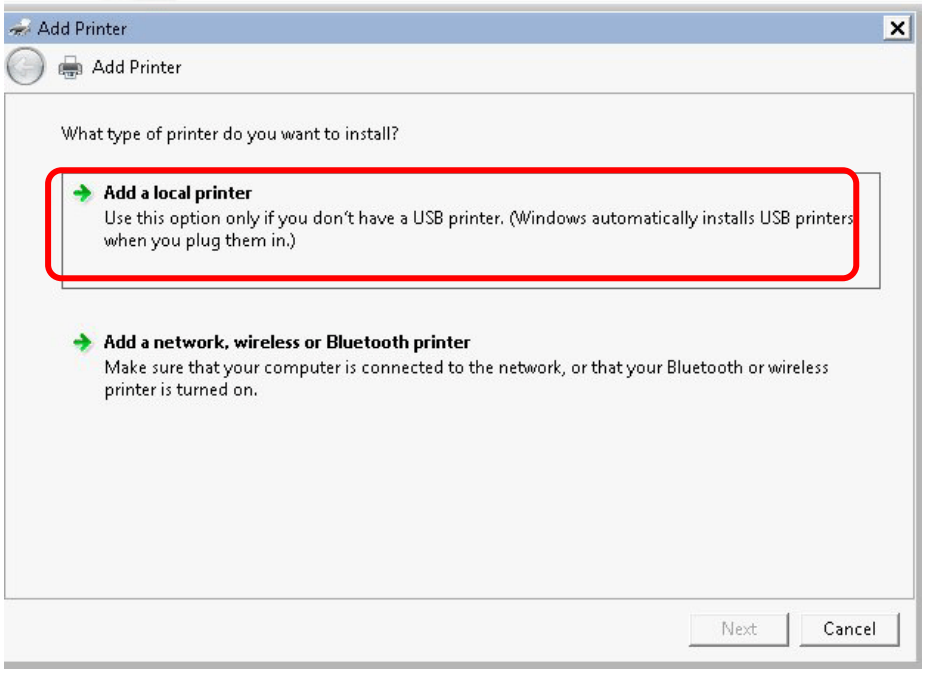
1. Connect the printer with the router through USB/parallel port.
2. Open **All Programs>>Getting Started>>Devices and Printers**.



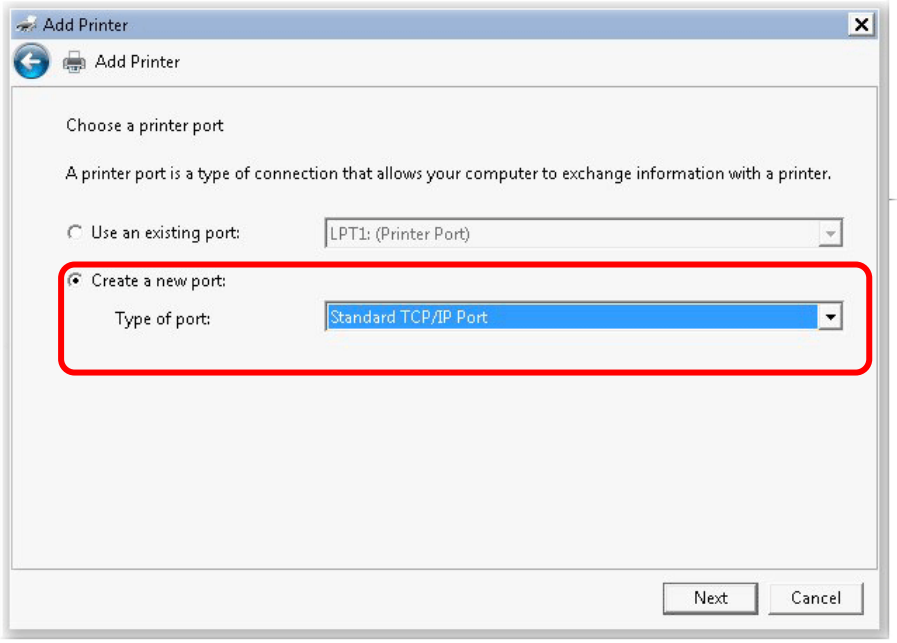
3. Click **Add a printer**.



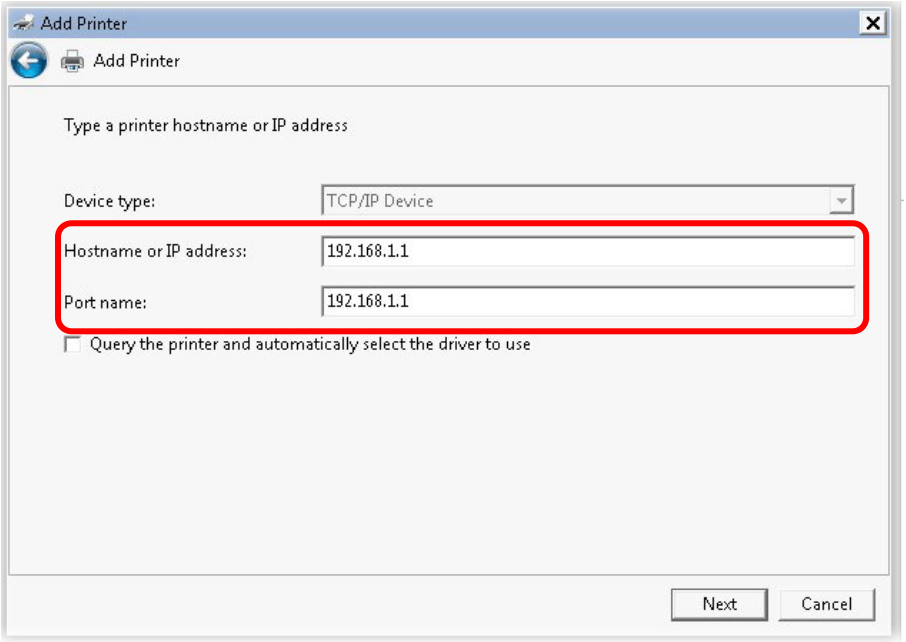
4. A dialog will appear. Click **Add a local printer** and click **Next**.



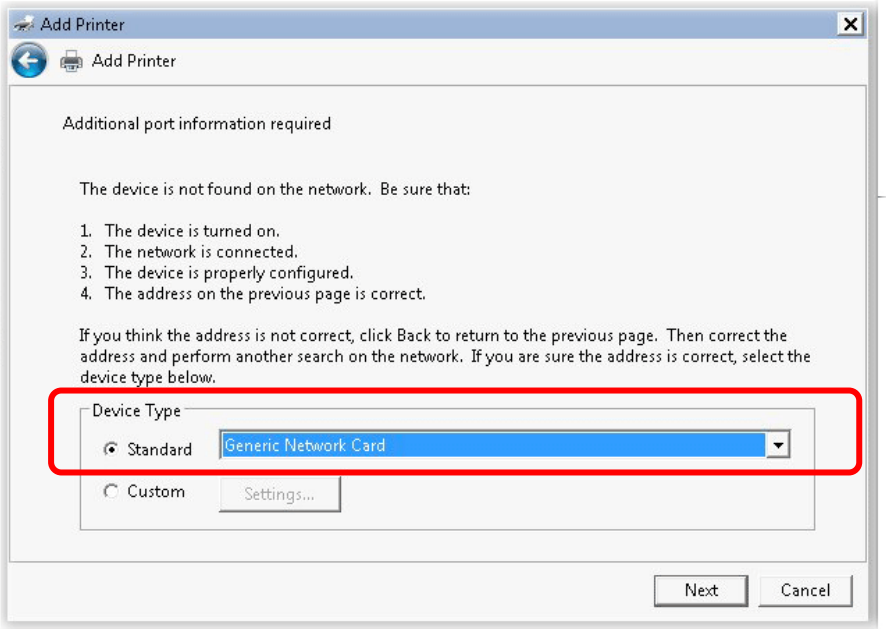
5. In this dialog, choose **Create a new port.** In the field of **Type of port,** use the drop down list to select **Standard TCP/IP Port**. Then, click **Next**.



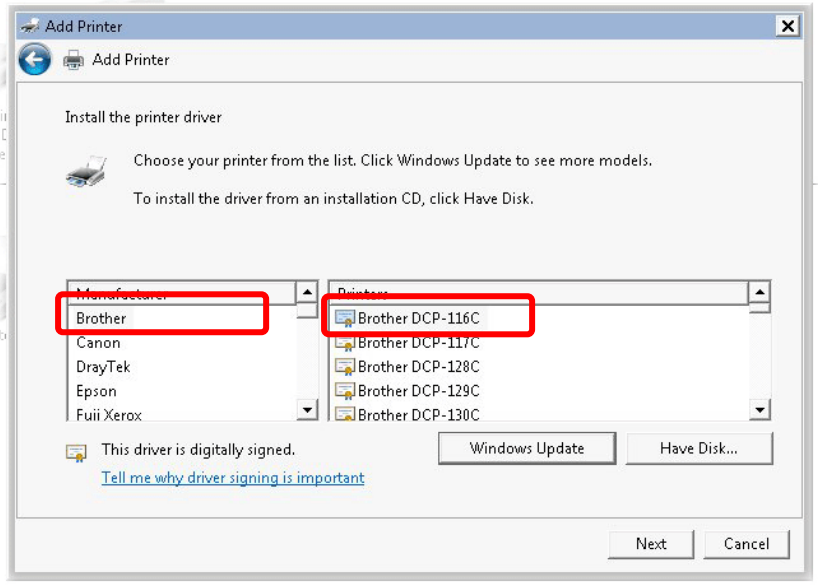
6. In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Hostname or IP Address** and type **192.168.1.1** as the **Port name**. Then, click **Next**.



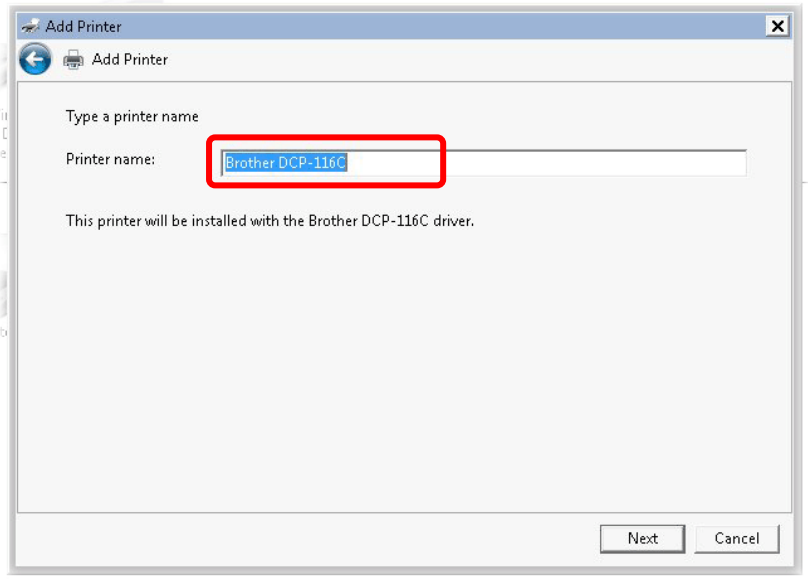
7. Click **Standard** and choose **Generic Network Card**.



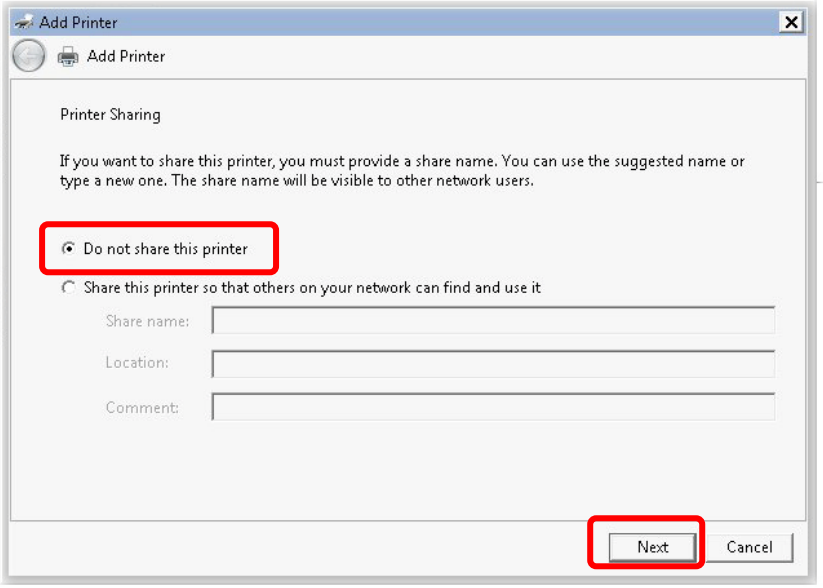
8. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



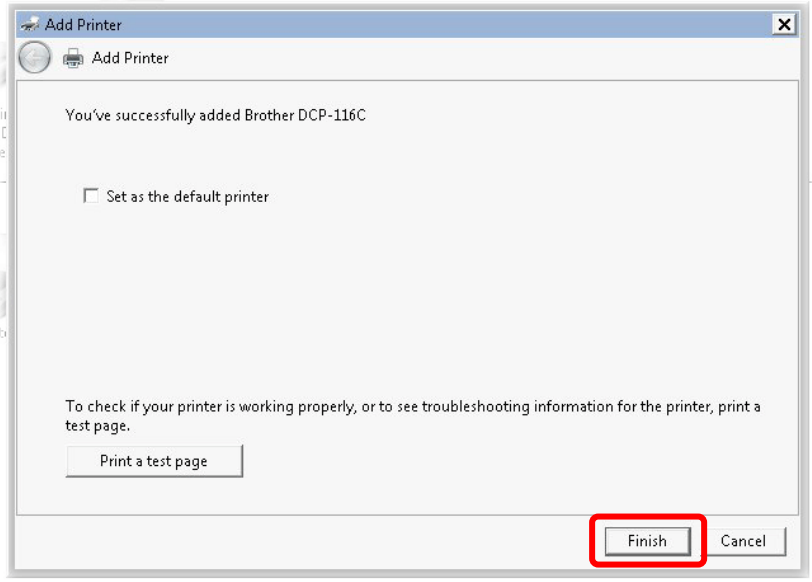
9. Type a name for the chosen printer. Click **Next.**



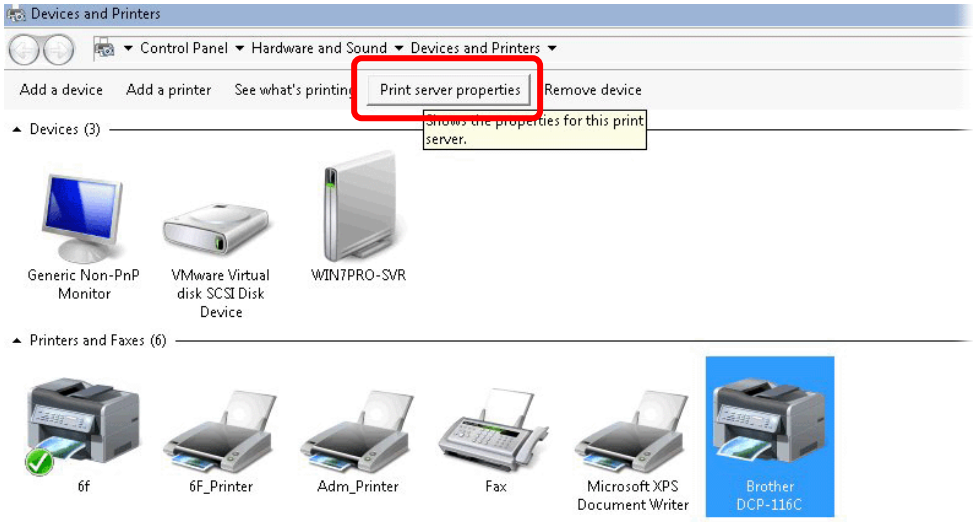
10. Choose **Do not share this printe**r and click **Next**.



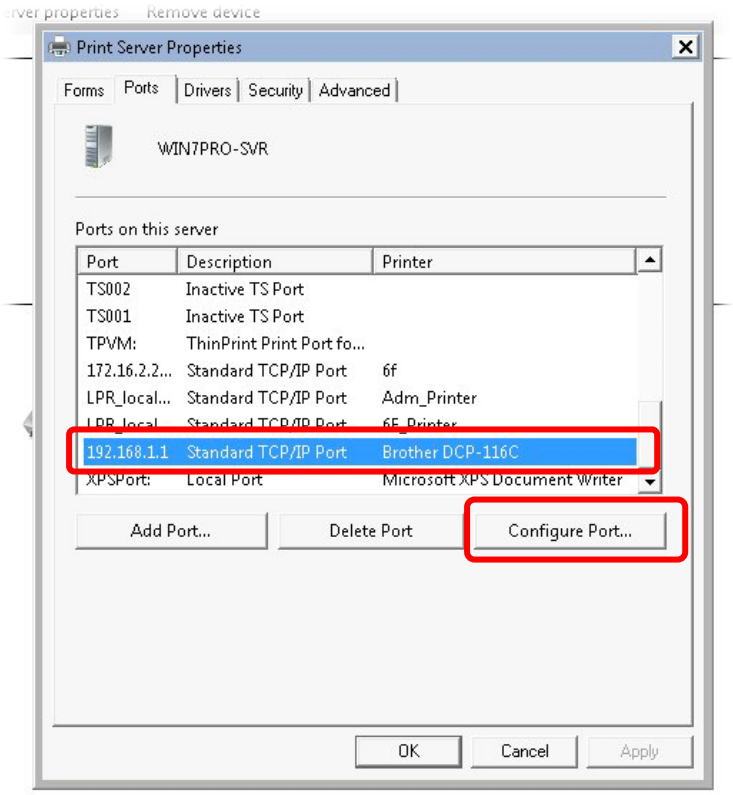
11. Then, in the following dialog, click **Finish**.



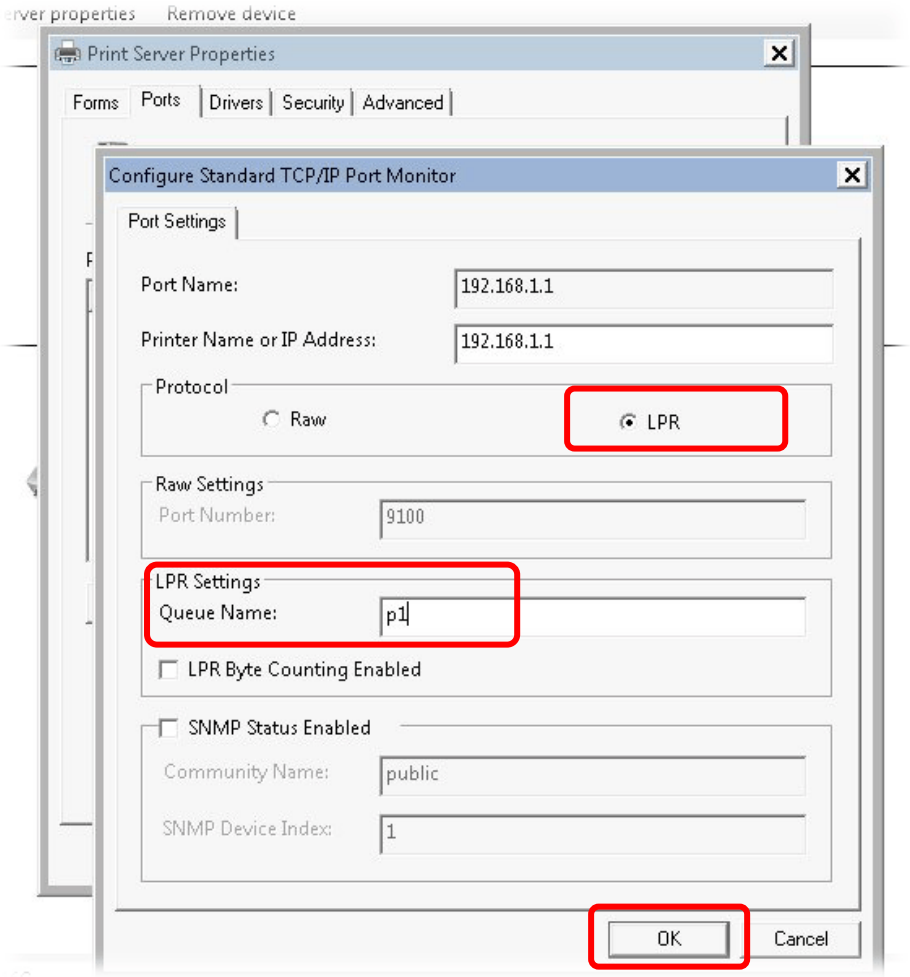
12. The new printer has been added and displayed under **Printers and Faxes**. Click the new printer icon and click **Printer server properties**.



13. Edit the property of the new printer you have added by clicking **Configure Port**.



14. Select "**LPR**" on Protocol, type **p1** (number 1) as **Queue Name**. Then click **OK**.



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/Application Notes**; find out the link of **Printer Server** and click it; then click the **What types of printers are compatible with Vigor router?** link.

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 Basic Settings

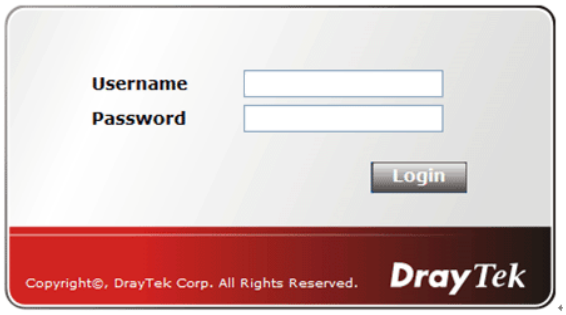
For using the router properly, it is necessary for you to change the password of web configuration for security and adjust primary basic settings.

2.1 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.

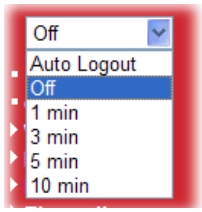
2. Open a web browser on your PC and type **http://192.168.1.1.** The following window will be open to ask for username and password.



3. Type “admin/admin” on Username/Password and click **Login** for web 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.

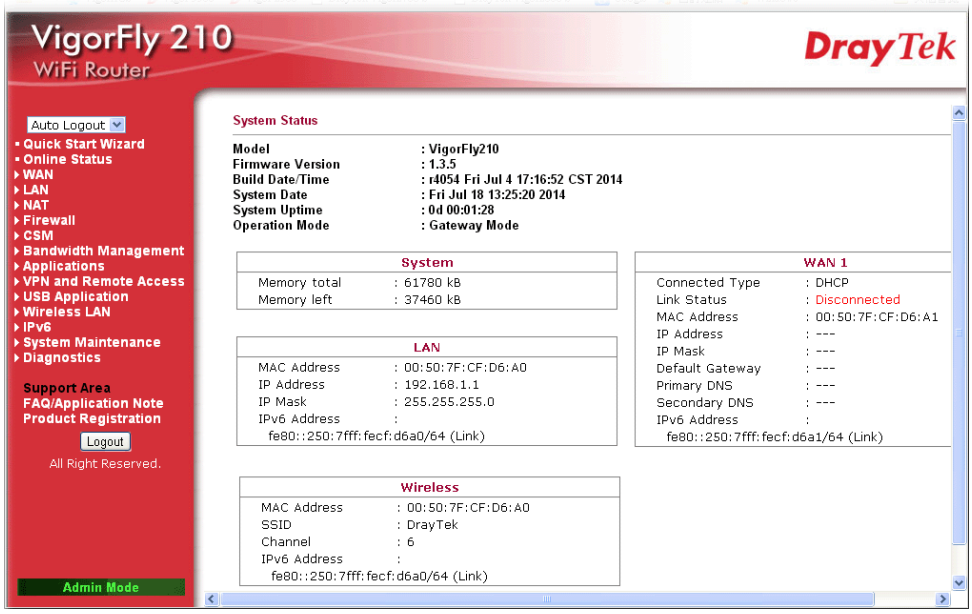


2.2 Changing Password

Before configuring the web pages, please change the password for the original security of the router.

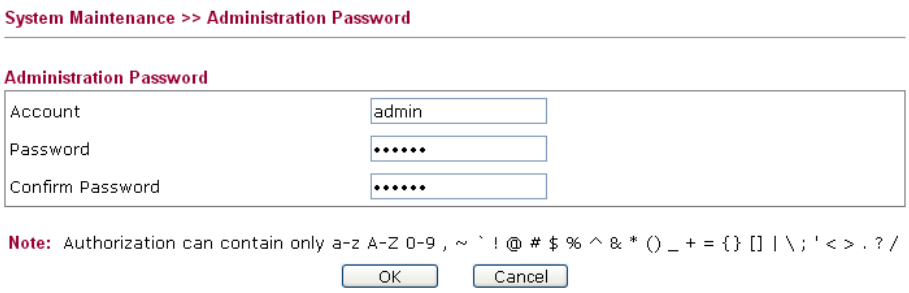
1. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for username and password.

2. Please type "admin/admin" on Username/Password for admin mode and click **Login**.



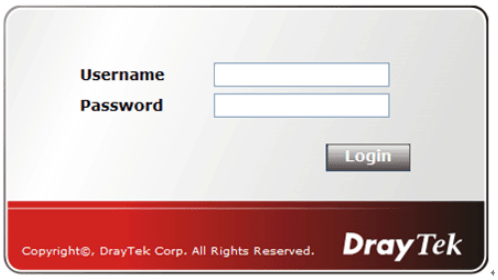
Note: The home page will change slightly in accordance with the type of the router you have.

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.

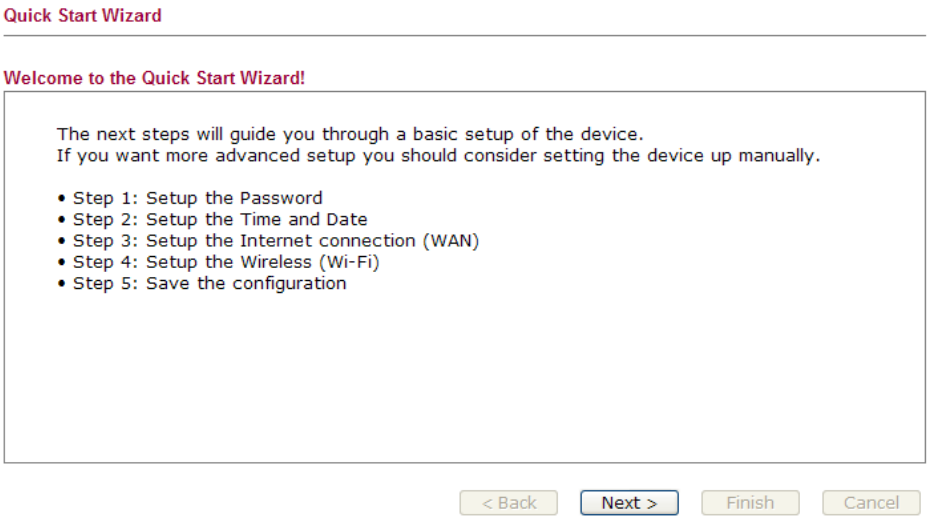
5. Now, the password has been changed. Next time, use the new username / password to access the web user interface of this router.



2.3 Quick Start Wizard

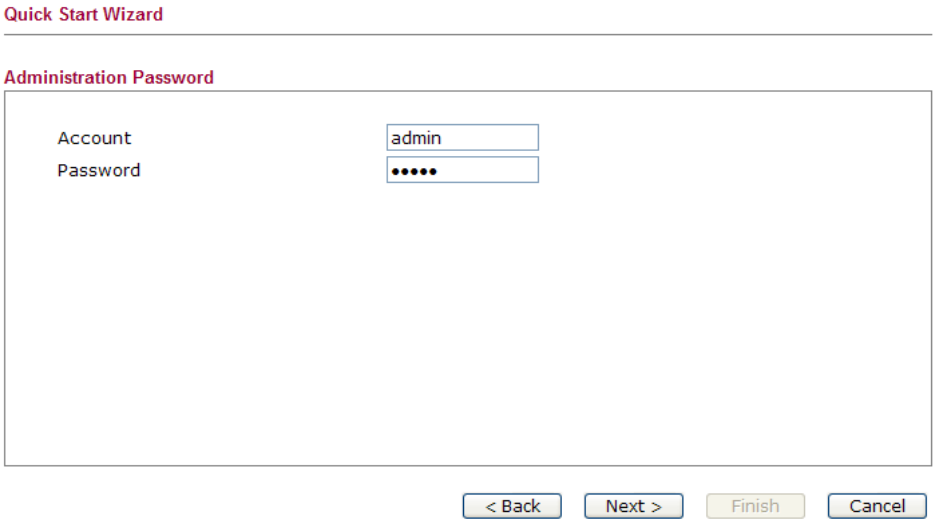
Notice: Quick Start Wizard for user mode operation is the same as for admin mode operation.

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**.



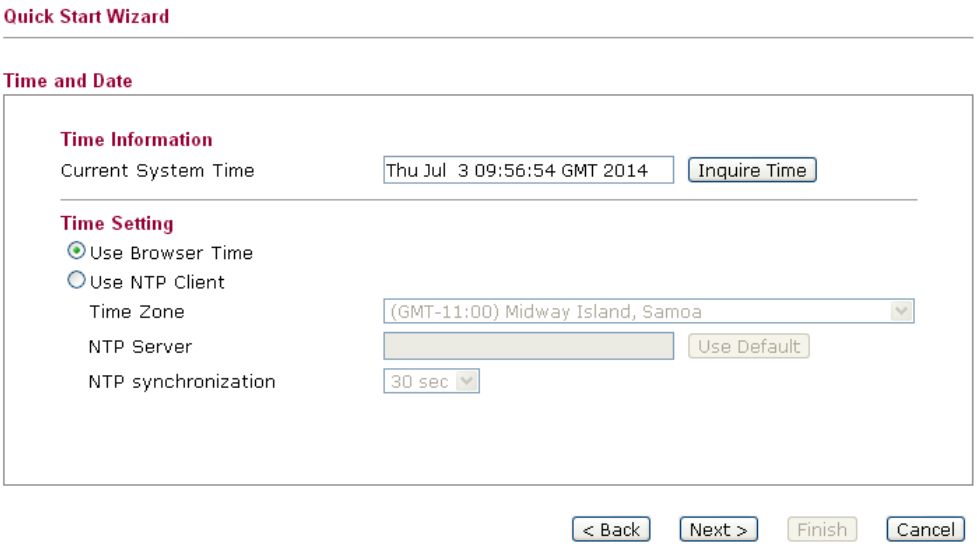
2.3.1 Setting up the Password

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



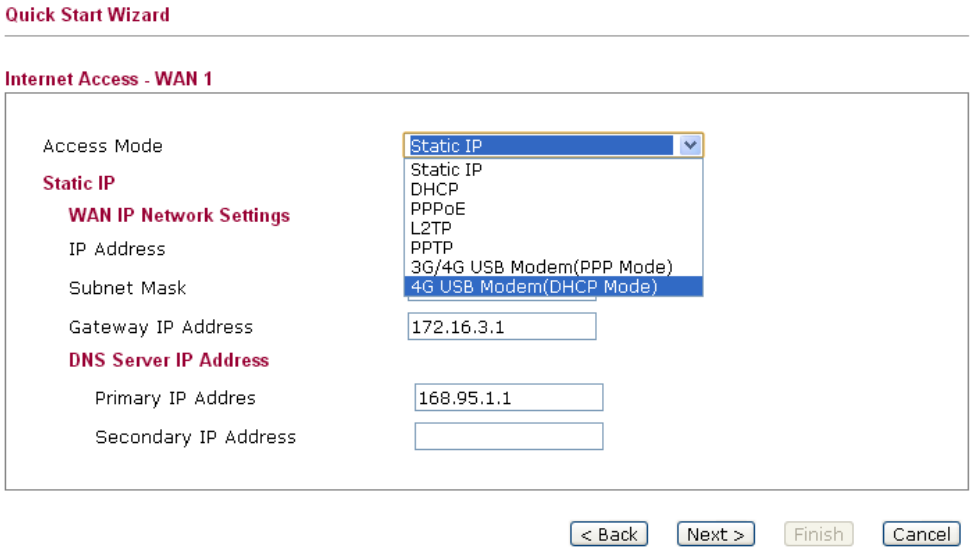
2.3.2 Setting up the Time and Date

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.



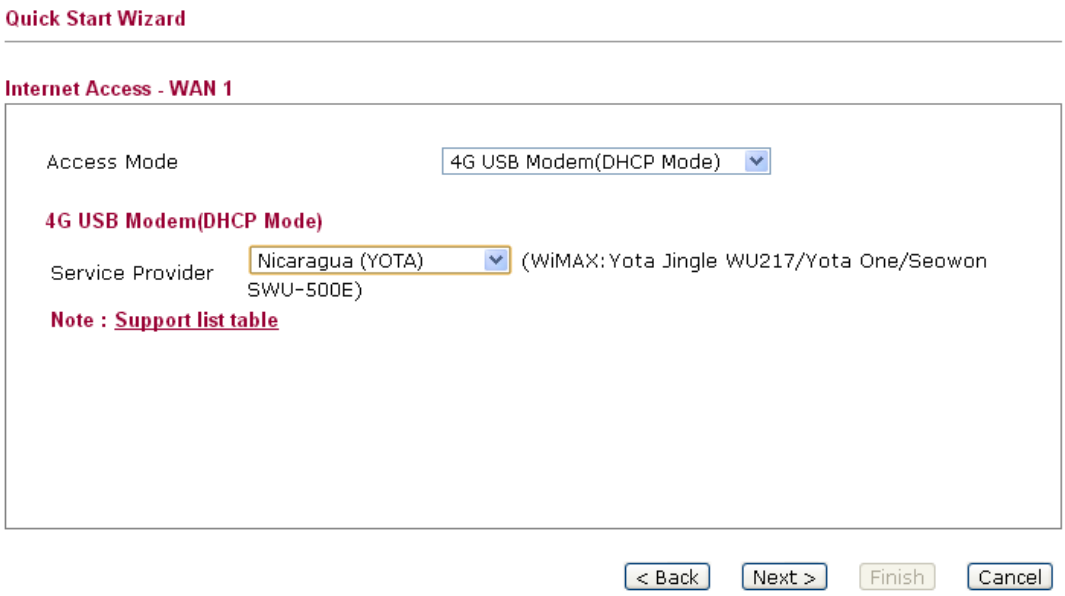
2.3.3 Setting up the Internet Connection for WAN1

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



4G USB Modem (DHCP Mode)

If you want to access Internet with 4G USB Modem, choose 4G USB Modem as the Access Mode. Corresponding settings will be displayed for you to configure.



Available parameters are listed below:

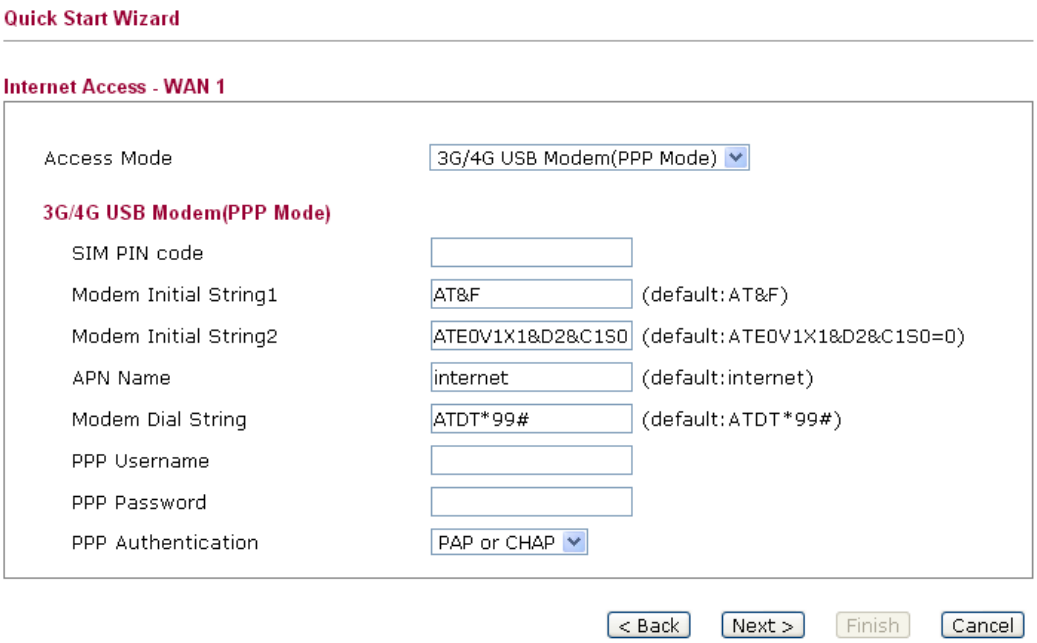
Item	Description
Service Provider	Choose the local service provider which can serve network service according to the nature of USB Modem (LTE/WiMAX) installed. For example, you live in Taiwan and have a WiMAX modem inserted onto VigorFly 210. You can choose Taiwan (Global Mobile) to configure necessary settings and then surf the Internet easily.  The available settings will be different based on the service provider specified. In this case, Taiwan (Global Mobile) is chosen as an example.

Item	Description
Username	Type the user name acquired from the service provider.
Password	Type the password acquired from the service provider.
Cipher Suite	**Cipher Suite –** There are two encryption methods offered for you to choose as cipher suite. Keep the default setting will be better. Such item is required for WiMAX USB Modem. DHE_RSA_AES_256_SHA RSA_RC4_128_MD5 RSA_AES_256_SHA DHE_RSA_AES_256_SHA

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

3G/4G USB Modem (PPP Mode)

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.



Available parameters are listed below:

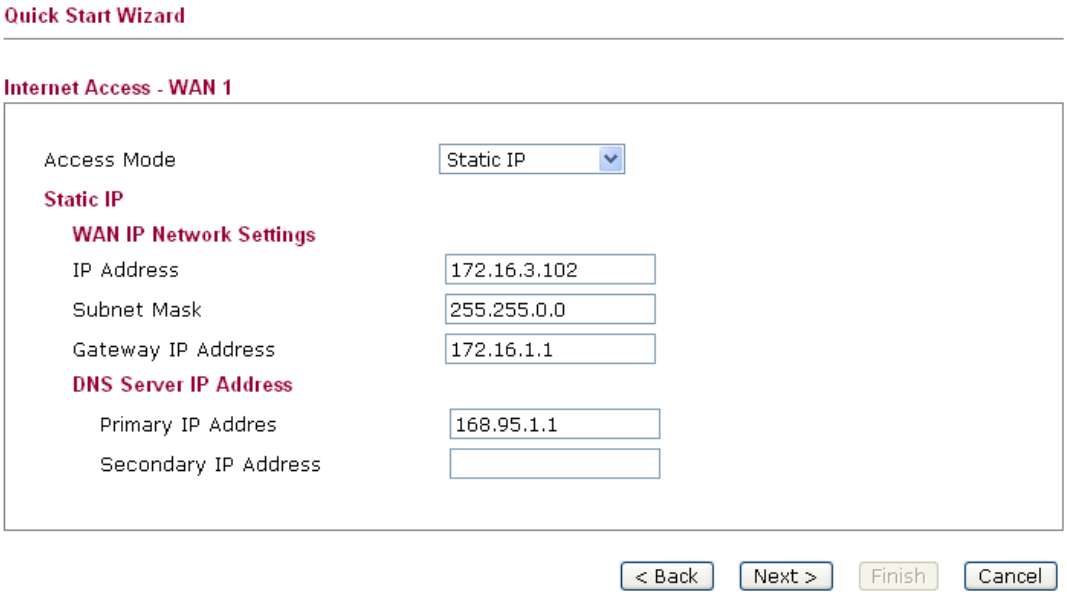
Item	Description
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet.
Modem Initial String1/2	Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.
APN Name	APN means Access Point Name which is provided 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

Item	Description
	your ISP.
PPP Username	Type the PPP username (optional).
PPP Password	Type the PPP password (optional).
PPP Authentication	Select **PAP only** or **PAP or CHAP** for PPP.

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

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.



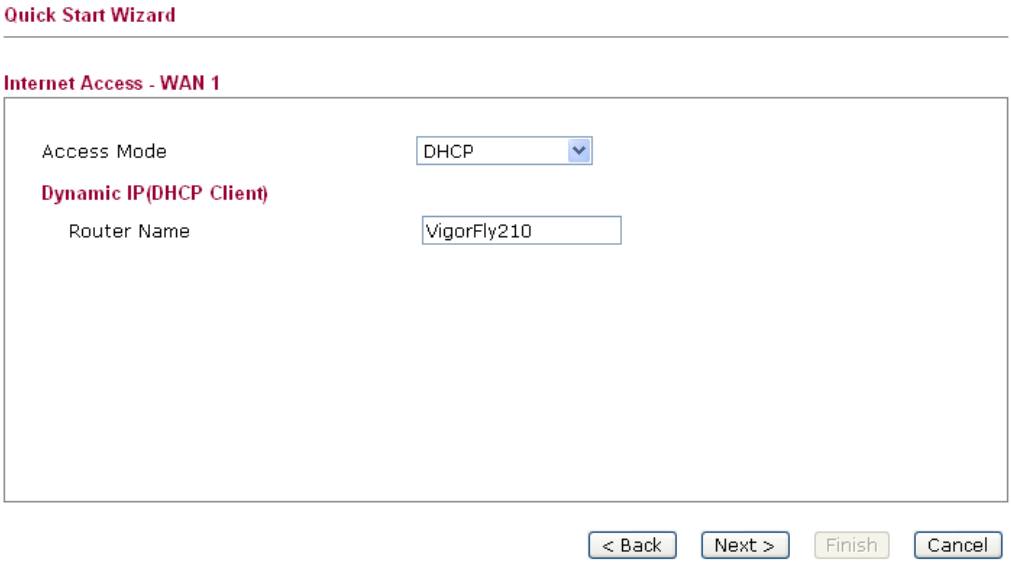
Available parameters are listed below:

Item	Description
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.

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.



Available parameters are listed below:

Item	Description
Router Name	Default setting is VigorFly210.

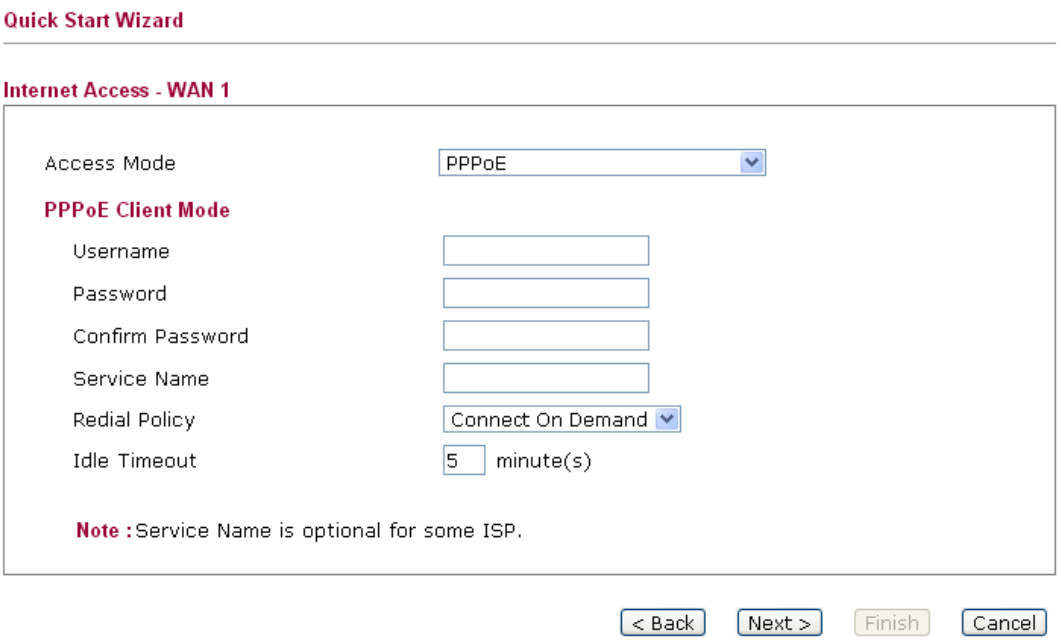
After finishing the settings here, please click **Next.**

PPPoE

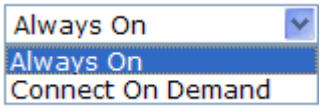
PPPoE stands for **Point-to-Point Protocol over Ethernet**. It relies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet can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



Available parameters are listed below:

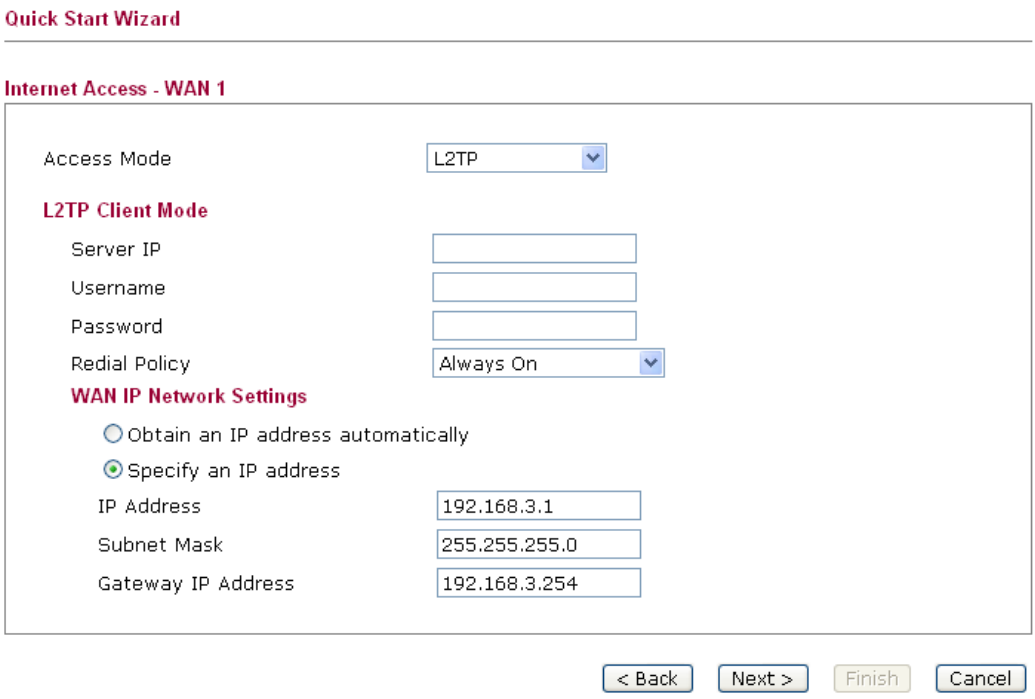
Item	Description
User Name	Assign a specific valid user name provided by the ISP.
Password	Assign a valid password provided by the ISP.
Confirmed Password	Type the password again for confirmation.
Service Name	Type the description of the specific network service.
Redial Policy	If you want to connect 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.

Item	Description
	Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action. The unit is seconds.

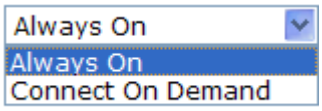
After finishing the settings here, please click **Next.**

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.



Available parameters are listed below:

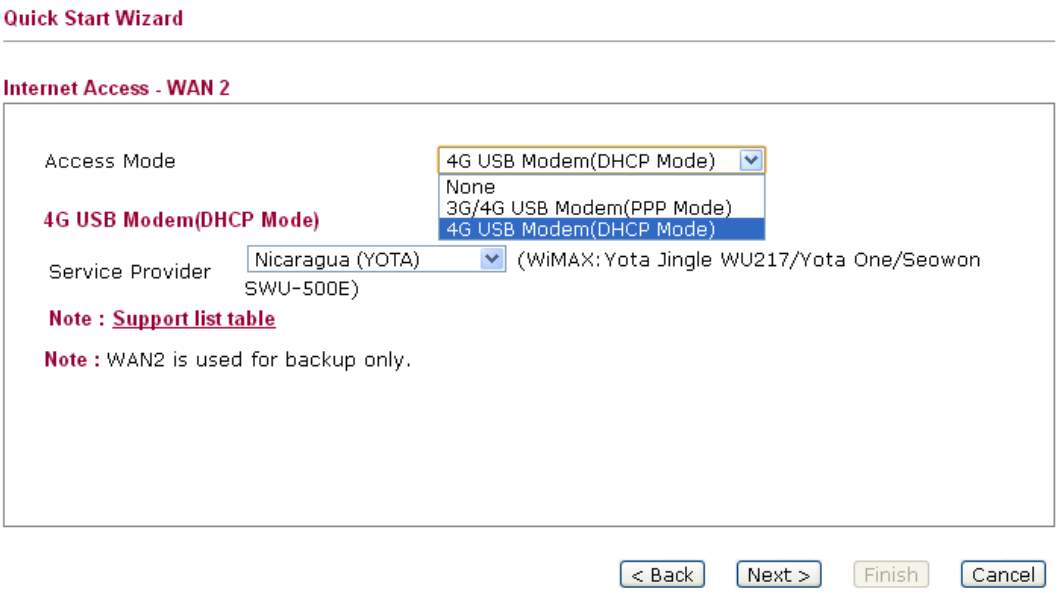
Item	Description
L2TP/PPTP Server IP	Specify the IP address of the PPTP/L2TP server.
Username	Assign a specific valid user name provided by the ISP.
Password	Assign a valid password provided by the ISP.
Redial Policy	If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, 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 Timeout -** Set the timeout for breaking down the Internet after passing through the time without any action.

Item	Description
	The unit is seconds.
WAN IP Network Settings	You can choose **Obtain an IP address automatically** or **Specify an IP address** 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**.

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

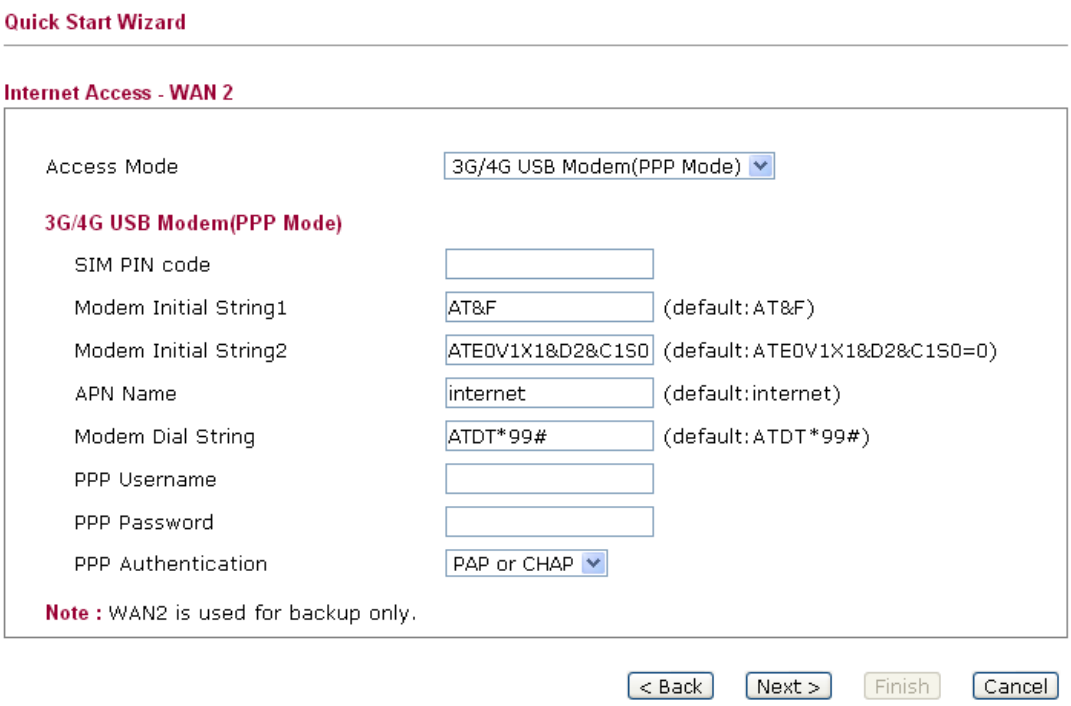
2.3.4 Setting up the Internet Connection for WAN2

WAN 2 is only used for **backup** WAN1 interface. You will get different web settings according to the service provider specified.



3G/4G USB Modem (PPP Mode)

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.



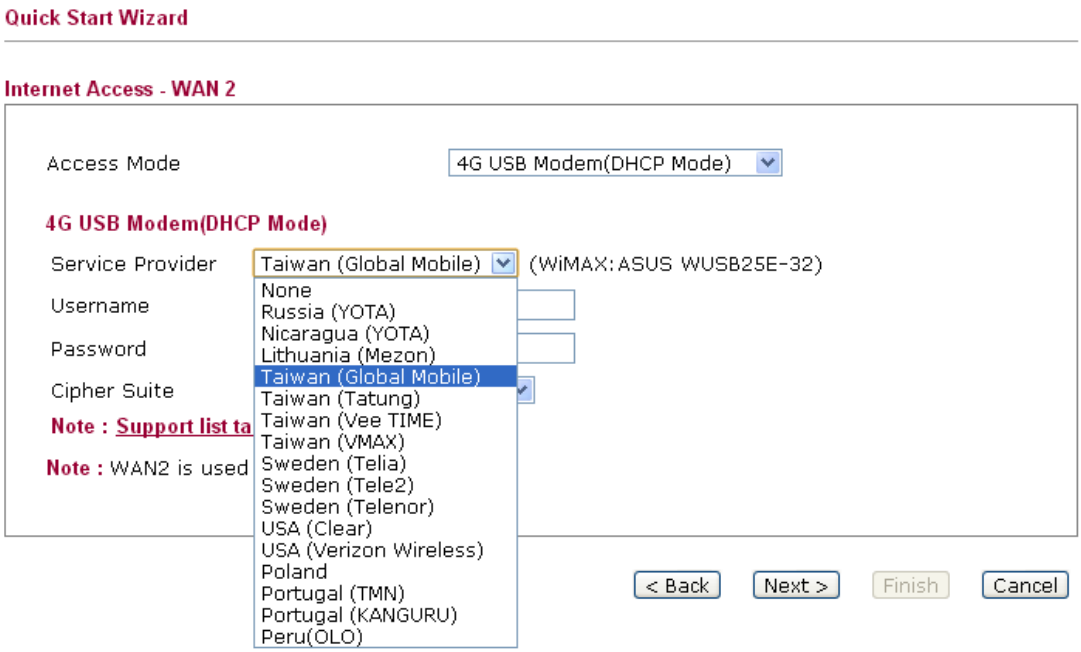
Available parameters are listed below:

Item	Description
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).
PPP Authentication	Select **PAP only** or **PAP or CHAP** for PPP.

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

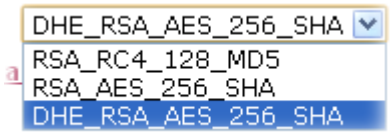
4G USB Modem (DHCP Mode)

If you want to access Internet with 4G USB Modem, choose 4G USB Modem as the Access Mode. Corresponding settings will be displayed for you to configure.



Available parameters are listed below:

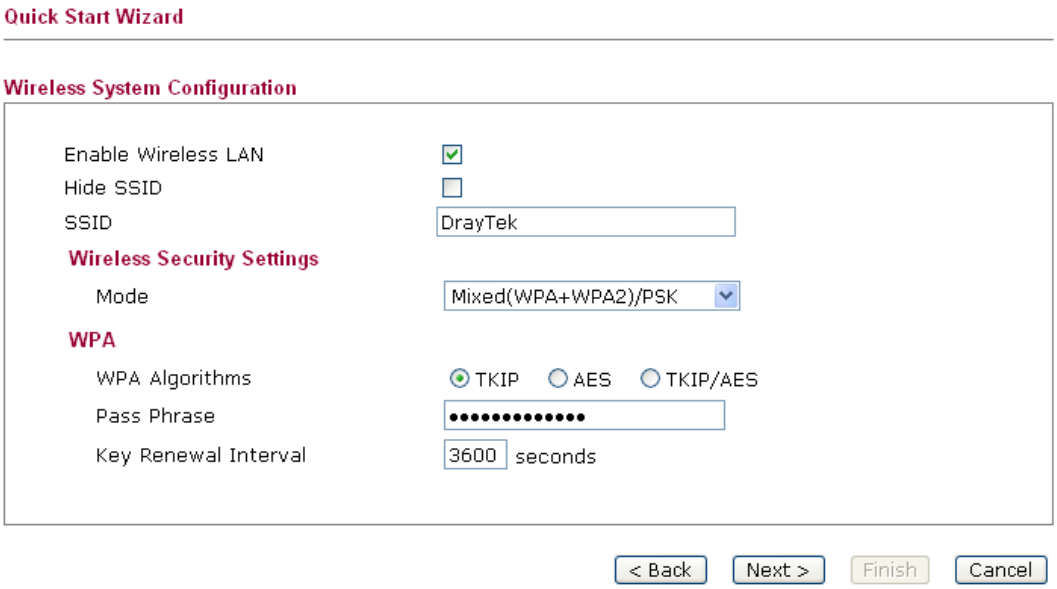
Item	Description
Service Provider	Choose the local service provider which can serve network service according to the nature of USB Modem (LTE/WiMAX) installed. For example, you live in Taiwan and have a WiMAX modem inserted onto VigorFly 210. You can choose Taiwan (Global Mobile) to configure necessary settings and then surf the Internet easily.  The available settings will be different based on the service

Item	Description
	provider specified. In this case, Taiwan (Global Mobile) is chosen as an example.
Username	Type the user name acquired from the service provider.
Password	Type the password acquired from the service provider.
Cipher Suite	**Cipher Suite –** There are two encryption methods offered for you to choose as cipher suite. Keep the default setting will be better. Such item is required for WiMAX USB Modem. 

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

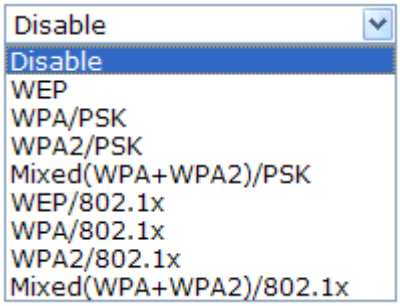
2.3.5 Setting up the Wireless Connection

Now, you have to set up the wireless connection.



Available parameters are listed below:

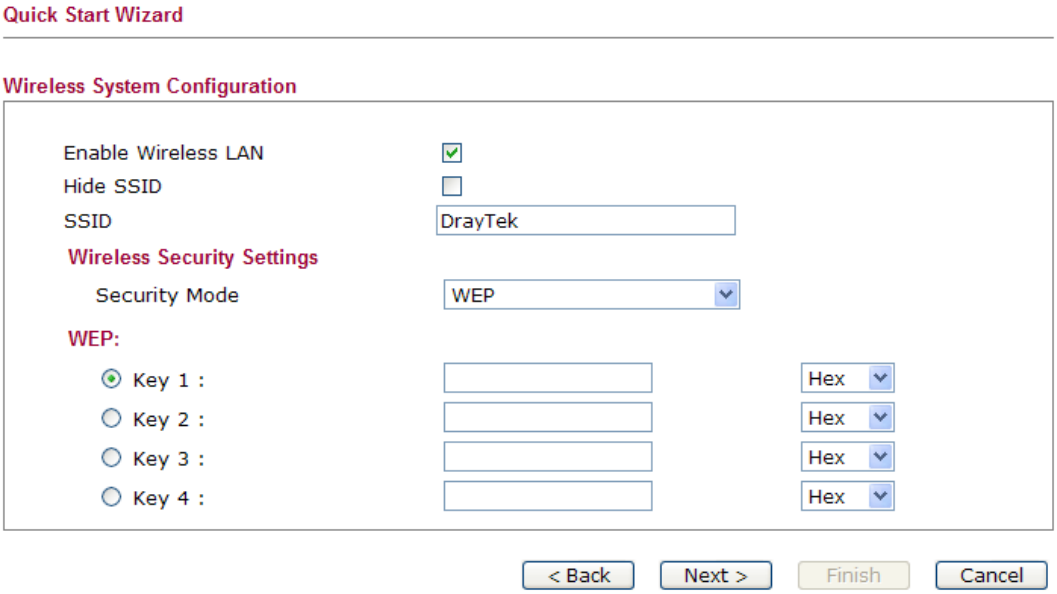
Item	Description
Enable Wireless LAN	Check the box to enable the wireless function.
Hide SSID	Check this box to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN.
SSID	It means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "DrayTek". We suggest you to change it.
Mode	Choose the wireless mode for this router.

Item	Description
	 Each encryption mode will bring out different web page and ask you to offer additional configuration.

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

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.



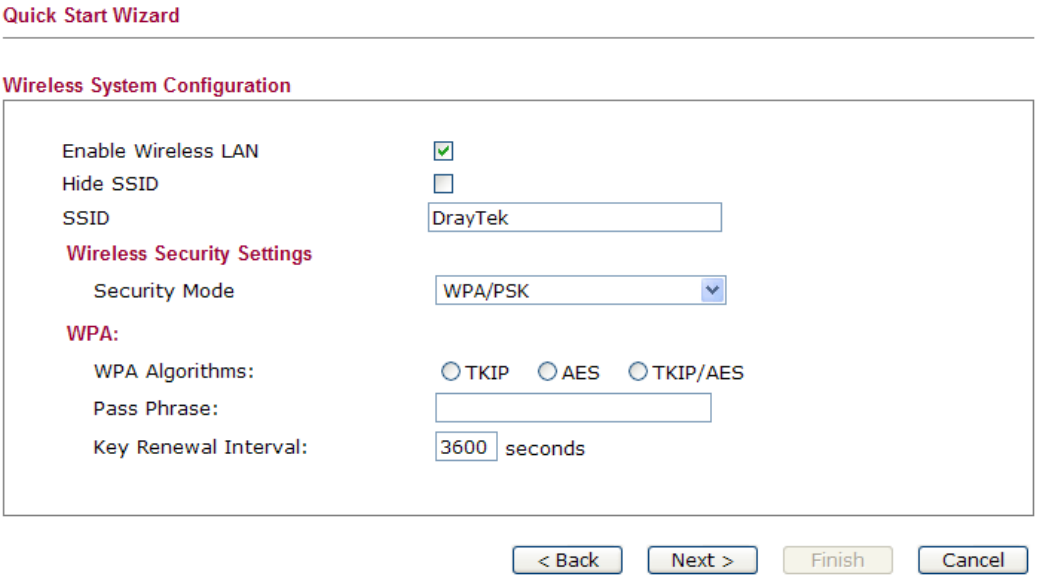
Available parameters are listed below:

Item	Description
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 ','.

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

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.



Available parameters are listed below:

Item	Description
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.

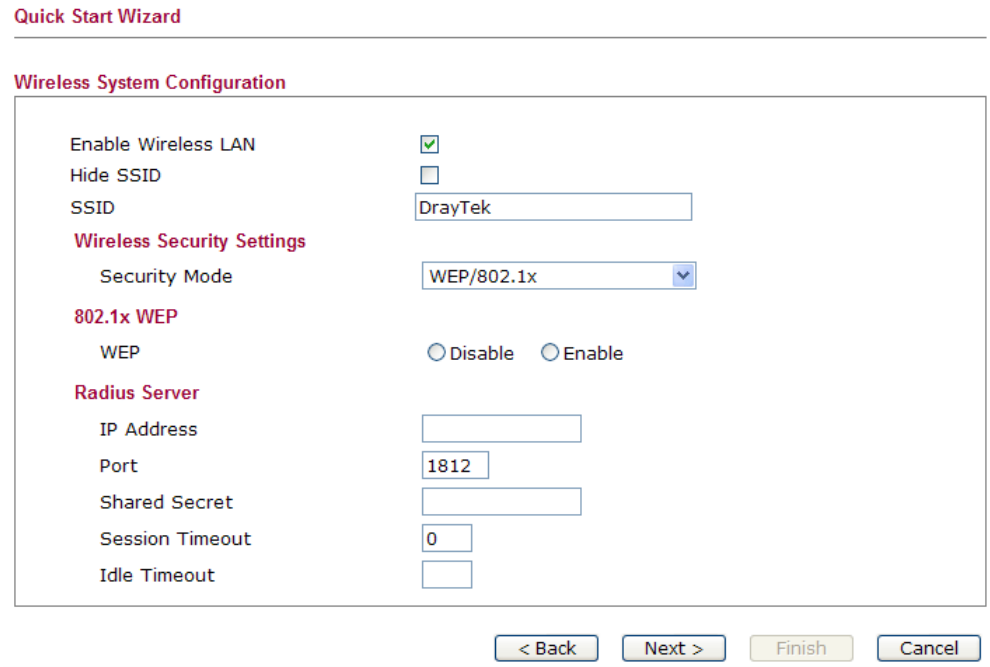
After finishing the settings here, please click **Next.**

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.

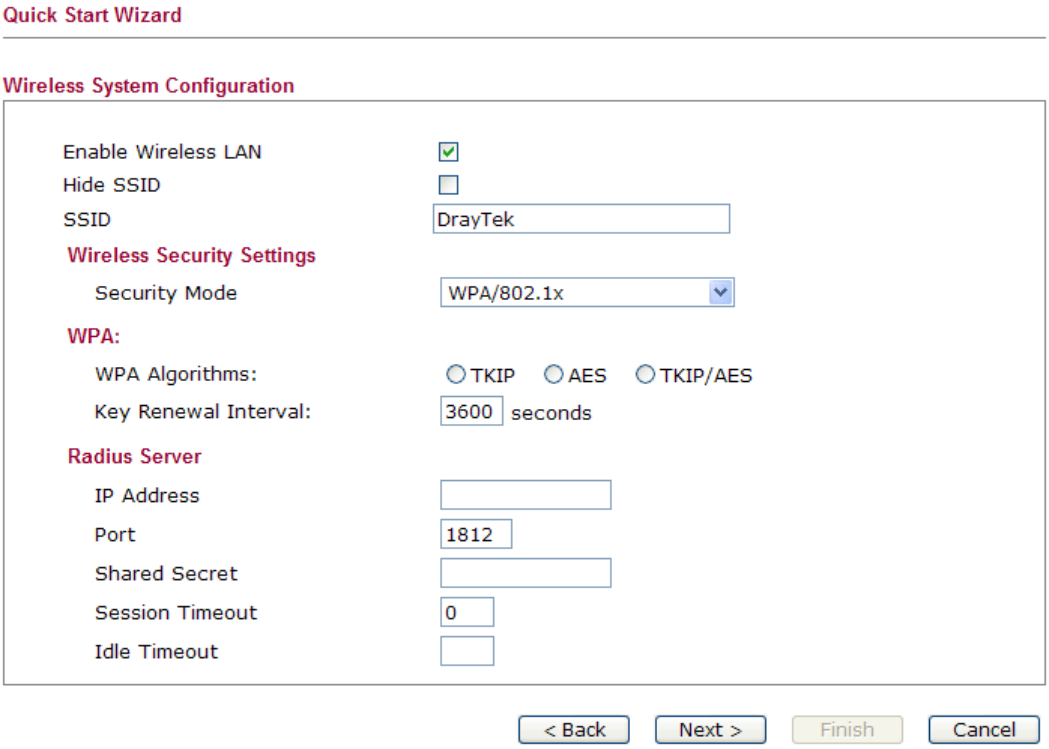


Available parameters are listed below:

Item	Description
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.

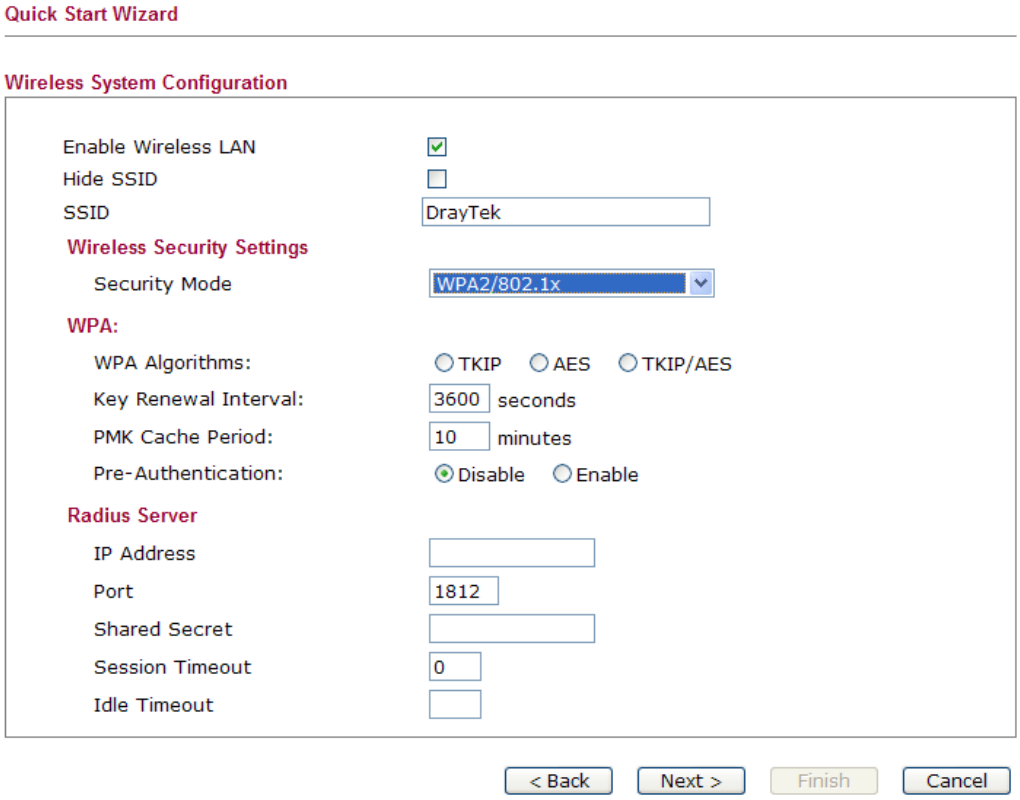


Available parameters are listed below:

Item	Description
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.



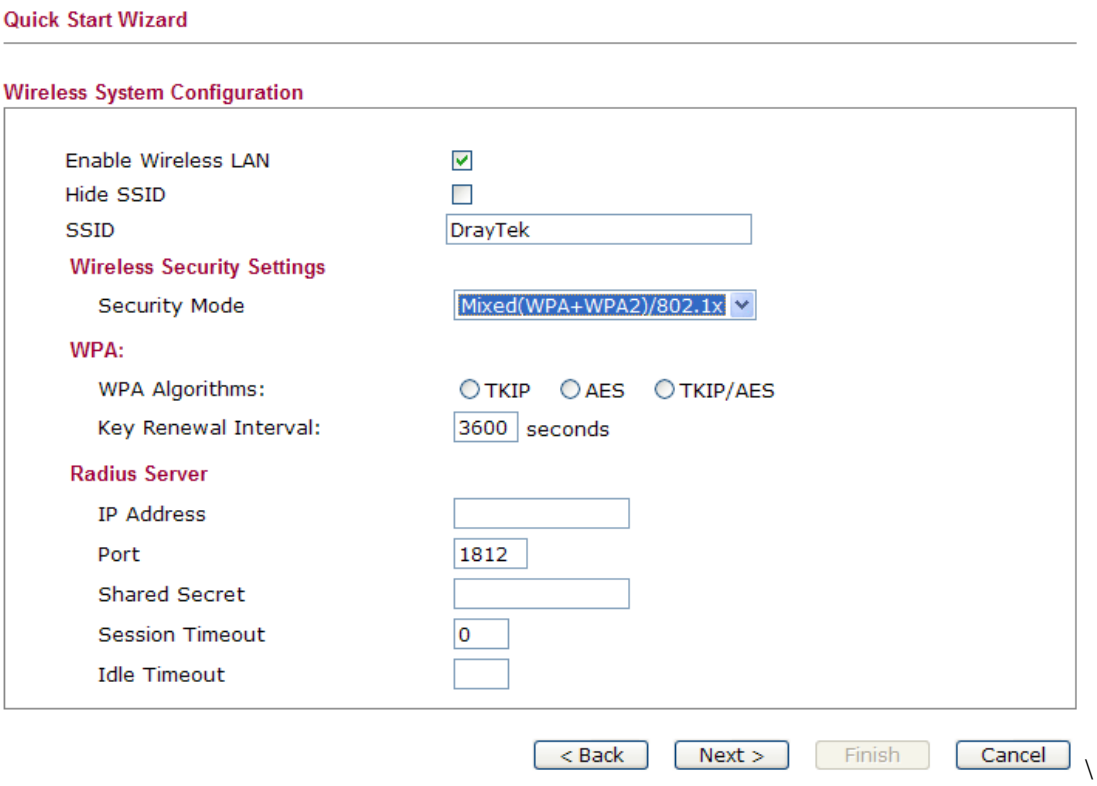
Available parameters are listed below:

Item	Description
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.

Item	Description
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.



Available parameters are listed below:

Item	Description
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

Item	Description
	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.)

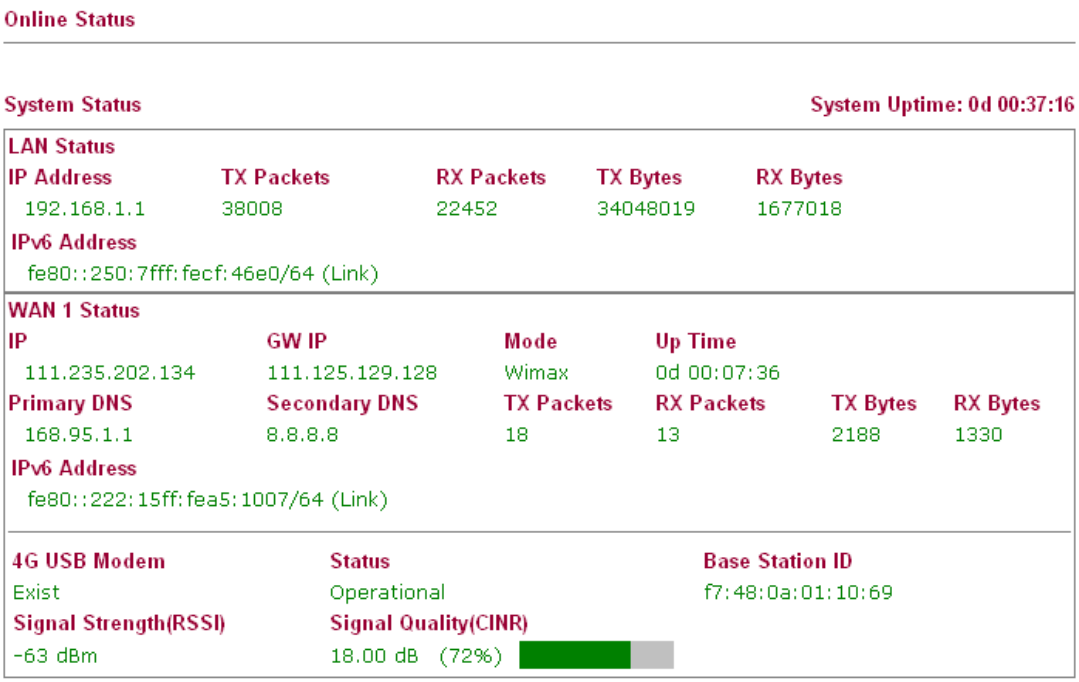
After finishing the settings here, please click **Next.**

2.3.6 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.

2.4 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.



Detailed explanation is shown below:

Item	Description
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. **TX Bytes** - Displays the total transmitted rate at the LAN interface. **RX Bytes** - Displays the total number of received rate 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. **IPv6 Address** - Display the IP address for Ipv6 protocol.
4G USB Modem	**4G USB Modem** - Display if such modem is connected or not. **Status** - Display the connection status (Disconnected/Connecting/Operational) for the connected dongle. **Base Station ID** - Display the MAC address of the remote base station. **Signal Strength (RSSI)** - Display the strength of the wireless signal. **Signal Quality (CINR)** - Display the quality of the wireless signal. The larger the value number is, the better the quality shall be.

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.

2.5 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.

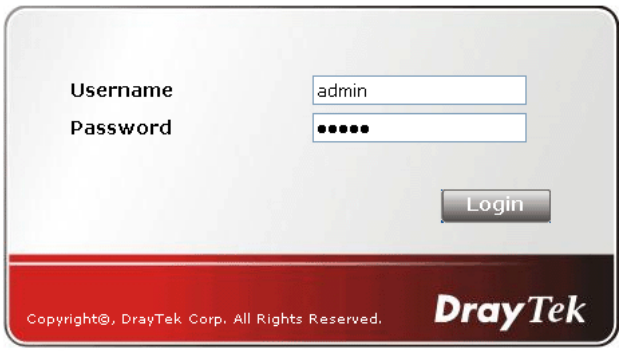
Ready indicates the system is ready for you to input settings.

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

2.6 Registering Vigor Router

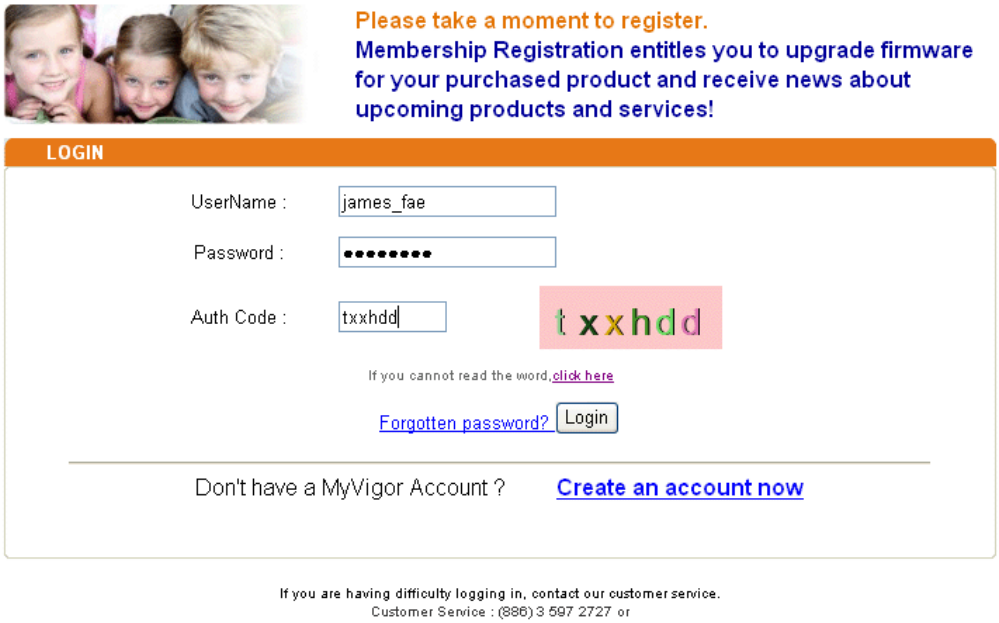
You have finished the configuration of Quick Start Wizard and you can surf the Internet at any time. Now it is the time to register your Vigor router to MyVigor website for getting more service. Please follow the steps below to finish the router registration.

1. Please login the web configuration interface of Vigor router by typing "**admin/admin**" as User Name / Password.

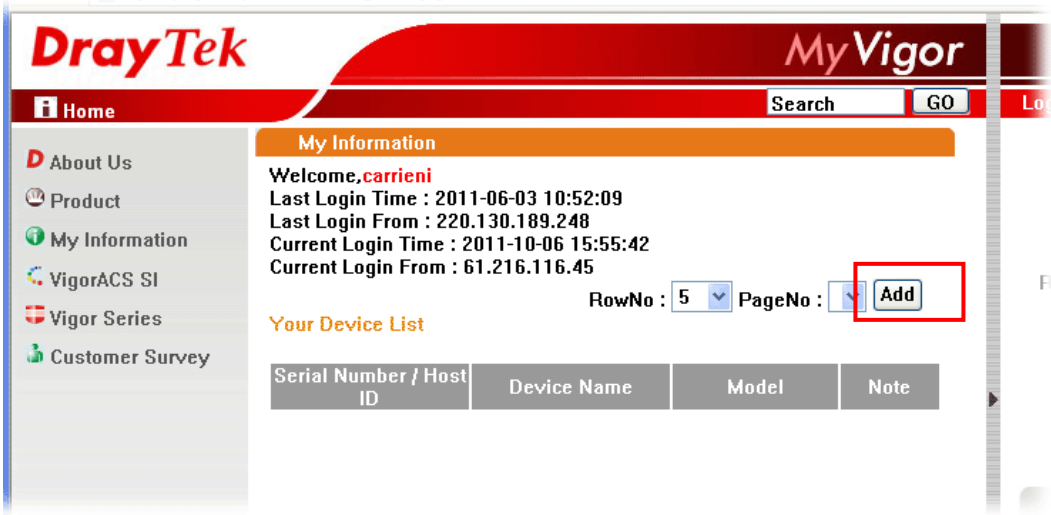


2. Click **Support Area>>Production Registration** from the home page.

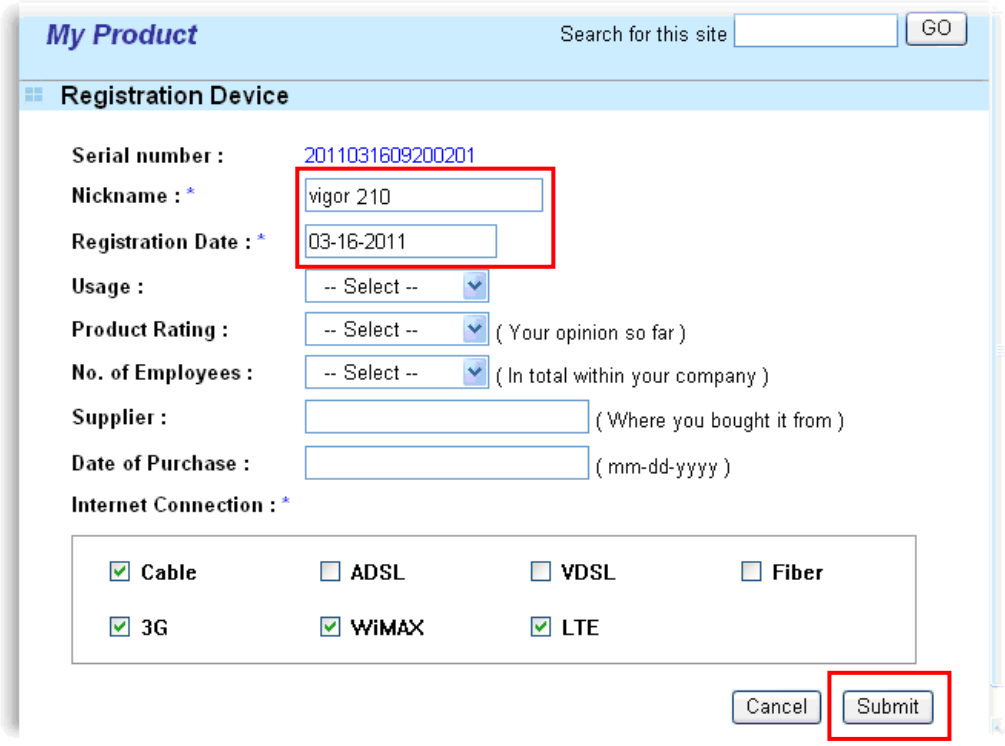
3. A **Login** page will be shown on the screen. Please type the account and password that you created previously. And click **Login**.



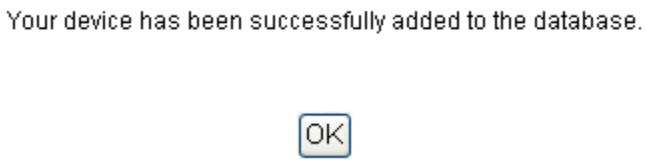
4. The following page will be displayed after you logging in MyVigor. From this page, please click **Add**.



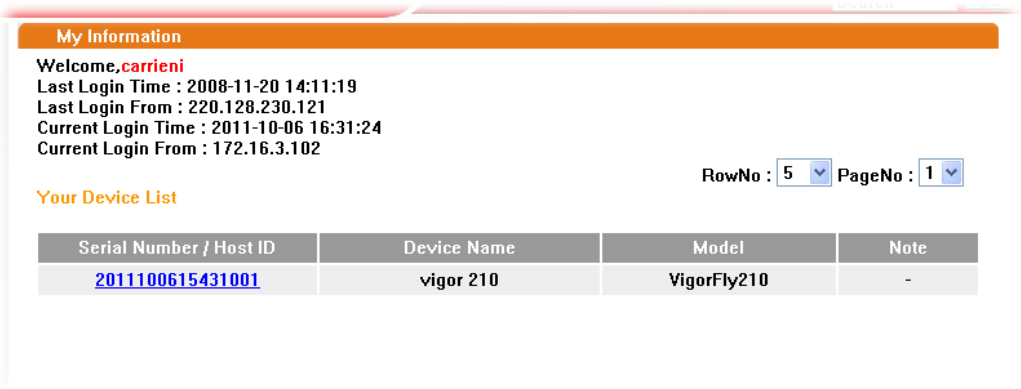
5. When the following page appears, please type in Nickname (for the router) and choose the right registration date from the popup calendar (it appears when you click on the box of Registration Date). After adding the basic information for the router, please click **Submit**.



6. When the following page appears, your router information has been added to MyVigor database.



7. Click **OK**. Now, you have finished the product registration.

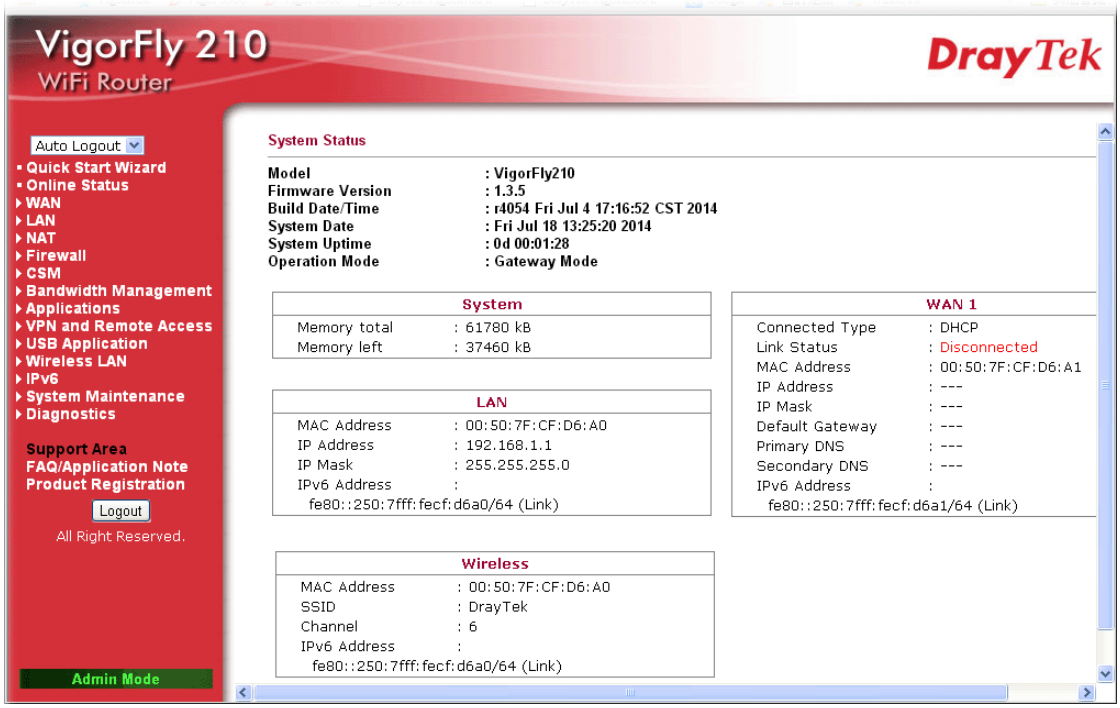


3 Advanced Web Configuration

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.



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 **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.

Network Connection by 4G USB Modem

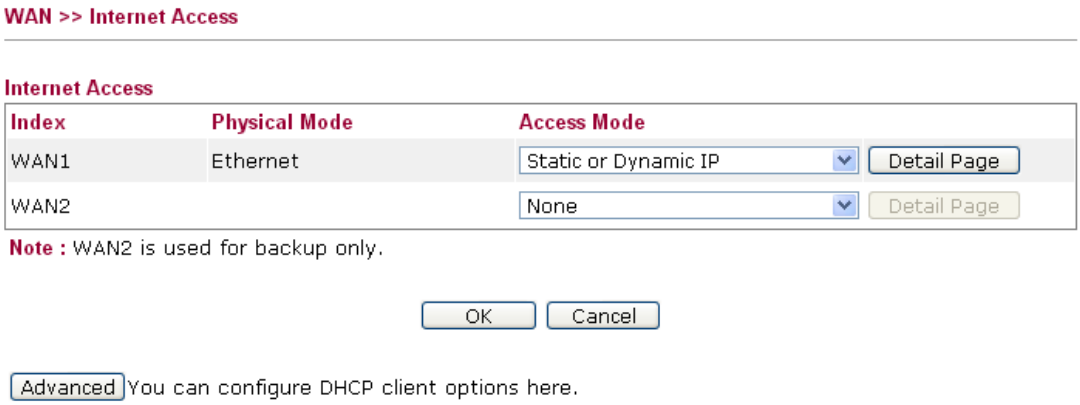
To meet the request in bandwidth / rate for data transmission via wireless connection, VigorFly 210 offers 4G USB Modem to satisfy requirements for different countries.

Also, it can be used as a backup device by configured with WAN2, and will be invoked instead whenever WAN1 connection is not available due to unexpected error.

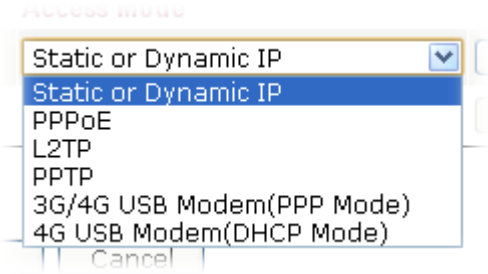
Below shows the menu items for **WAN**.

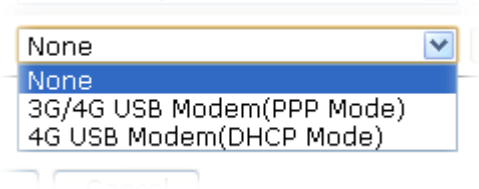
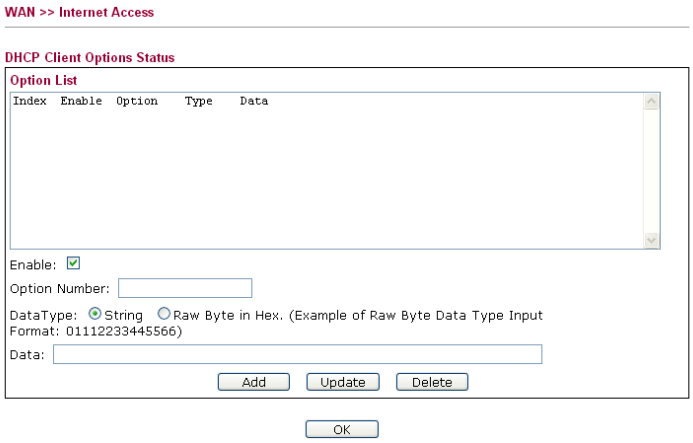
3.1.1 Internet Access

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.



Each item is explained as follows:

Item	Description
Index	Display the WAN interface.
Physical Mode	It shows the physical connection for WAN1(Ethernet)/WAN2 (3G/4G Backup) according to the real network connection.
Access Mode	Use the drop down list to choose a proper access mode. The details page of that mode will be popped up. If not, click Details Page for accessing the page to configure the settings.  for WAN1

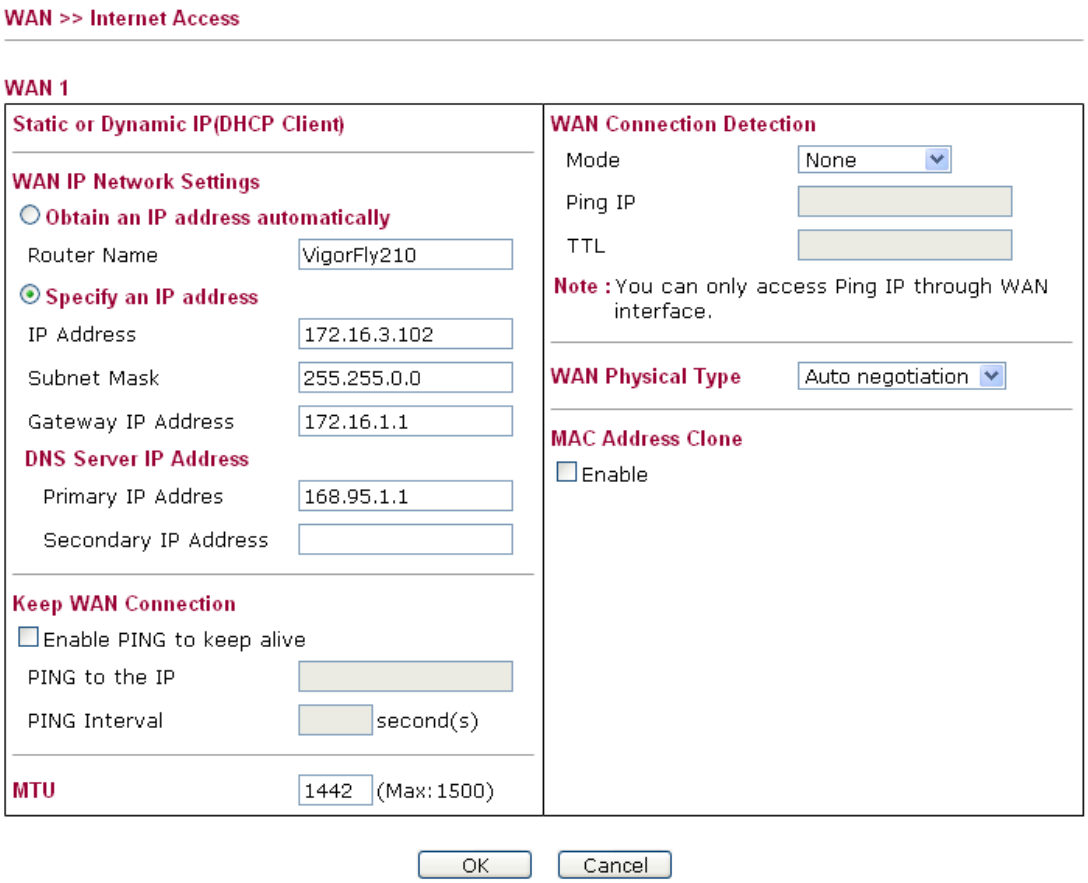
	 for WAN2
Details Page	This button will open different web page according to the access mode that you choose in WAN interface.
Advanced	This button allows you to configure DHCP client options. DHCP packets can be processed by adding option number and data information when such function is enabled and configured.  **Enable** – Enable the function of DHCP Option. Each DHCP option is composed by an option number with data. For example, Option number:100 Data: abcd When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets. **Option Number** – Type a number for such function. **Note:** If you choose to configure option 61 here, the detailed settings in WAN>>Internet Access will be overwritten. **DataType** – Choose the type (ASCII or Hex) for the data to be stored. **Data** – Type the content of the data to be processed by the function of DHCP option.

Static or Dynamic IP for WAN1

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.

Dynamic IP allows a user to obtain an IP address automatically from a DHCP server on the Internet.

To use **Static IP** or **Dynamic IP** as the accessing protocol of the internet, please choose **Static or Dynamic IP** mode from **Access** drop down menu. Then click **Detail Page** to open the following web page.



Available parameters are listed below:

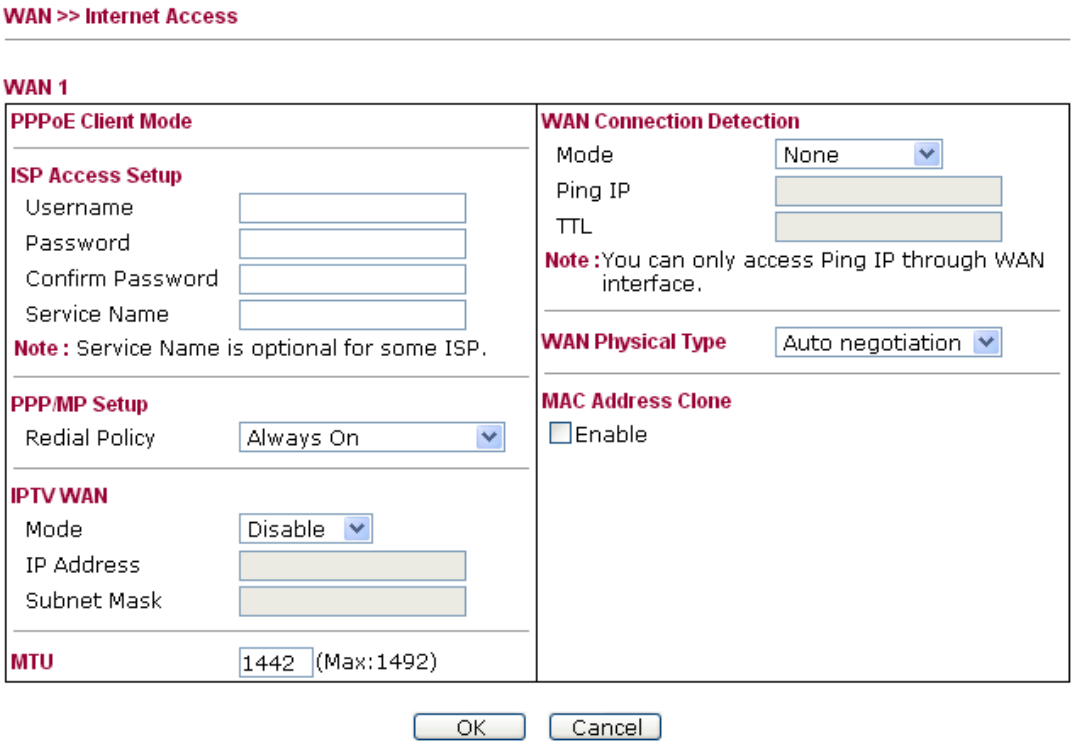
Item	Description
Obtain an IP address automatically	To get an IP address from DHCP server, simply click this button. The default router name will be displayed. Modify the name if required.
Specify an IP Address	Click this radio button to specify some data if you want to use **Static IP** mode. **IP Address**: Type the IP address. **Subnet Mask**: Type the subnet mask. **Gateway IP Address**: Type the gateway IP address.
DNS Server IP Address	**Primary DNS Server -** You must specify a DNS server IP

Item	Description
	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.
Keep WAN Connection	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check **Enable PING to keep alive** box to activate this function. **PING to the IP -** If you enable the PING function, please specify the IP address for the system to PING it for keeping alive. **PING Interval -** Enter the interval for the system to execute the PING operation.
MTU	It means Max Transmit Unit for packet. The default setting is 1442.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. **Mode** – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection. **Ping IP** – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. **TTL (Time to Live)** – Displays value for your reference. TTL value is set by telnet command.
WAN Physical Type	Specify the data transmitting rate for such mode.
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. MAC Address Clone ☑ Enable MAC Address MAC Address Clone

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

PPPoE for WAN1

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.



Available parameters are listed below:

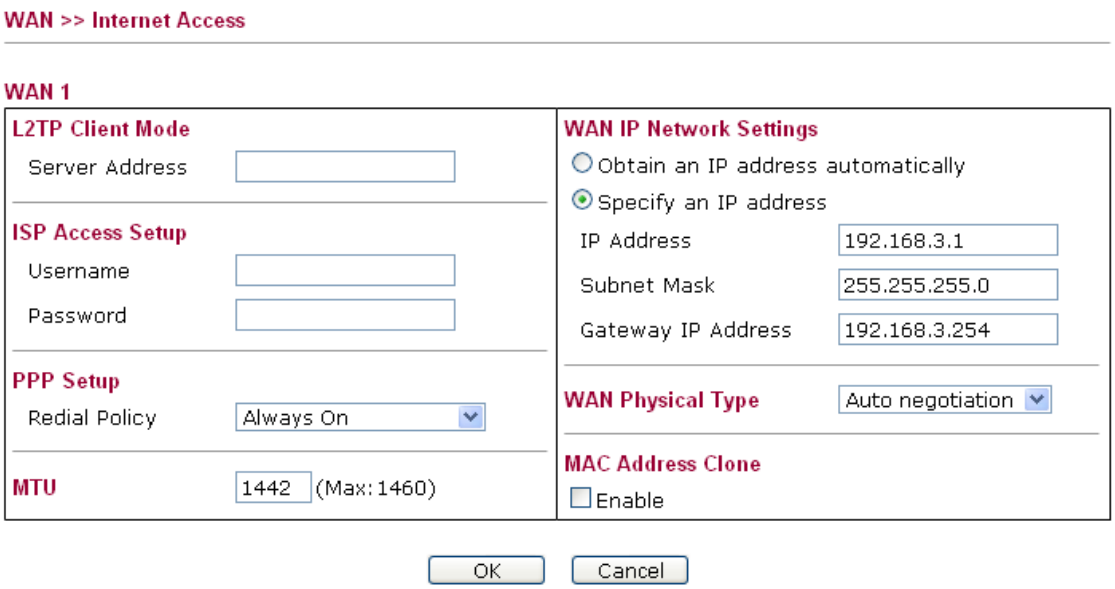
Item	Description
ISP Access Setup	**Username -** Type in the username provided by ISP in this field. **Password -** Type in the password provided by ISP in this field. **Confirm Password -** Re-enter the password for confirmation. **Service Name -** Enter the description of the specific network service.
PPP/MP Setup	**Redial Policy -** If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, choose **Connect on Demand**. Connect on Demand Connect on Demand Always On **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.
IPTV WAN	VigorFly 210 supports IPTV application (traditional television channel, movie or VoD service) through the second WAN IP under PPPoE connection mode. **Mode -** Choose DHCP or Static IP.

Item	Description
	IP Address - Type the IP address if Static IP is selected as the Mode for IPTV WAN application. **Subnet Mask -** Type the subnet mask if Static IP is selected as the Mode for IPTV WAN application.
MTU	It means Max Transmit Unit for packet. The default setting is 1442.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. **Mode** – Choose **None** or **Ping Detect** for the system to execute for WAN detection. **Ping IP** – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. **TTL (Time to Live)** – Displays value for your reference. TTL value is set by telnet command.
WAN Physical Type	Specify the data transmitting rate for such mode.
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. MAC Address Clone ☑ Enable MAC Address MAC Address Clone

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

PPTP/L2TP for WAN1

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.



Available parameters are listed below:

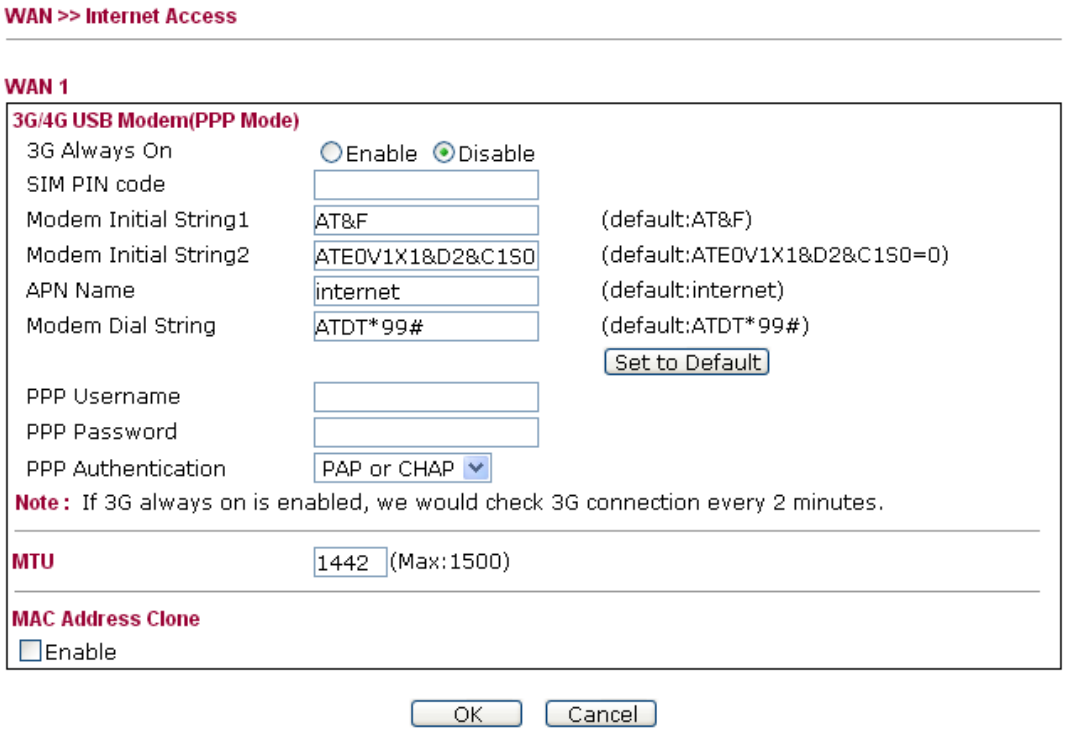
Item	Description
L2TP Client Mode / PPTP Client Mode	**Server IP -** Type in the IP address of the PPTP/L2TP server.
ISP Access Setup	**User Name -** Type in the username provided by ISP in this field. **Password -** Type in the password provided by ISP in this field.
PPP Setup	**Redial Policy -** If you want to connect to Internet all the time, you can choose **Always On**. Otherwise, choose **Connect on Demand**. Connect on Demand Connect on Demand Always On **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.
MTU	It means Max Transmit Unit for packet. The default setting is 1442.
WAN IP Network Settings	**Obtain an IP address automatically** – Click this button to obtain the IP address automatically. **Specify an IP address** – Click this radio button to specify some data. **IP Address** – Type the IP address. **Subnet Mask** – Type the subnet mask.

Item	Description
	Default Gateway - Type the gateway address for this router.
WAN Physical Type	Specify the data transmitting rate for such mode.
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. MAC Address Clone ☑ Enable MAC Address MAC Address Clone

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

3G/4G USB Modem (PPP Modem) for WAN1

If your router connects to a 3G/4G modem and you want to access Internet via 3G/4G modem, choose 3G/4G as connection type and type the required information in this web page.



Available parameters are listed below:

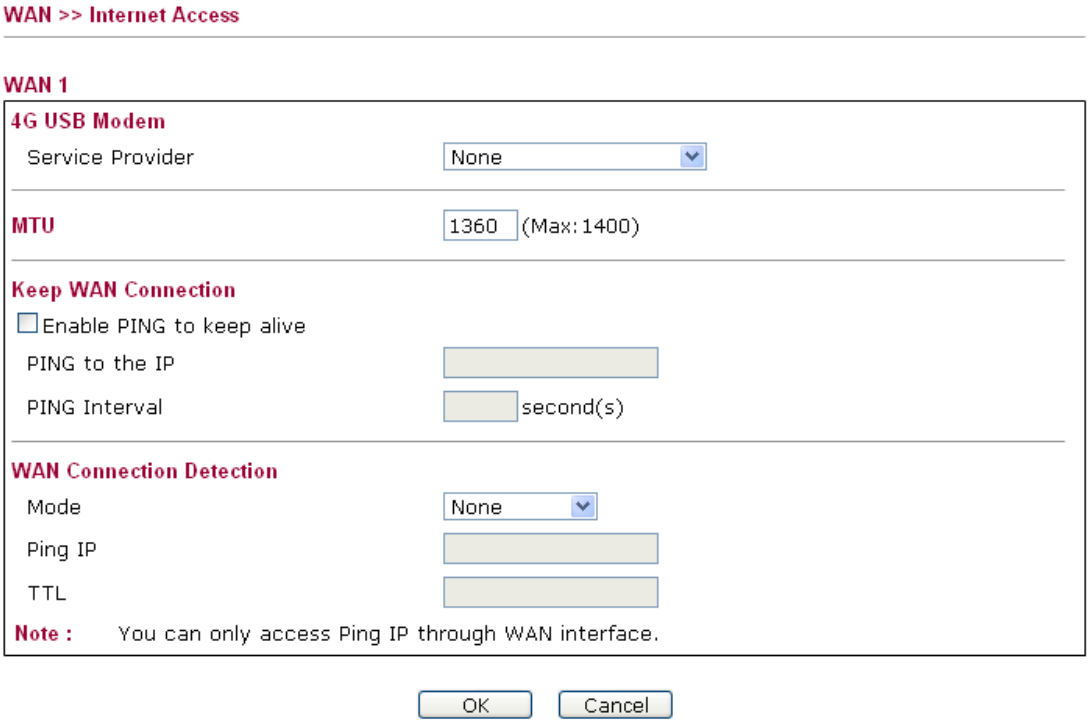
Item	Description
3G USB Modem	**3G Always On –** **SIM PIN code -** Type PIN code of the SIM card that will be used to access Internet. **Modem Initial String1/2 -** Such value is used to initialize USB modem. Please use the default value. If you have any

	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). **PPP Authentication** - Select **PAP only** or **PAP or CHAP** for PPP.
MTU	It means Max Transmit Unit for packet. The default setting is 1442.
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. MAC Address Clone ☑ Enable MAC Address MAC Address Clone

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

4G USB Modem (DHCP Mode) for WAN1

If your router connects to a 4G modem and you want to access Internet via 4G modem, choose 4G as connection type and type the required information in this web page.



Available parameters are listed below:

Item	Description
4G USB Modem	**Service Provider –** Choose the local service provider which can serve network service according to the nature of USB Modem (LTE/WiMAX) installed. For example, you live in Taiwan and have a WiMAX modem inserted onto VigorFly 210. You can choose Taiwan (Global Mobile) to configure necessary settings and then surf the Internet easily.  **Username -** Type the user name acquired from the service provider. Such item is required for WiMAX USB Modem. **Password -** Type the password acquired from the service provider. Such item is required for WiMAX USB Modem. **Cipher Suite –**There are two encryption methods offered for you to choose as cipher suite. Keep the default setting will be better. Such item is required for WiMAX USB Modem.
MTU	It means Max Transmit Unit for packet. The default setting is 1360.
Keep WAN Connection	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check **Enable PING to keep alive** box to activate this function. **PING to the IP -** If you enable the PING function, please specify the IP address for the system to PING it for keeping alive. **PING Interval -** Enter the interval for the system to execute the PING operation.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. **Mode** – Choose **None** or **Ping Detect** for the system to execute for WAN detection. **Ping IP** – If you choose Ping Detect as detection mode, you

Item	Description
	have to type IP address in this field for pinging. **TTL (Time to Live)** – Displays value for your reference. TTL value is set by telnet command.

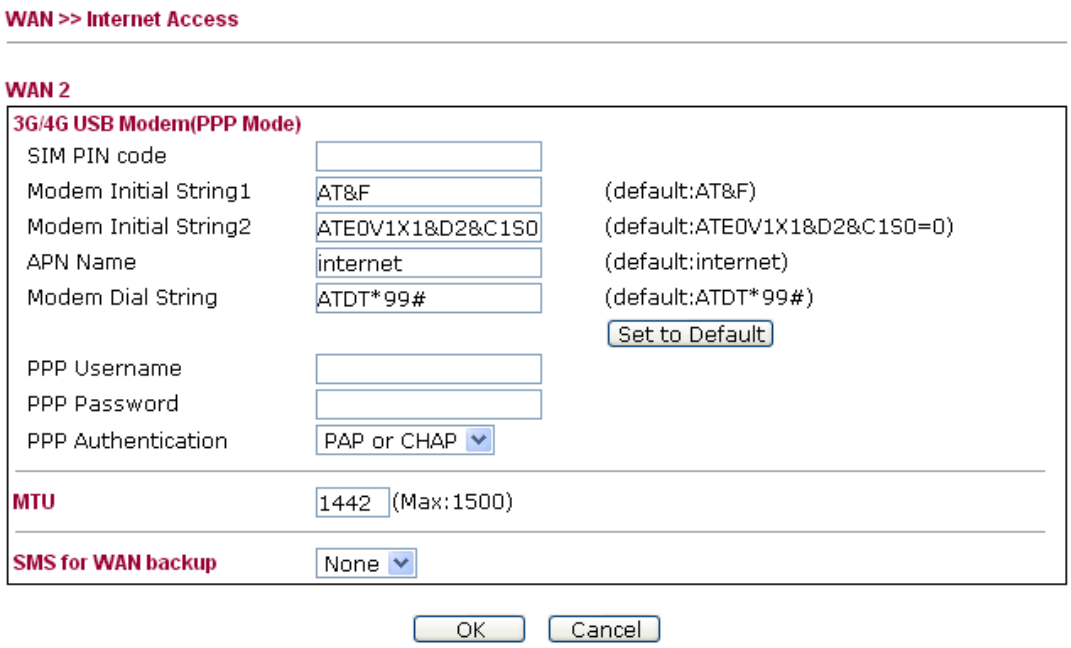
After finishing all the settings here, please click **OK** to activate them.

3G/4G USB Modem (PPP Mode) for WAN2

WAN2 is used for **backup** only. Therefore, it is an optional setting. The default is **None** for **Access Mode**. If it is required, choose 3G USB Modem or 4G USB Modem as a backup WAN interface to access into Internet.

If you want to enable 3G/4G USB Modem in WAN2, make sure your WAN1 connection type is not in 3G/4G mode. When the WAN1 connection is broken, the router will try to keep the connection with 3G mode. After WAN1 connection is recovered, router will disconnect the 3G/3G connection automatically.

Below shows the configuration page for 3G/4G USB Modem:



Available parameters are listed below:

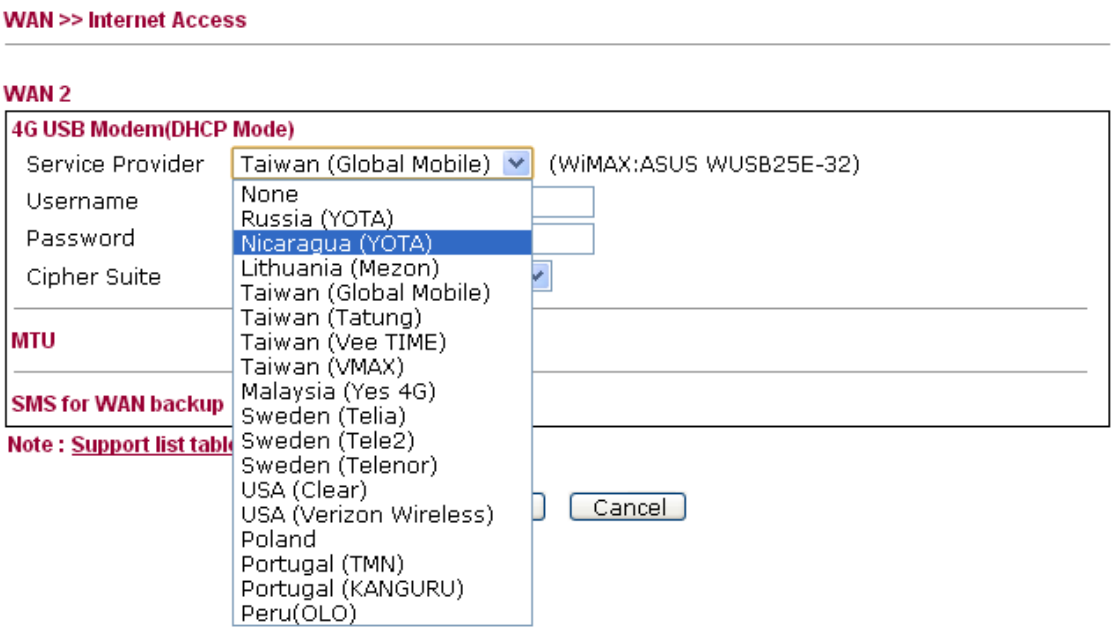
Item	Description
3G USB Modem	**SIM PIN code -** Type PIN code of the SIM card that will be used to access Internet. **Modem Initial String1/2 -** Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP. **APN Name -** APN means Access 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). **PPP Authentication** - Select **PAP only** or **PAP or CHAP** for PPP.
MTU	It means Max Transmit Unit for packet. The default setting is 1442.
SMS for WAN backup	Use the drop down list to choose one of the SMS profiles (created in **Application>>SMS**) which will take effect when WAN2 is up.

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

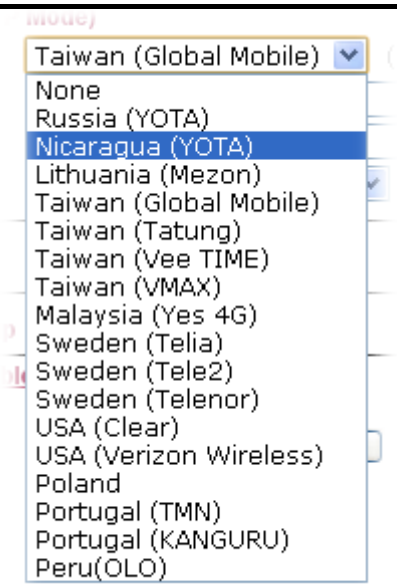
4G USB Modem (DHCP Mode) for WAN2

Below shows the configuration page for 4G USB Modem:



Available parameters are listed below:

Item	Description
4G USB Modem	**Service Provider –**Choose the local service provider which can serve network service according to the nature of USB Modem (LTE/WiMAX) installed. For example, you live in Taiwan and have a WiMAX modem inserted onto VigorFly 210. You can choose Taiwan (Global Mobile) to configure necessary settings and then surf the Internet easily.

	 The available settings will be different based on the service provider specified. In this case, Taiwan (Global Mobile) is chosen as an example.
Username	Type the user name acquired from the service provider. Such item is required for WiMAX USB Modem.
Password	Type the password acquired from the service provider. Such item is required for WiMAX USB Modem.
Cipher Suite	**Cipher Suite –**There are two encryption methods offered for you to choose as cipher suite. Keep the default setting will be better. Such item is required for WiMAX USB Modem.
MTU	It means Max Transmit Unit for packet. The default setting is 1360.
SMS for WAN backup	Use the drop down list to choose one of the SMS profiles (created in **Application>>SMS**) which will take effect when WAN2 is up.

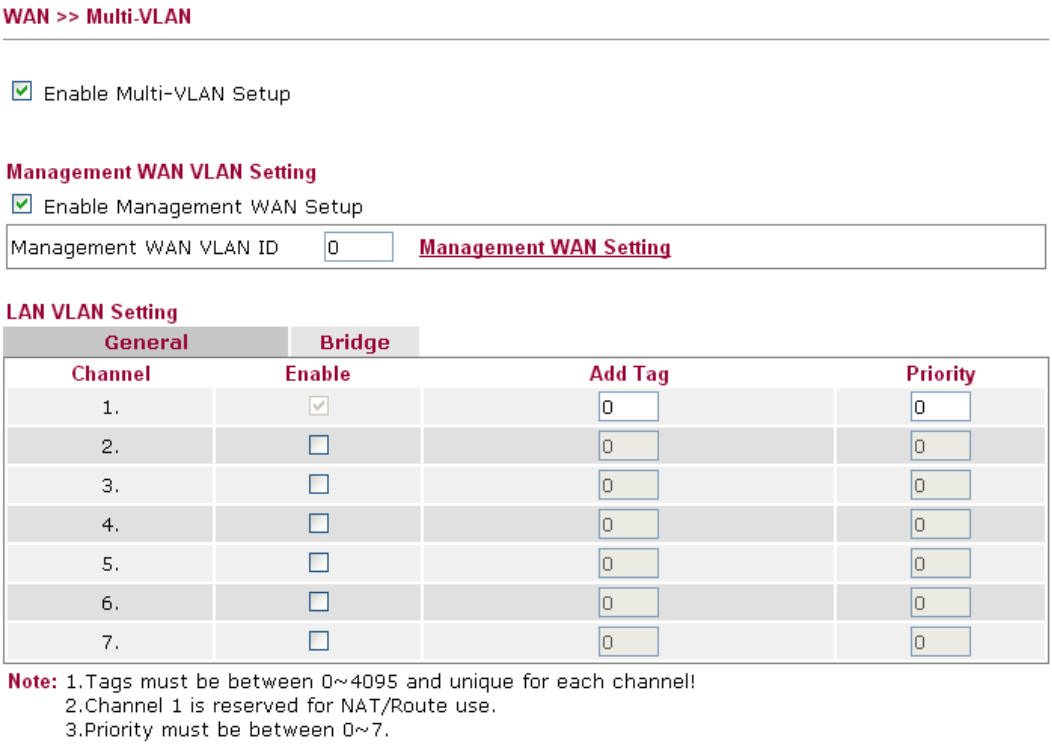
After finishing all the settings here, please click **OK** to activate them.

3.1.2 Multi-VLAN

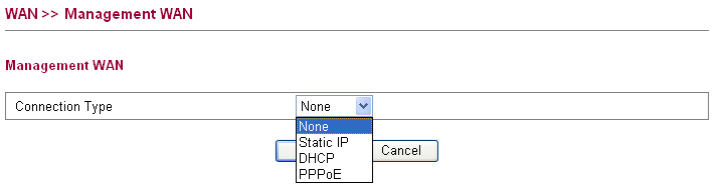
This router allows you to create multi-VLAN for different purposes of data transferring. Simply go to **WAN** and select **Multi-VLAN**.

General

The system allows you to set up to eight channels for multi-VLAN.



Available settings are explained as follows:

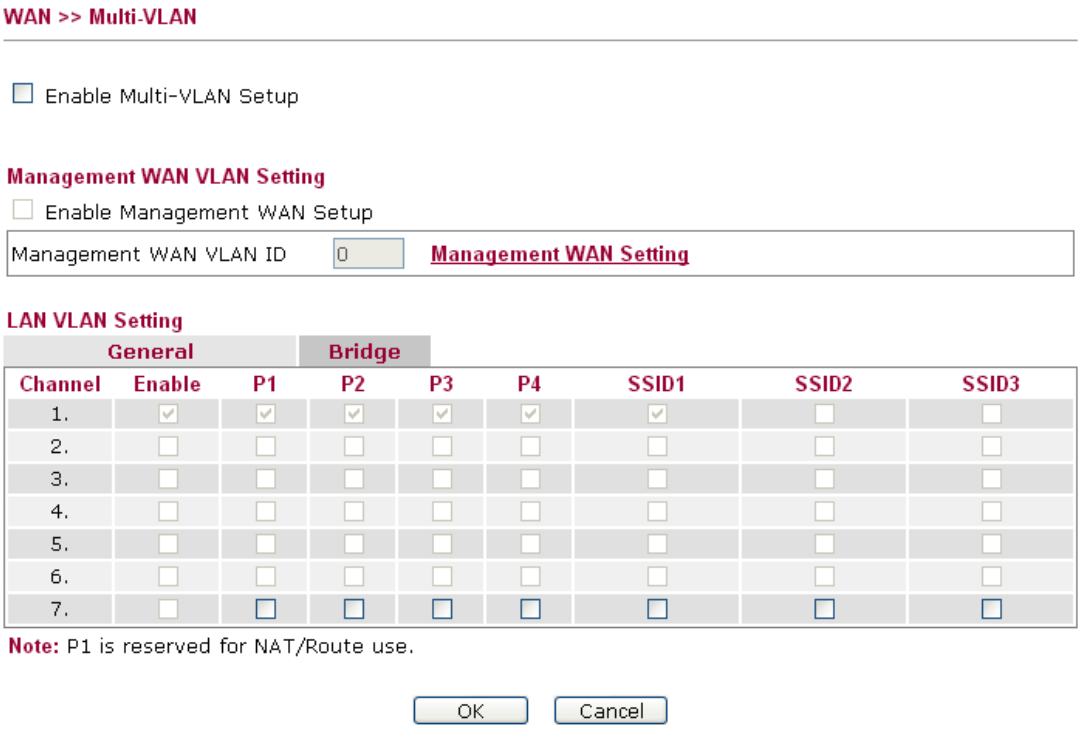
Item	Description
Enable Multi-VLAN Setup	Check this box to activate such setting.
Management WAN VLAN Setting	**Enable Management WAN Setup-** Check the box to enable **Management WAN** configuration. **Management WAN VLAN ID -** Data sent out through the WAN port will be tagged with VLAN ID number specified here. The range of ID number you can type is from 0 - 4095. **Management WAN Setting** – Click this link to open Management WAN setting. 
Channel	Display the number of each channel.
Enable	Check this box to enable that channel. The channels that you enabled here will be shown in the **Multi-VLAN** channel drop down list on the web page of **Internet Access**. Though you can

	enable eight channels in this page, yet only one channel can be chosen on the web page of **Internet Access**.
Add Tag	To identify the usage of VLAN, check this box to invoke this setting. And type the number for VLAN ID (number).
Priority	It is used to set the priority for the audio and/or video data transmission. The adjustable range is from 0 (lowest) to 7 (highest).

After finishing all the settings here, please click **OK** to save the configuration.

Bridge

General page lets you set general channel for multi-VLAN. This page allows you to configure VLAN settings under Bridge mode. Simply click the **Bridge** tab to open **Bridge** configuration page.



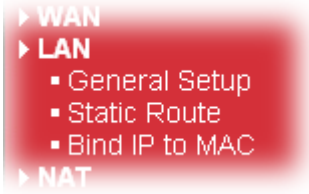
Available settings are explained as follows:

Item	Description
Enable Multi-VLAN Setup	Check this box to activate such setting.
Enable	Check this box to enable that channel. Only channel 3 to 8 can be set in this page, for channel 1 to 2 are reserved for NAT using.
P1 to P4	It means the LAN port 1 to 4. Check the box to designate the LAN port for channel 2 to 7.
SSID1 to SSID3	Check the box to designate the SSID for channel 2 to 7.

When you finish the configuration, please click **OK** to save and exit this page.

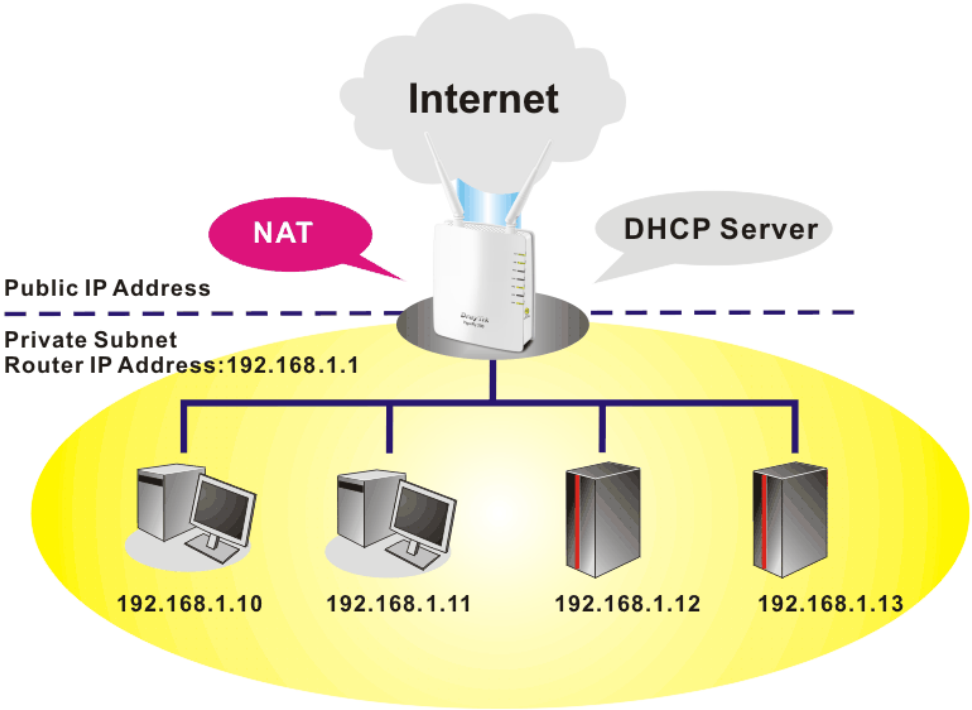
3.2 LAN

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.

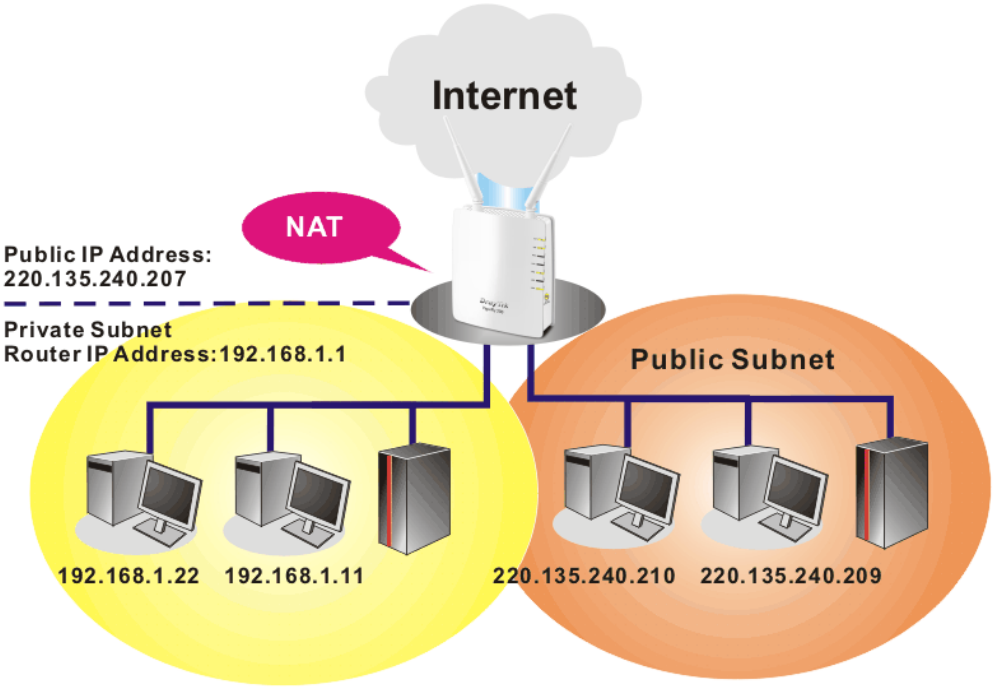


Basics of LAN

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.

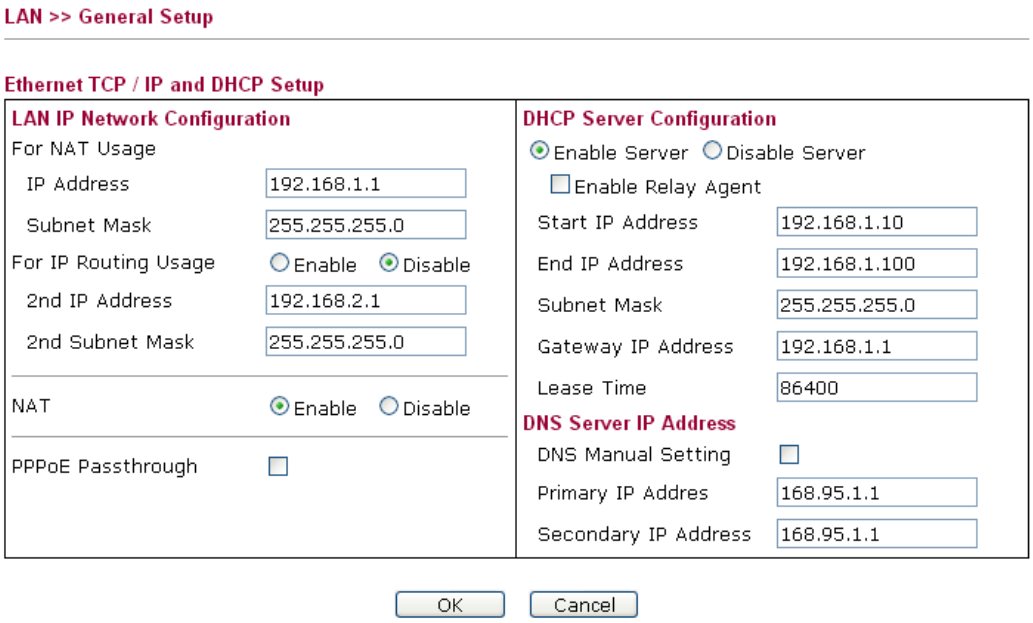
What is Static Route

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.

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**.



Available settings are explained as follows:

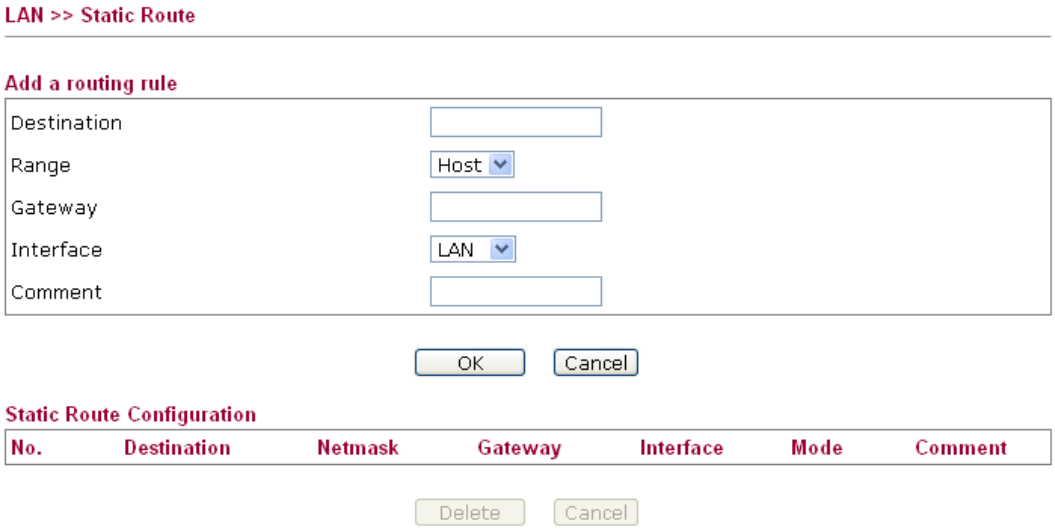
Item	Description
LAN IP Network Configuration	**IP Address -** Type in private IP address for connecting to a local private network (Default: 192.168.1.1). **Subnet Mask-** Type in an address code that determines the size of the network. (Default: 255.255.255.0) **For IP Routing Usage -** Click **Enable** 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. **NAT** – Check the box to execute the function of NAT in LAN. **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. **Enable Server-** Let the router assign IP address to every host in the LAN. **Disable Server-** Let you manually assign IP address to

Item	Description
	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 Server IP Address	**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.

3.2.2 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.



Available settings are explained as follows:

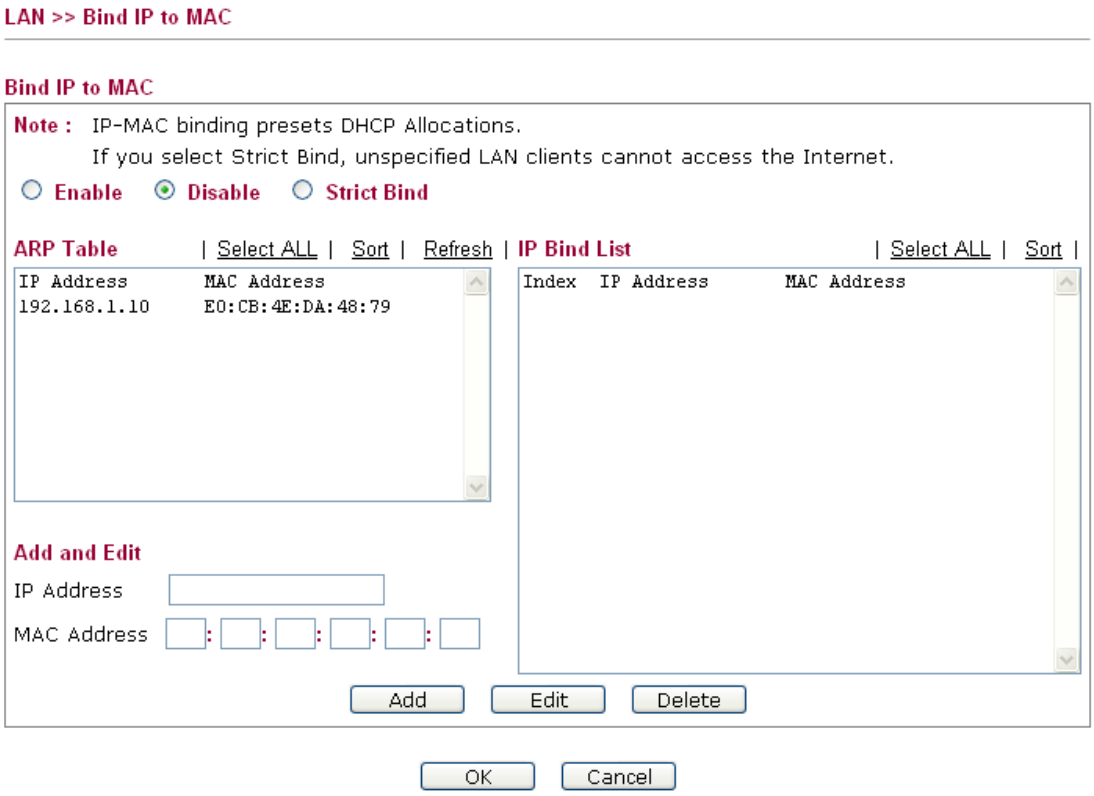
Item	Description
Add a routing rule	**Destination -** Type the IP address for the routing rule applied to. **Range -** Choose **Host** or **Net** for specifying gateway or netmask setting of such routing rule. **Netmask -** Type the netmask for such routing rule if you choose **Net** as **Range** setting. **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.

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

3.2.3 Bind IP to MAC

This function is used to bind the IP and MAC address in LAN to have a strengthening control in network. When this function is enabled, all the assigned IP and MAC address binding together cannot be changed. If you modified the binding IP or MAC address, it might cause you not access into the Internet.

Click **LAN** and click **Bind IP to MAC** to open the setup page.



Available settings are explained as follows:

Item	Description
Enable	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
Disable	Click this radio button to disable this function. All the settings on this page will be invalid.
Strict Bind	Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List.
ARP Table	This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking **Add** below. **Select All -** Click this link to select all the items in the ARP table. **Sort -** Reorder the table based on the IP address. **Refresh -** Refresh the ARP table listed below to obtain the newest ARP table information.

Add or Update	**IP Address** – Type the IP address that will be used for the specified MAC address. **Mac Address** – Type the MAC address that is used to bind with the assigned IP address.
IP Bind List	It displays a list for the IP bind to MAC information. **Add -** It allows you to add the one you choose from the ARP table or the IP/MAC address typed in **Add and Edit** to the table of **IP Bind List**. **Update -** It allows you to edit and modify the selected IP address and MAC address that you create before. **Delete -** You can remove any item listed in **IP Bind List**. Simply click and select the one, and click **Delete**. The selected item will be removed from the **IP Bind List**.

After finishing all the settings here, please click **OK** to save the configuration.

Note: Before you select **Strict Bind**, you have to bind one set of IP/MAC address for one PC. If not, no one of the PCs can access into Internet. And the web user interface of the router might not be accessed.

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 Port Redirection

Port Redirection is usually set up for server related service inside the local network (LAN), such as web servers, FTP servers, E-mail servers etc. Most of the case, you need a public IP address for each server and this public IP address/domain name are recognized by all users. Since the server is actually located inside the LAN, the network well protected by NAT of the router, and identified by its private IP address/port, the goal of Port Redirection function is to forward all access request with public IP address from external users to the mapping private IP address/port of the server.

Note that the port redirection can only apply to incoming traffic.

Open Port allows you to open a range of ports for the traffic of special applications. Common application of Open Port 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.

To use Port Redirection, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 30 port-mapping entries for the internal hosts.

NAT >> Port Redirection

Port Redirection

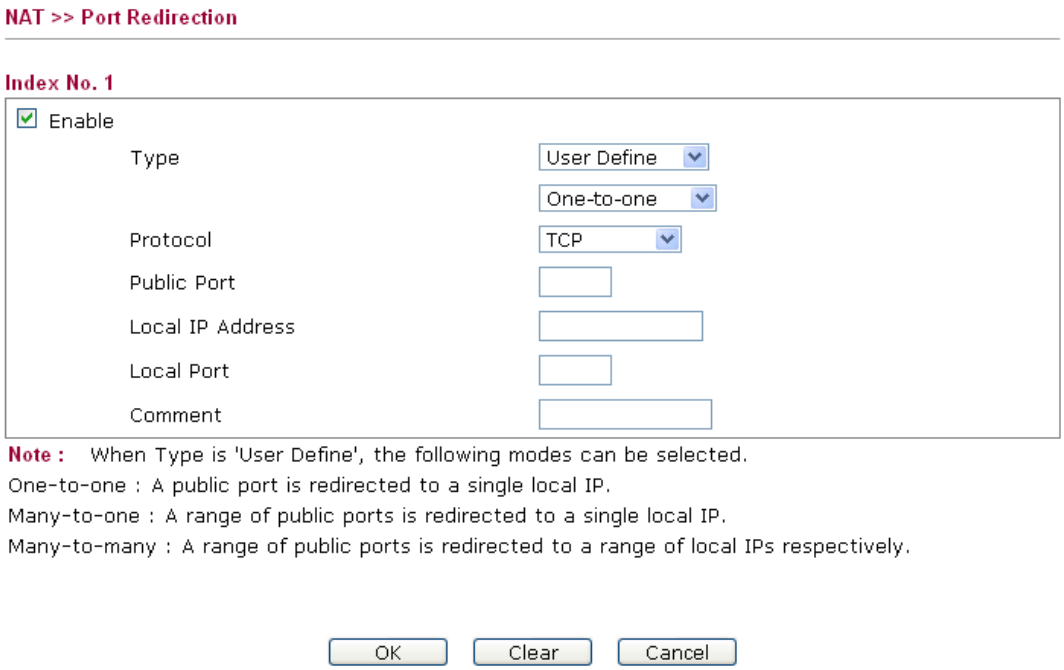
No.	Protocol	Public Port	Local IP Address	Local Port	Comment	Status
1.						x
2.						x
3.						x
4.						x
5.						x
6.						x
7.						x
8.						x
9.						x
10.						x

<< 1-10 | 11-20 | 21-30 >> Next >>

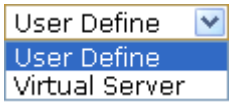
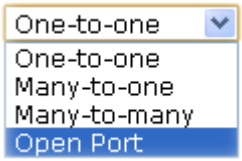
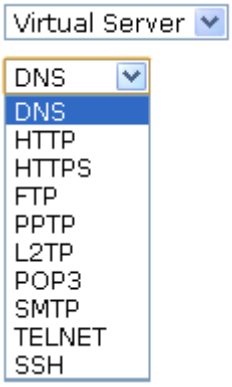
Each item is explained as follows:

Item	Description
No	Display the number of the profile.
Protocol	Display the description of the specific network service.
Public Port	Display the port number which will be redirected to the specified **Private IP** and **Port** of the internal host.
Local IP Address	Display the private IP address of the internal host.
Local Port	Display the private port of the internal host.
Comment	Display the brief description for such profile.
Status	Display if the profile is enabled (v) or not (x).

Press any number under Index to access into next page for configuring port redirection.



Available settings are explained as follows:

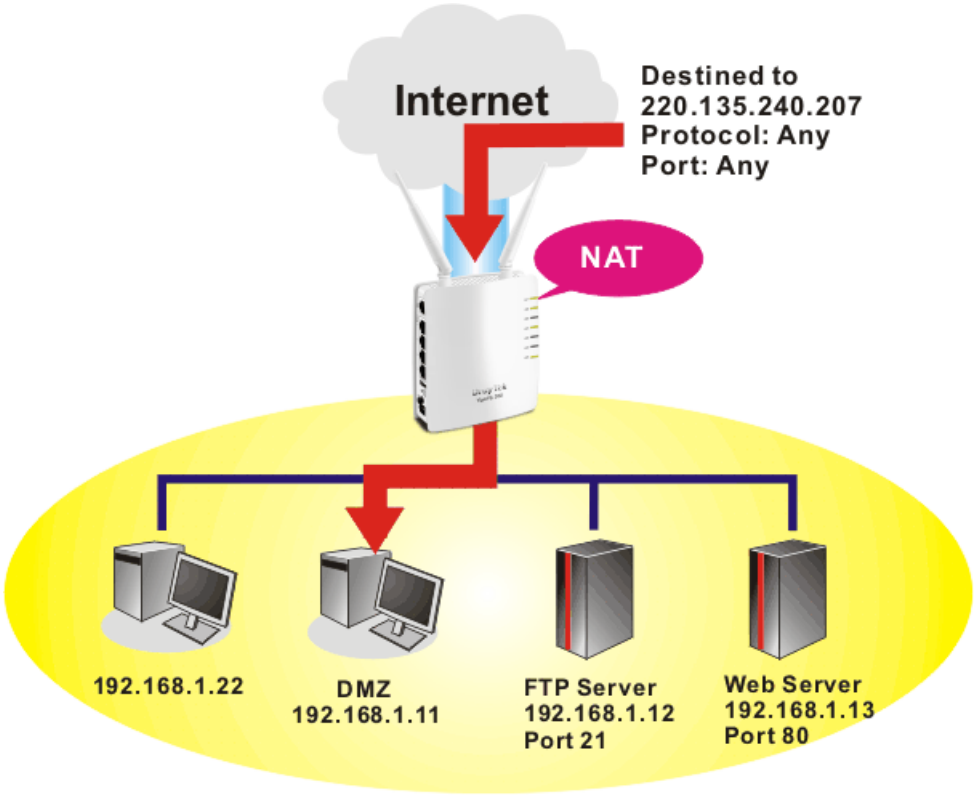
Item	Description
Enable	Check this box to enable such Port Redirection profile.
Type	Specify the type for such profile. The type of Virtual server offers several options with dedicated server and port number. Packets passing through such port number will be redirected into the local IP address and local port assigned below.  If **User Define** is selected, there are four sub-options offered to choose.  If **Virtual Server** is selected, specify a server from the drop down list. 

Protocol	Select the transport layer protocol (TCP or UDP or TCP+UDP).
Local IP Address	Specify the private IP address of the internal host providing the service. I
Local Port	Specify the private port number of the service offered by the internal host.
Comment	Type a brief description for such profile if required. The Maximum length is 23–character long.

After finishing all the settings here, please click **OK** to save the configuration.

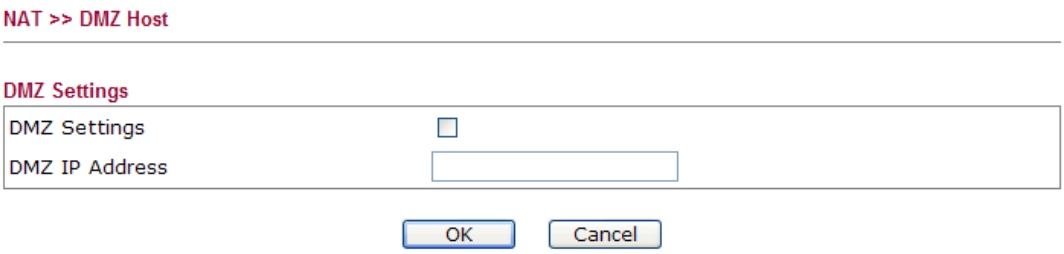
3.3.2 DMZ Host

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:



Available settings are explained as follows:

Item	Description
DMZ Settings	Check this box to enable the DMZ Host function.
DMZ IP Address	Enter the private IP address of the DMZ host.

After finishing all the settings here, please click **OK** to save the configuration.

3.4 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.

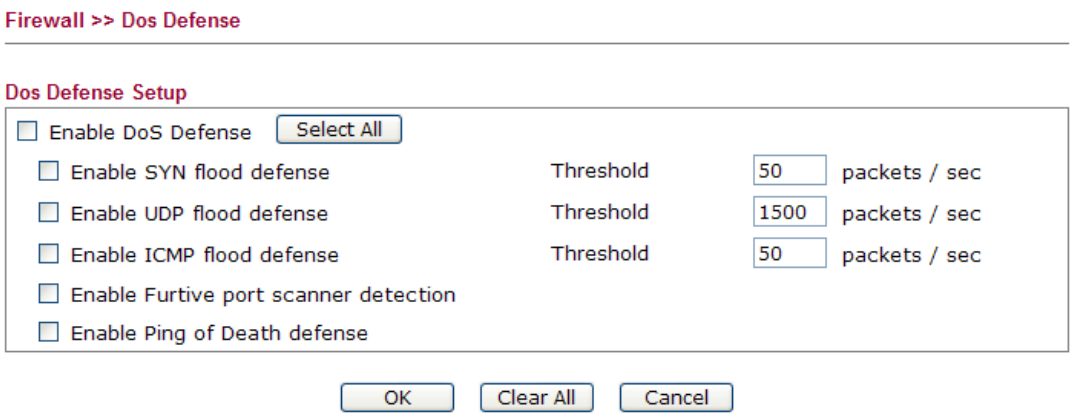
Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

Below shows the menu items for Firewall.

3.4.1 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.



Available settings are explained as follows:

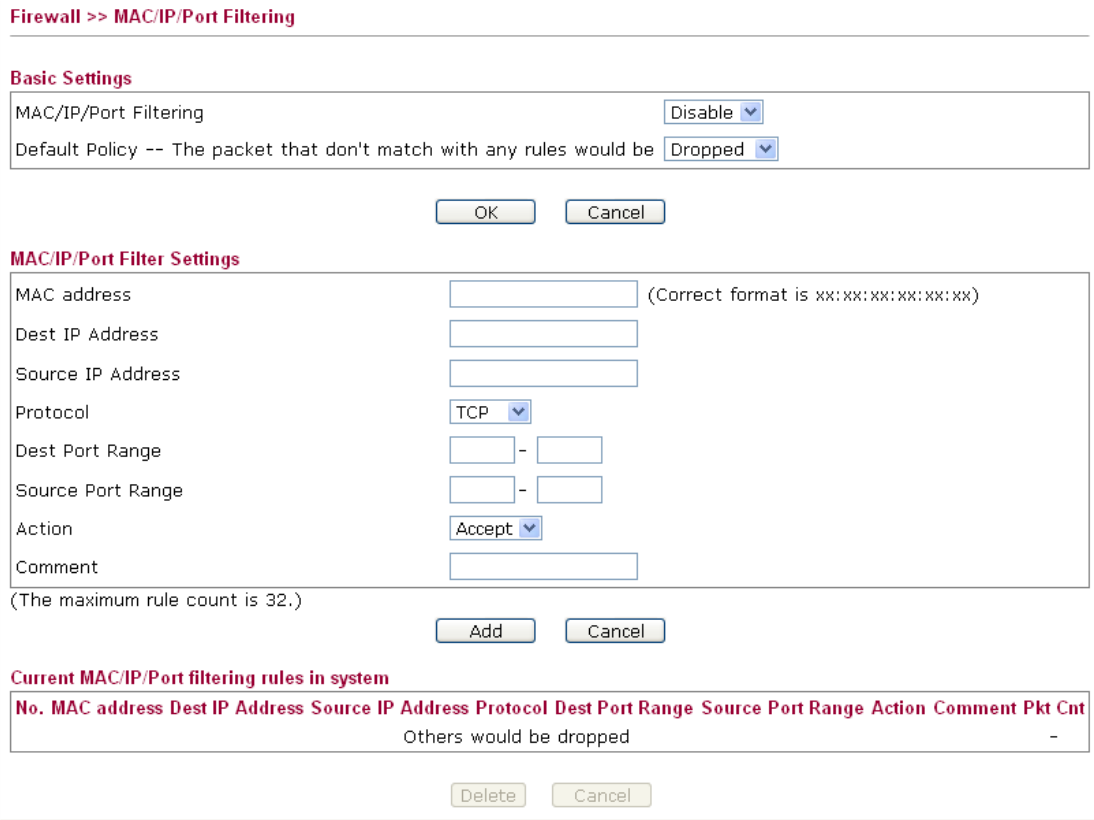
Item	Description
Enable Dos Defense	Check the box to activate the DoS Defense Functionality.
Enable SYN flood defense	Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start 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 1500 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.

After finishing all the settings here, please click **OK** to save the configuration.

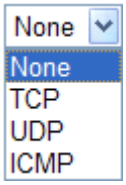
3.4.2 MAC/IP/Port Filtering

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.



Available parameters are listed below:

Item	Description
Basic Settings	**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/IP/Port Filter Settings	**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.

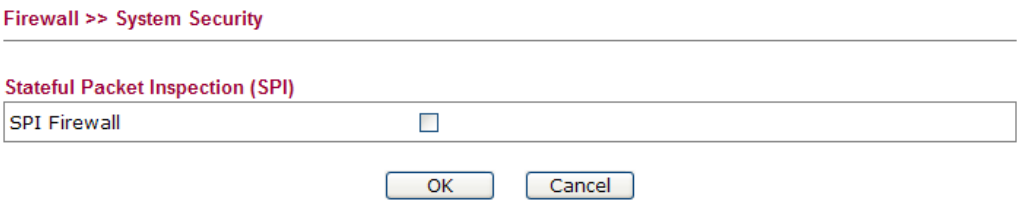
	Protocol - Specify the protocol(s) which this filter rule will apply to.  **Dest Port Range -** Determine the port range for the destination. **Source Port Range -** Determine the port range for the source. **Action –** **Accept:** the packets that match with such rule will be accepted. **Drop**: the packets that match with such rule will be blocked. **Comment -** Enter filter set comments/description. Maximum length is 23–character long.
Add	After typing required information on above, click this button to create a new filtering rule. The new rule will be displayed on the bottom of this web page.

After finishing all the settings here, please click **OK** to save the configuration.

3.4.3 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**.



3.4.4 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.

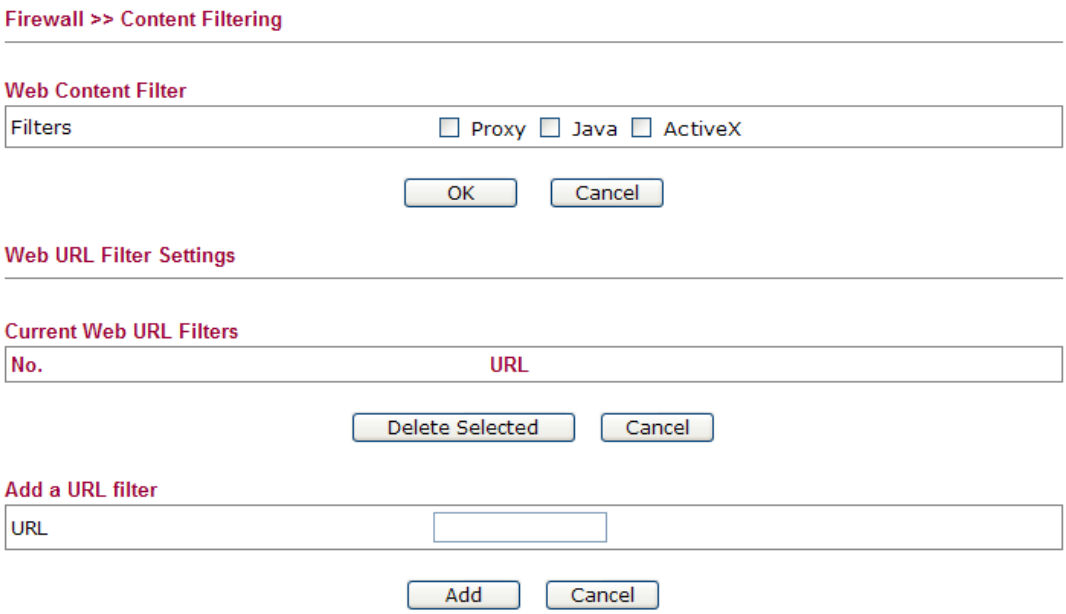
URL Content Filter

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.

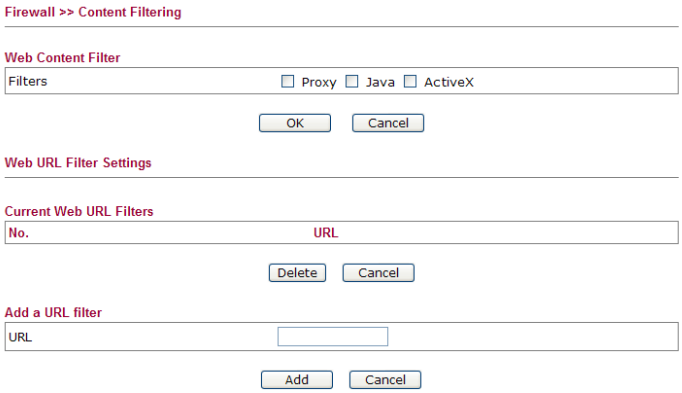
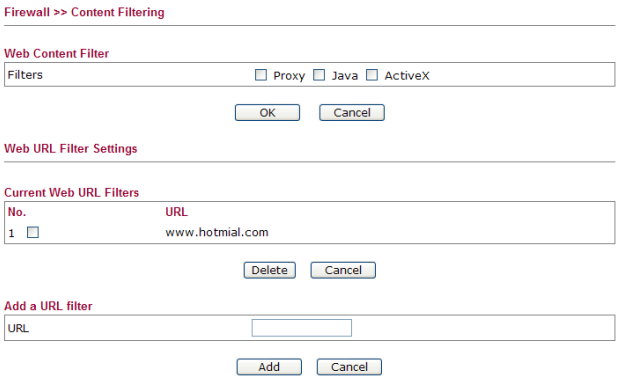
On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from 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>>Content Filtering** to access into the following page.



Available parameters are listed below:

Item	Description
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. 

After finishing all the settings here, please click **OK** to save the configuration.

3.5 CSM

Content Security Management (CSM)

CSM is an abbreviation of **Content Security Management** which is used to filter the web content to reach a goal of security management.

3.5.1 Web Content Filter

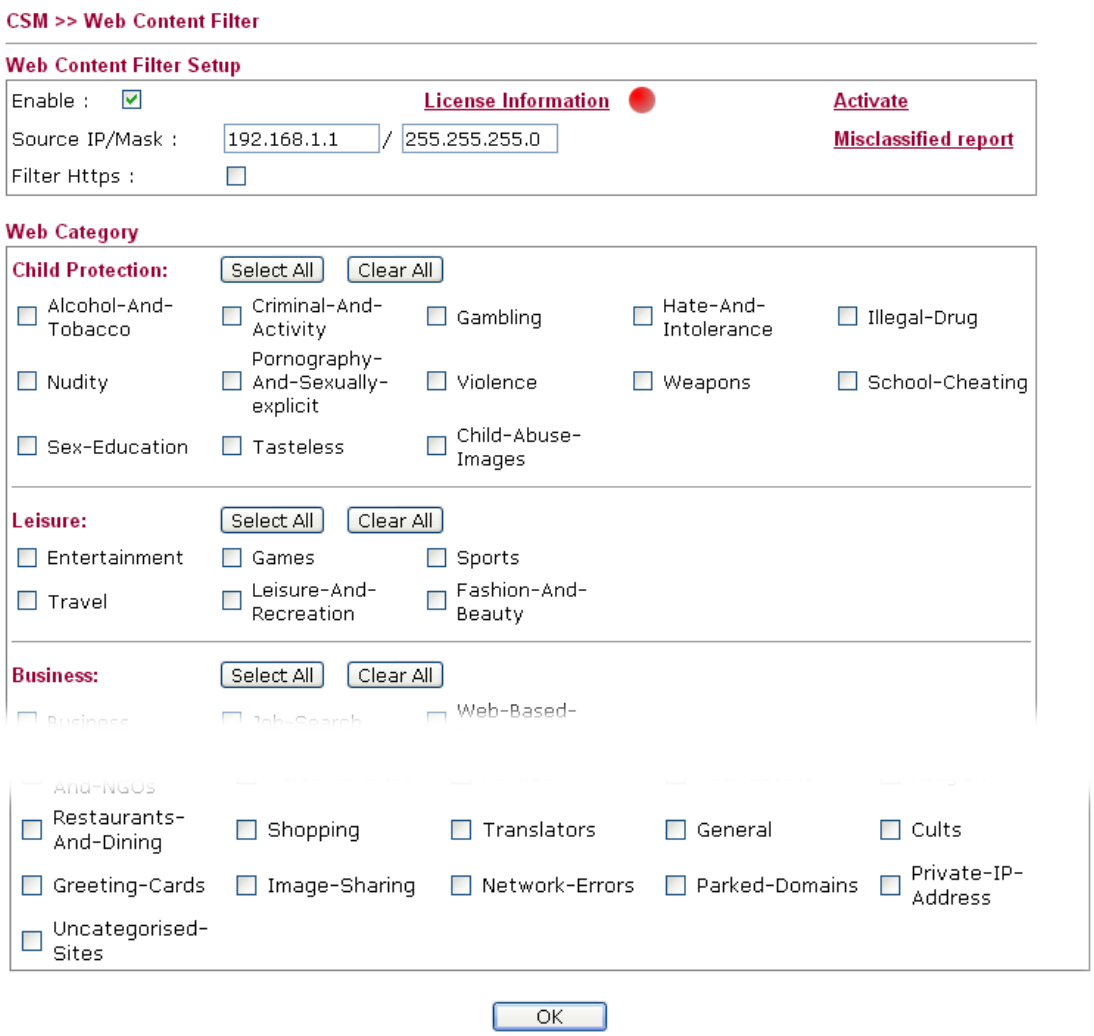
We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary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

security threats. For parents, you can protect your children from viewing adult websites or chat rooms.

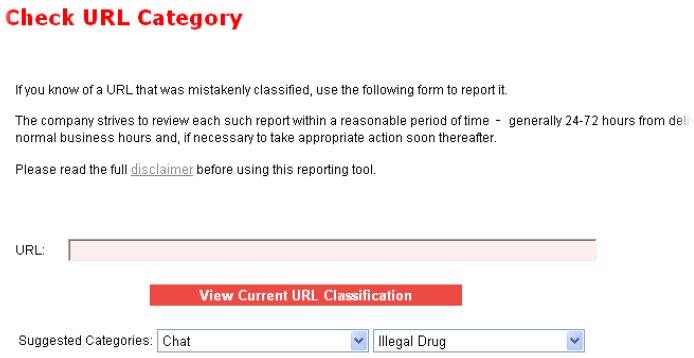
Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g.www.bbc.co.uk) will be checked against our server database. This database is updated as frequent as daily by a global team of Internet researchers. 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.

Note 1: Web Content Filter (WCF) is not a built-in service of Vigor router but a service powered by **Commtouch**. If you want to use such service (trial or formal edition), you have to perform the procedure of activation first. For the service of formal edition, please contact with your dealer/distributor for detailed information.
Note 2: Commtouch is merged by **Cyren,** and **GlobalView** services will be continued to deliver powerful cloud-based information security solutions! Refer to:
http://www.prnewswire.com/news-releases/commtouch-is-now-cyren-239025151.html

Click **CSM>>Web Content Filter** to open the following page:



Available parameters are listed below:

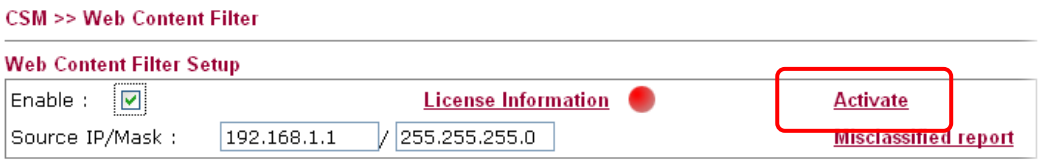
Item	Description
Enable	Check the box to enable WCF filtering function.
Source IP/Mask	Type the IP address with mask address (e.g.,192.168.1.0/255.255.255.0 to indicate a network or type 192.168.1.10/255.255.255.255 to indicate a single IP) to be filtered by WCF mechanism.
Filter Https	Check the box to enable HTTPS service.
License Information	Display the license information for current used.  CSM >> License Information License Service Provider: Commtouch License Status: enable License Url: auth.draytek.com License Start Date: 2011-02-23 License Expired Date: 2012-02-23 If the WCF mechanism has been activated successfully, a green light will be shown on the screen.  License Information / 255.255.255.0 Activate Misclassified report
Activate	Click it to activate Commtouch WCF mechanism.
Misclassified Report	You can send a report for mistaken classified URL to Commtouch by clicking such link.  Check URL Category If you know of a URL that was mistakenly classified, use the following form to report it. The company strives to review each such report within a reasonable period of time - generally 24-72 hours from deli normal business hours and, if necessary to take appropriate action soon thereafter. Please read the full disclaimer before using this reporting tool. URL: View Current URL Classification Suggested Categories: Chat Illegal Drug

How to activate web content filter?

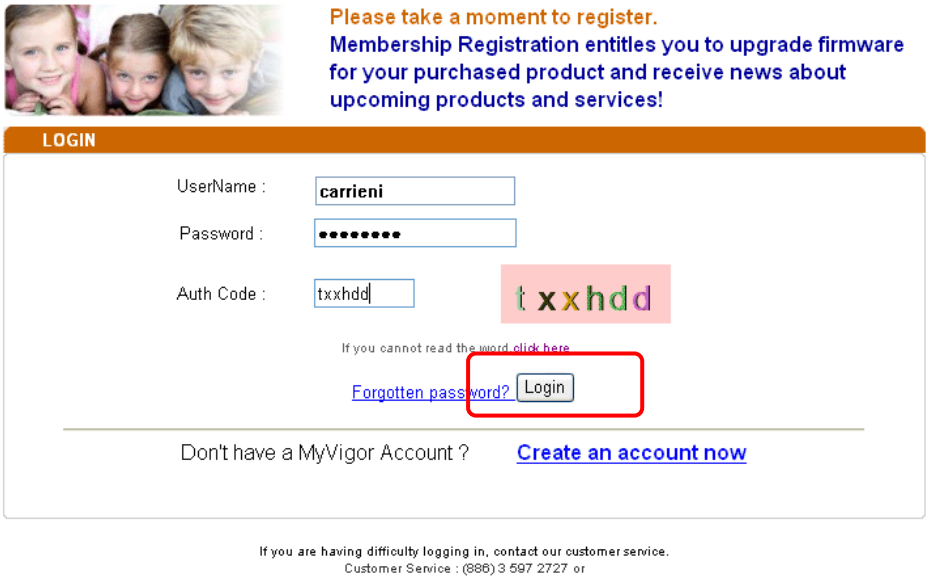
Before activating web content filter, register your Vigor router first. Refer to **2.6 Registering Vigor Router** for detailed information.

Then, follow the steps listed blow to activate WCF.

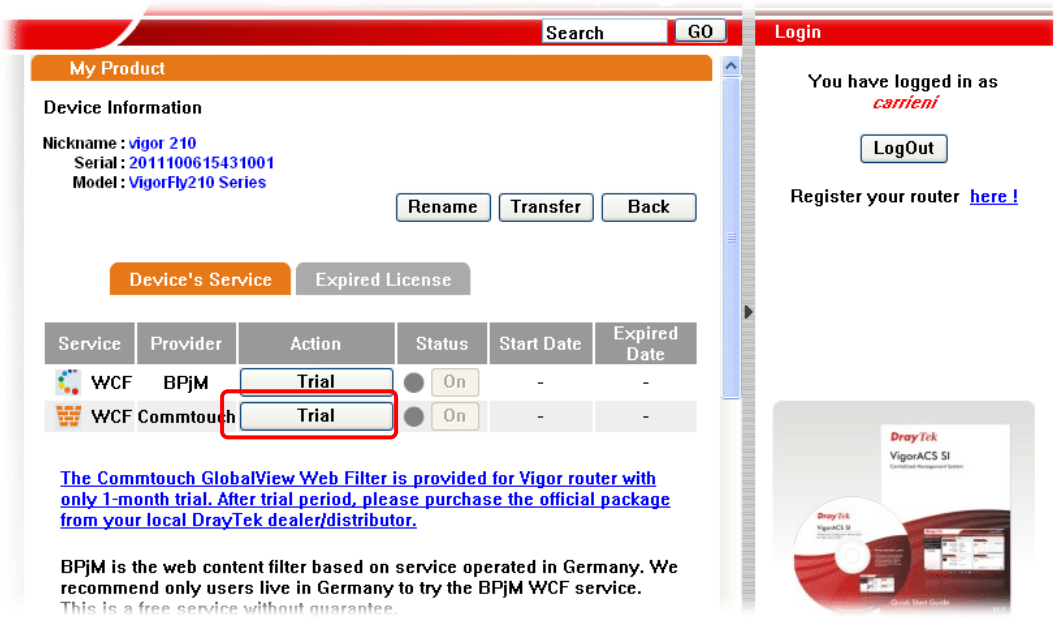
1. Click the **Activate** link from Web-Filter License to activate WCF service.



2. A **Login** page will be shown on the screen. Please type the account and password that you created previously. And click **Login**.



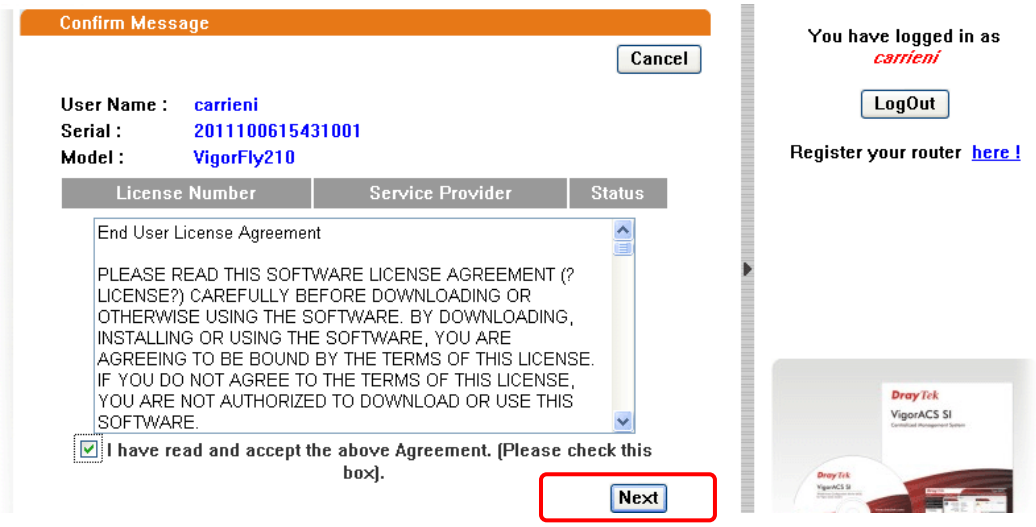
3. From the **Device's Service** section, click the **Trial** button for WCF service with provider **Commtouch**.



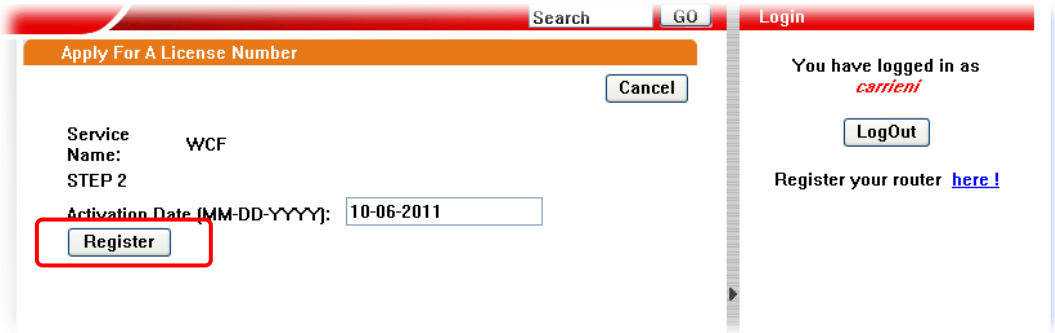
Available parameters are listed below:

Item	Description
Rename	It allows you to change the account name.
Transfer	It allows you to transfer the Vigor device together with applied license to someone who has already registered another account in myvigor.draytek.com. Be sure to press this button to transfer the product to whom you want to give. Otherwise he/she might not be able to maintain the license hooked up to the Vigor device.
Back	It allows you to return to the previous account.

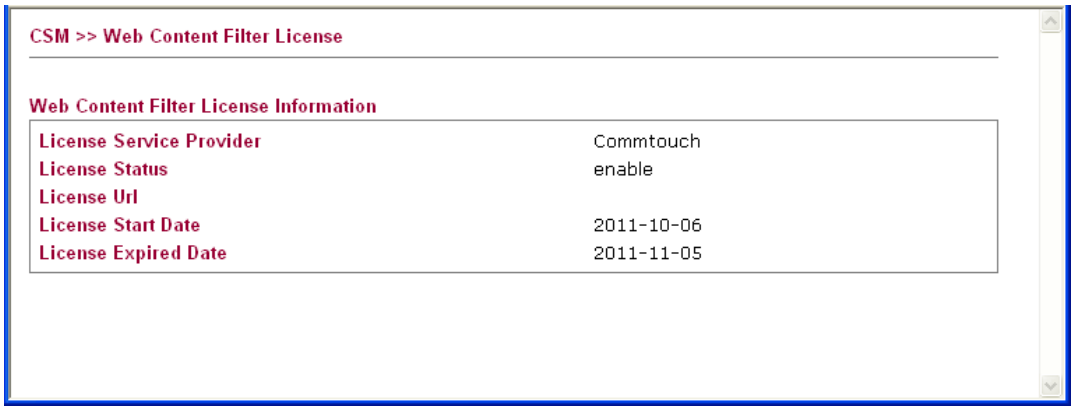
4. In the following page, check the box of "**I have read and accept the above Agreement**". The system will find out the date for you to activate this version of service. Then, click **Next**.



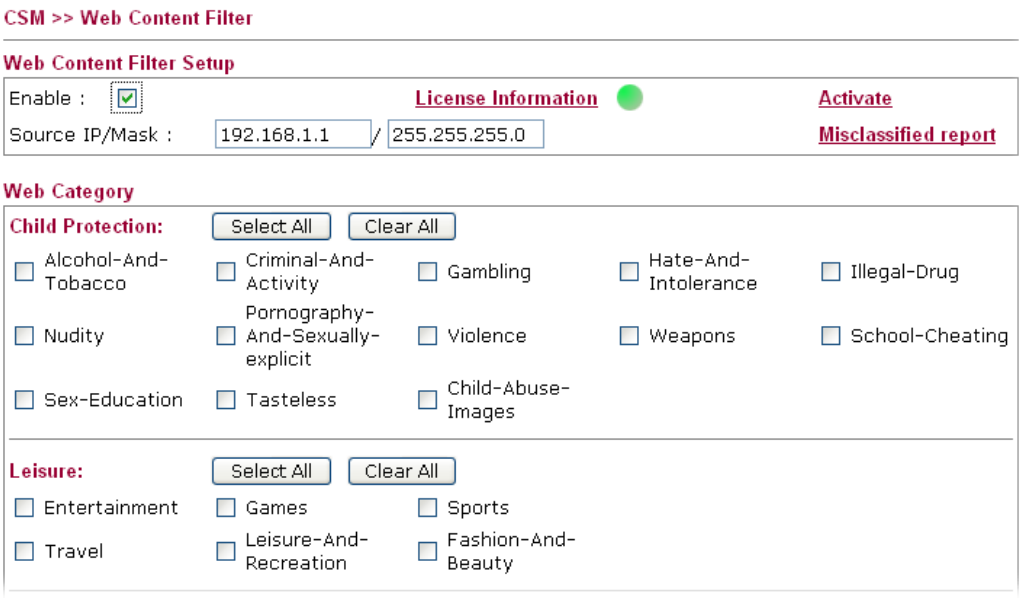
5. When this page appears, click **Register**.



6. Next, when the registration is completed. You will get the following screen.



7. Return to web configuration of VigorFly 210.
8. Refresh the page of **CSM>>Web Content Filter**.



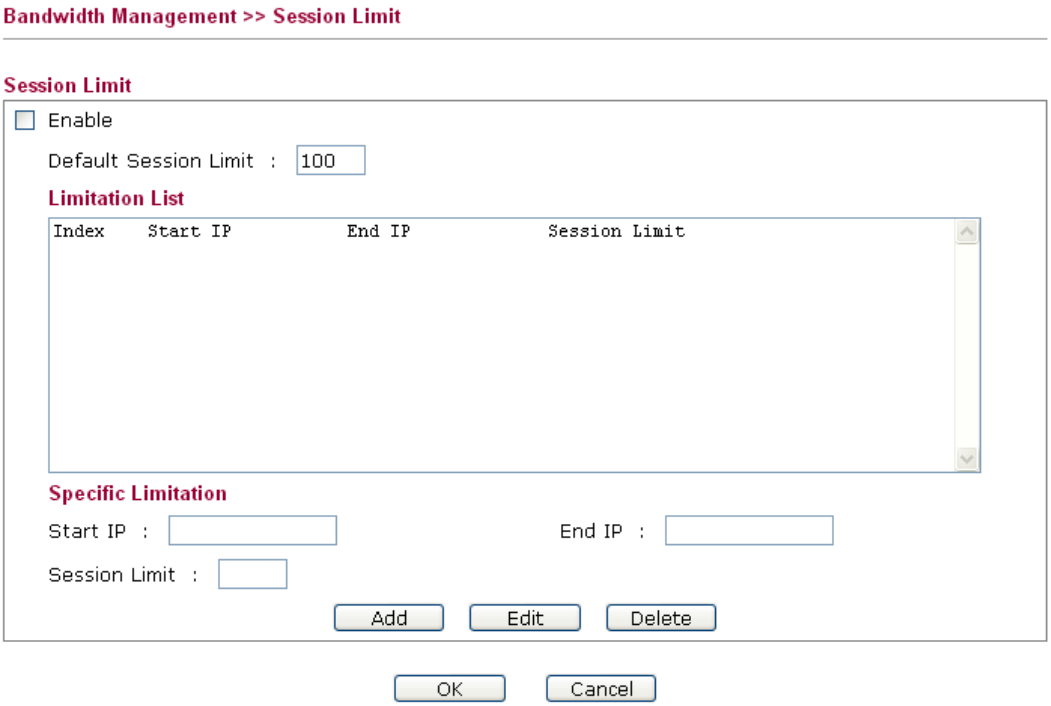
A green circle appears next to the link of License Information. It means the WCF license is valid.

3.6 Bandwidth Management

Below shows the menu items for Bandwidth Management.

3.6.1 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.



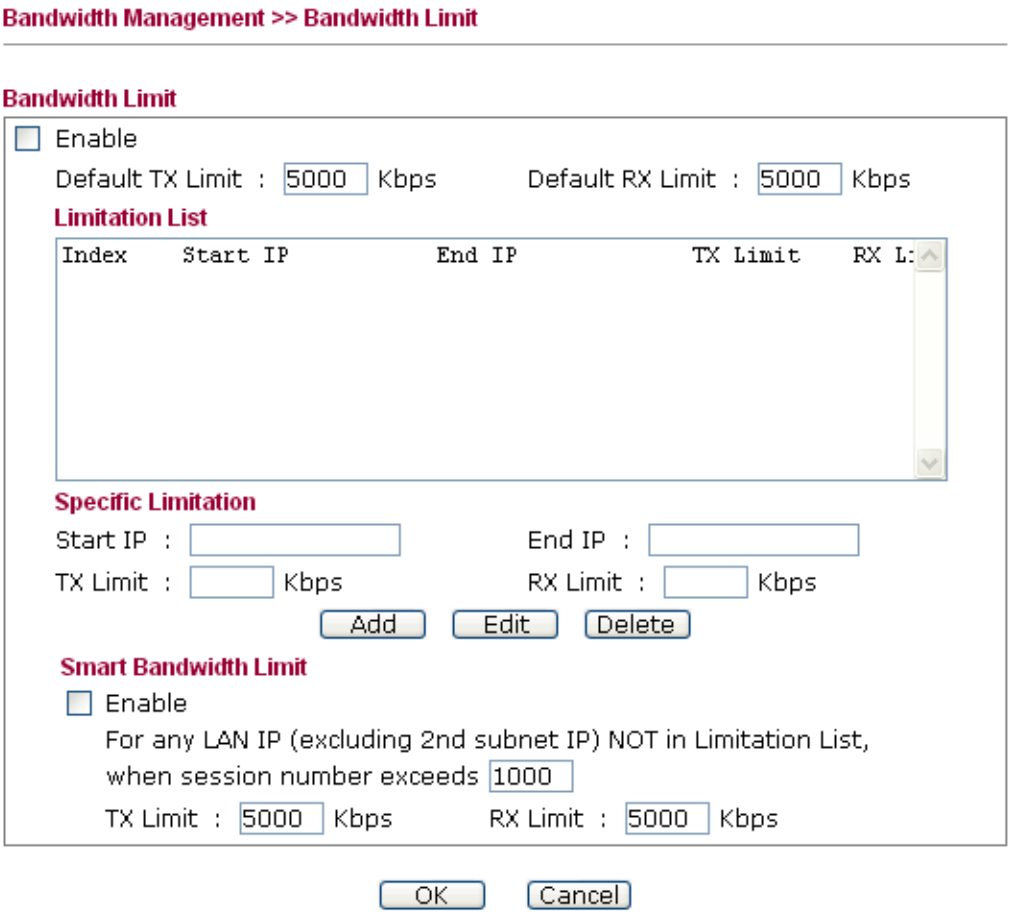
Available settings are explained as follows:

Item	Description
Session Limit	**Enable** – Check it to activate the function of limit session. **Default session limit -** Defines the default session number used for each computer in LAN.
Limitation List	Displays a list of specific limitations that you set on this web page.
Specific Limitation	**Start IP-** Defines the start IP address for limit session. **End IP -** Defines the end IP address for limit session. **Session Limit -** Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index. **Add -** Adds the specific session limitation onto the list above. **Edit -** Allows you to edit the settings for the selected limitation. **Delete -** Remove the selected settings existing on the limitation list.

After finishing all the settings, please click **OK** to save the configuration.

3.6.2 Bandwidth Limit

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Limit Bandwidth to make the bandwidth usage more efficient.



Available settings are explained as follows:

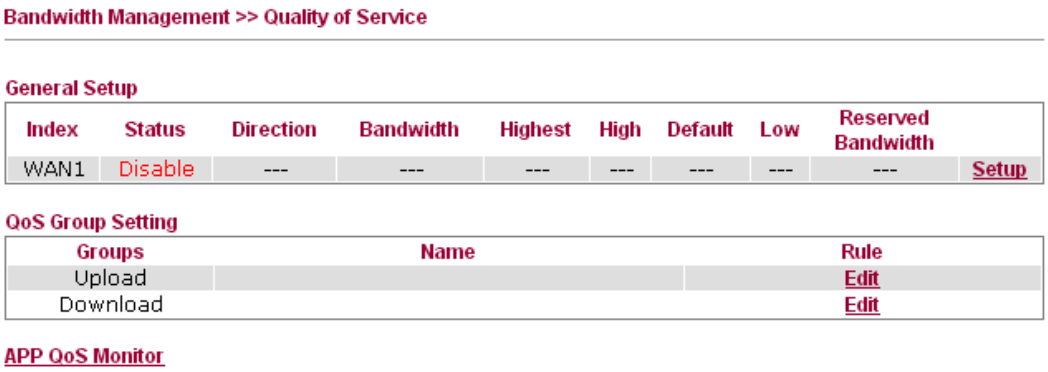
Item	Description
Bandwidth Limit	**Enable** – Check it to activate the function of limit bandwidth. **Default TX limit -** Define the default speed of the upstream for each computer in LAN. **Default RX limit -** Define the default speed of the downstream for each computer in LAN.
Limitation List	Display a list of specific limitations that you set on this web page.
Specific Limitation	**Start IP -** Define the start IP address for limit bandwidth. **End IP -** Define the end IP address for limit bandwidth. **TX limit -** Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index. **RX limit -** Define the limitation for the speed of the

	downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index. **Add -** Add the specific speed limitation onto the list above. **Edit -** Allow you to edit the settings for the selected limitation. **Delete -** Remove the selected settings existing on the limitation list.
Smart Bandwidth Limit	**Enable -** Check this box to have the bandwidth limit determined by the system automatically. **TX limit -** Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index. **RX limit -** Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.

After finishing all the settings, please click **OK** to save the configuration.

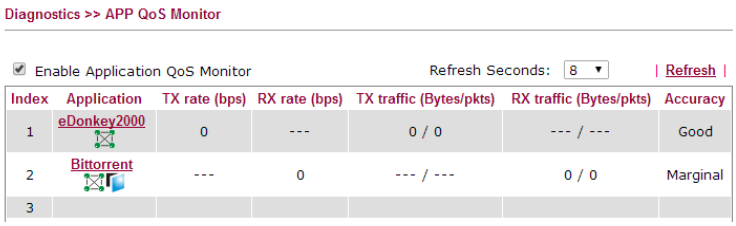
3.6.3 Quality of Service

Deploying QoS (Quality of Service) management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network.



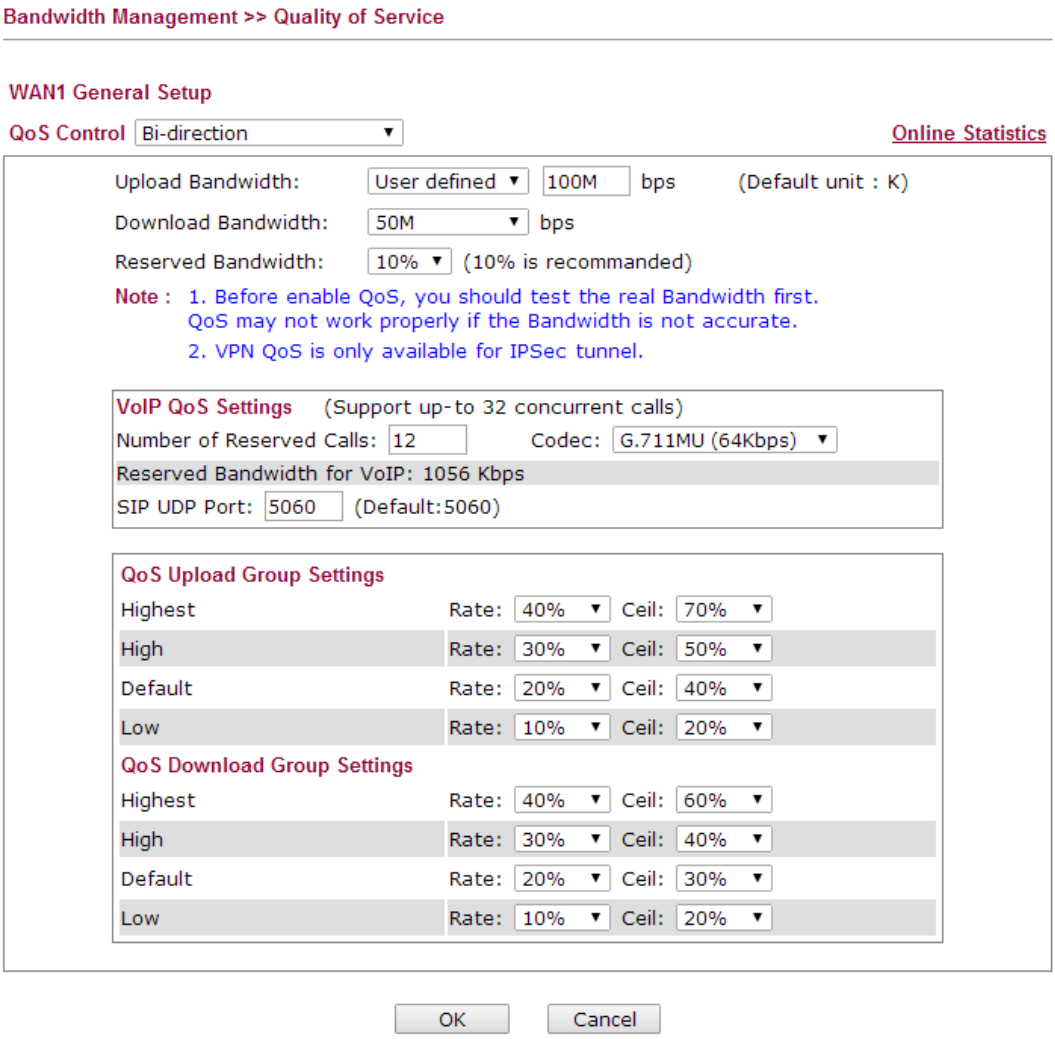
Available settings are explained as follows:

Item	Description
General Setup	**Index** – Display the WAN interface number that you can edit. **Status** – Display if the WAN interface is available for such function or not. **Direction** – Display which direction that such function will influence. **Bandwidth** – Display the inbound and outbound bandwidth setting for the WAN interface. **Highest/High/Default/Low** – Display the bandwidth

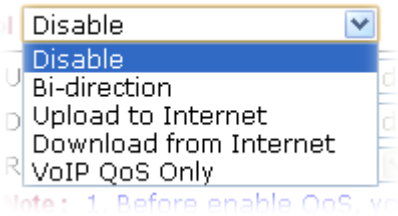
Item	Description
	percentage for each class. **Reserved Bandwidth** – Display the percentage of bandwidth reserved for the router. **Setup** – Allow to configure general QoS setting for WAN interface.
QoS Group Setting	**Group** – Display the purpose (Upload / Download) of the rule to be applied. **Name** – Display the name(s) grouped for Upload / Download. **Rule** – Allow to configure detailed settings for the selected group. Click **Edit** to access into the detailed setting page.
APP QoS Monitor	Check the box of **Enable Application QoS Monitor.** The system will monitor the application and display current status on this page periodically.  Diagnostics >> APP QoS Monitor ☑ Enable Application QoS Monitor Refresh Seconds: 8 | Refresh | Index / Application / TX rate (bps) / RX rate (bps) / TX traffic (Bytes/pkts) / RX traffic (Bytes/pkts) / Accuracy 1 / eDonkey2000 / 0 / --- / 0 / 0 / --- / --- / Good 2 / Bittorrent / --- / 0 / --- / --- / 0 / 0 / Marginal 3

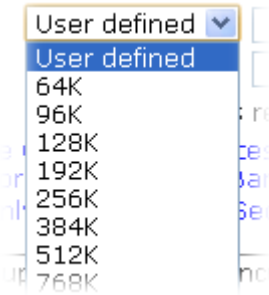
General Setup for WAN Interface

When you click **Setup**, you can configure the bandwidth ratio for QoS of the WAN interface.



Available settings are explained as follows:

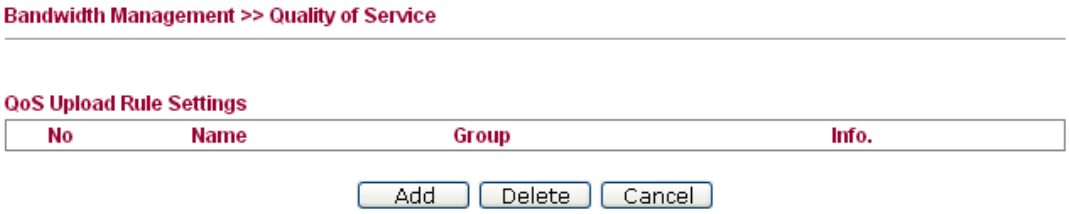
Item	Description
QoS Control	There are four classes of QoS offered by Vigor router. Each class contains different settings. Here we take **Bi-direction** as an example. Related settings will be explained below. 
Upload Bandwidth	It will be applied to outgoing traffic. Use the drop down list to specify the bandwidth for data transmission. If you choose **User defined**, you have to type the value manually.

	
Download Bandwidth	It will be applied to incoming traffic. Use the drop down list to specify the bandwidth for data receiving. If you choose **User defined**, you have to type the value manually.
Reserved Bandwidth	Such percentage of bandwidth is reserved for the usage of the router only.
VoIP QoS Settings	**Number of Reserved Calls** – Type the number of the VoIP calls that QoS configuration would apply to. **Codec** – Select one of five codecs as the default for your VoIP calls. The codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality. If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711. **SIP UDP Port** – Set a port number used for SIP.
QoS Upload Group Settings	There are four classes of Highest, High, Normal and Low which represent the priority of data transmission. **Rate** – Define the transmission/receiving percentage of upload/download bandwidth for each class. **Ceil** – It determines the largest bandwidth that each class (highest, high, default, low) can utilize. That is, if there is no class with higher priority occupies the bandwidth, others with lower priority can use the remained bandwidth.
QoS Download Group Settings	Highest, High, Normal and Low represent the priority for data receiving. **Rate** – Define the transmission/receiving rate respectively under different levels. **Ceil** –It determines the largest bandwidth that each class (highest, high, default, low) can utilize. That is, if there is no class with higher priority occupies the bandwidth, others with lower priority can use the remained bandwidth.

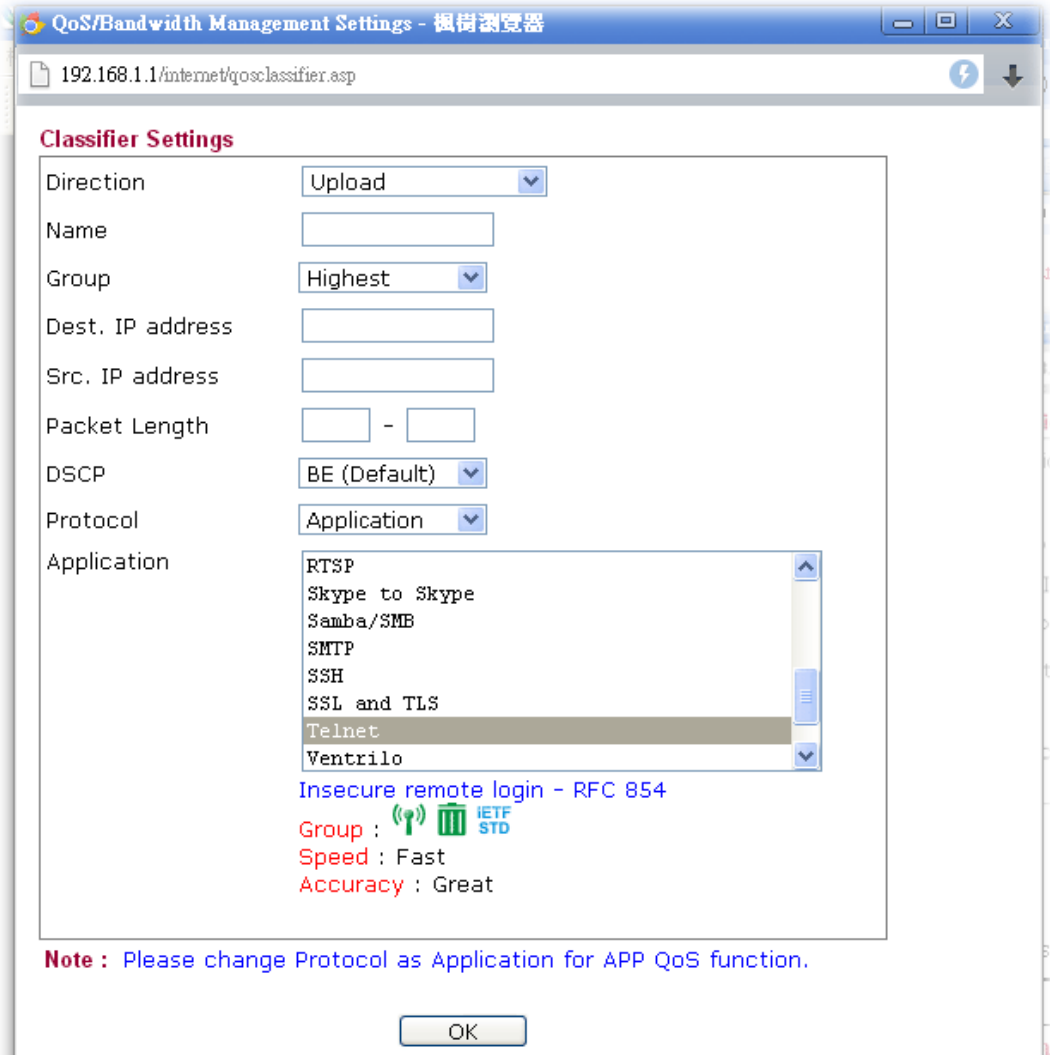
After finishing all the settings, please click **OK** to save the configuration.

Edit the QoS Rule

QoS Rule is allowed you to specify certain conditions for data Upload and Download. After clicking the **Edit** link under **Rule**, you will get the following web page.

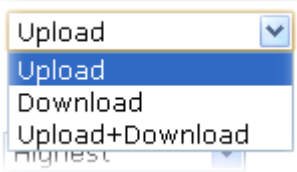
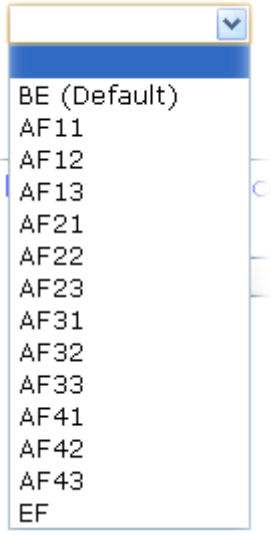
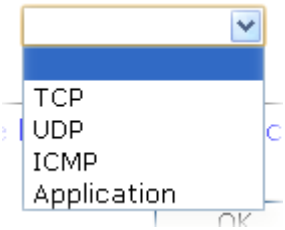


To configure the detailed settings for the rule, click **Add** to open the following dialog.



Available settings are explained as follows:

Item	Description
Direction	Choose Upload or Download that such function will influence.

	 **Download -** apply to incoming traffic only. **Upload -** apply to outgoing traffic only. **Upload+Download -** apply to both incoming and outgoing traffic.
Name	Define the name of such rule.
Group	Determine the priority of such rule.
Dest. IP address	Type the destination IP address influenced by such rule.
Src. IP address	Type the source IP address influenced by such rule.
Packet Length	Specify the length of the packets. The adjustable range is from 0 ~2048.
DSCP	DSCP (Differentiated Services Code Point) allows each IP packet to be tagged with different service class for different network transmission. The default setting is "BE". 
Protocol	Specify the protocol for such QoS rule. 
Dest. Port/Src. Port	It is available when TCP or UDP is selected as the protocol.
Application	It is available when Application is selected as the protocol. At present, there are eight applications which can be selected for APP QoS management. The usage of APP QoS can be seen by clicking **APP QoS**

	Monitor link.

After finished settings, click **OK** to save the settings. The new rule setting profile will be added and displayed on the page. Below shows the QoS rule example for your reference:

Bandwidth Management >> Quality of Service

QoS Upload Rule Settings

No	Name	Group	Info.
1 ☐	9001	Highest	Protocol: TCP Dest. port: 9001
2 ☐	9002	High	Protocol: TCP Dest. port: 9002
3 ☐	9003	Default	Protocol: TCP Dest. port: 9003
4 ☐	9004	Low	Protocol: TCP Dest. port: 9004

Add Delete Cancel

In the QoS Group Setting page, you will see:

Bandwidth Management >> Quality of Service

General Setup

Index	Status	Direction	Bandwidth	Highest	High	Default	Low	Reserved Bandwidth	
WAN1	Disable	---	---	---	---	---	---	---	Setup

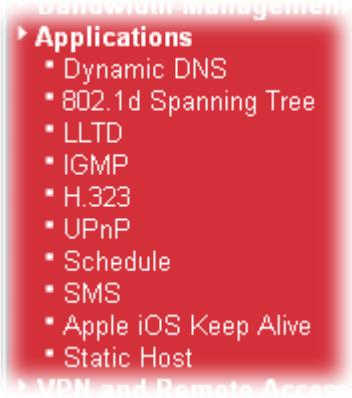
QoS Group Setting

Groups	Name	Rule
Upload	9001,9002,9003,9004	Edit
Download		Edit

APP QoS Monitor

3.7 Applications

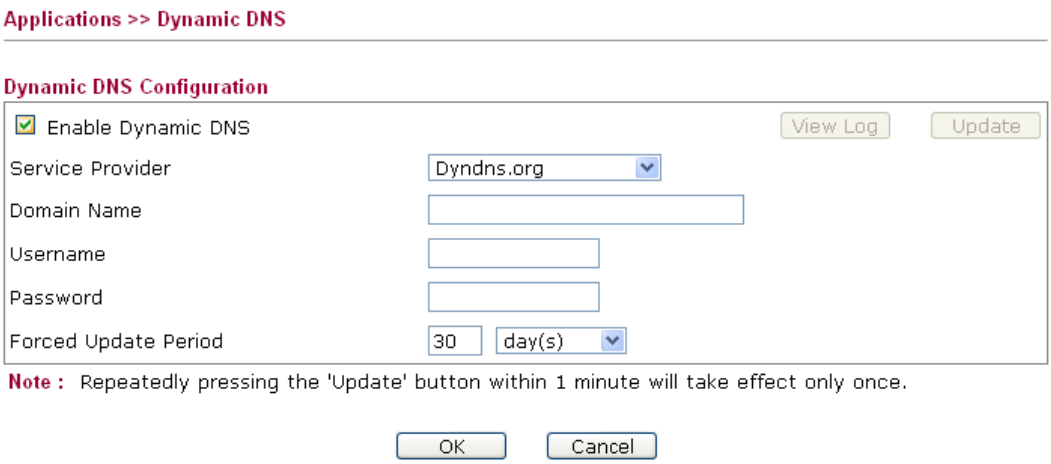
Below shows the menu items for Applications.



3.7.1 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.



Available parameters are listed below:

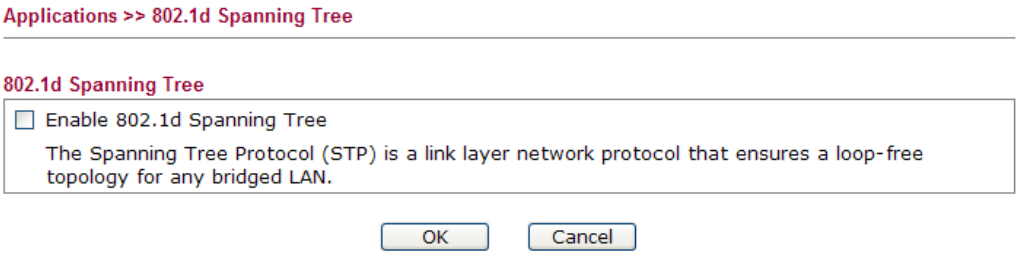
Item	Description
Enable Dynamic DNS	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
Service Provider	Select the service provider for the DDNS account.

	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.
Forced Update Period	Select a time interval for updating from the NTP server.

After finishing all the settings here, please click **OK** to save the configuration.

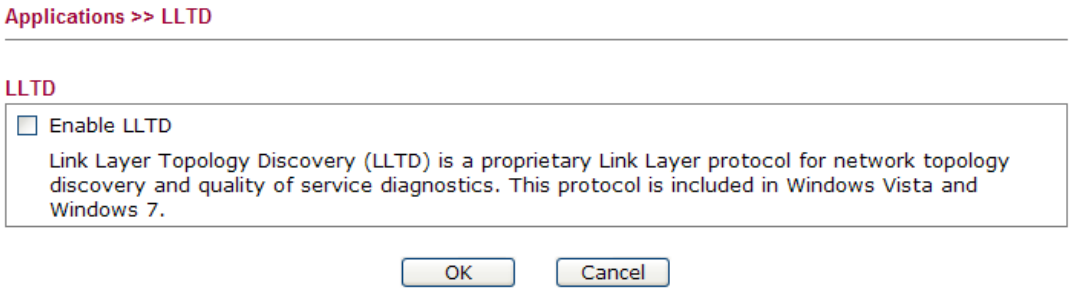
3.7.2 802.1d Spanning Tree

The Spanning Tree Protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN. Check the box to invoke such feature and click **OK** to save it.



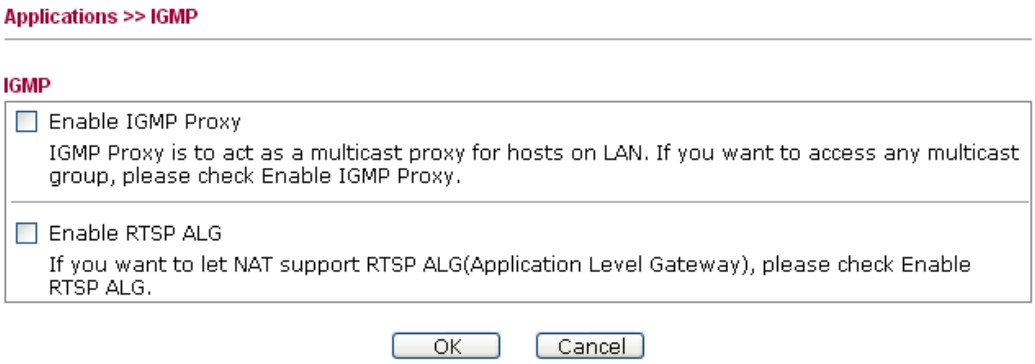
3.7.3 LLTD

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. Check the box to invoke such feature and click **OK** to save it.



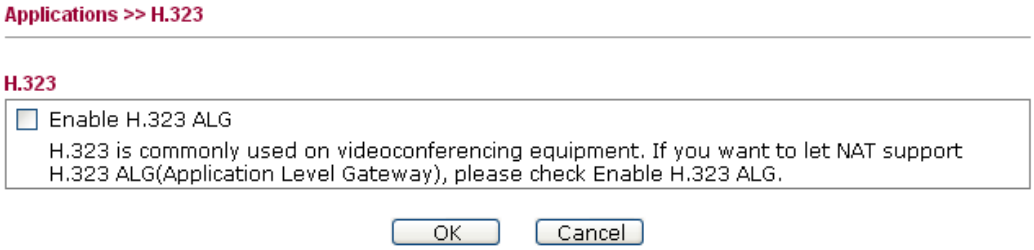
3.7.4 IGMP

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. Check the box to invoke such feature and click **OK** to save it.



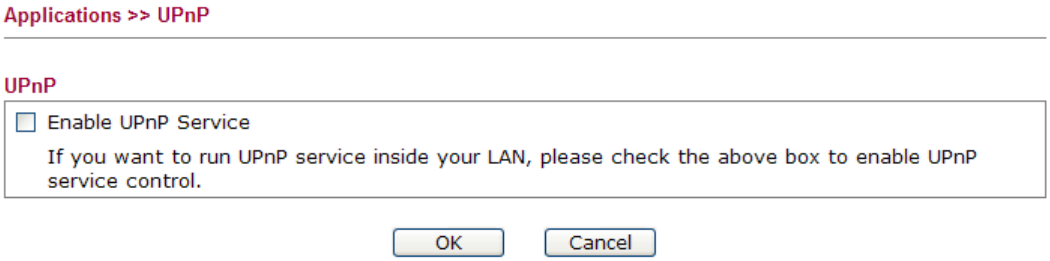
3.7.5 H.323

The H.323 ALG allows incoming and outgoing VoIP calls passing through NAT. If required, check the box and click **OK** to save the settings.



3.7.6 UPnP

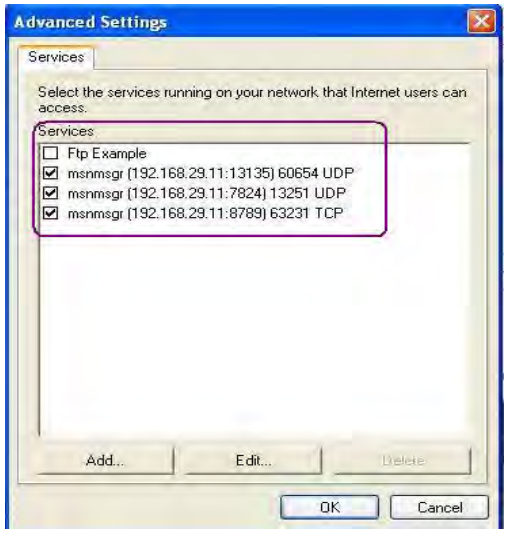
The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on 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.

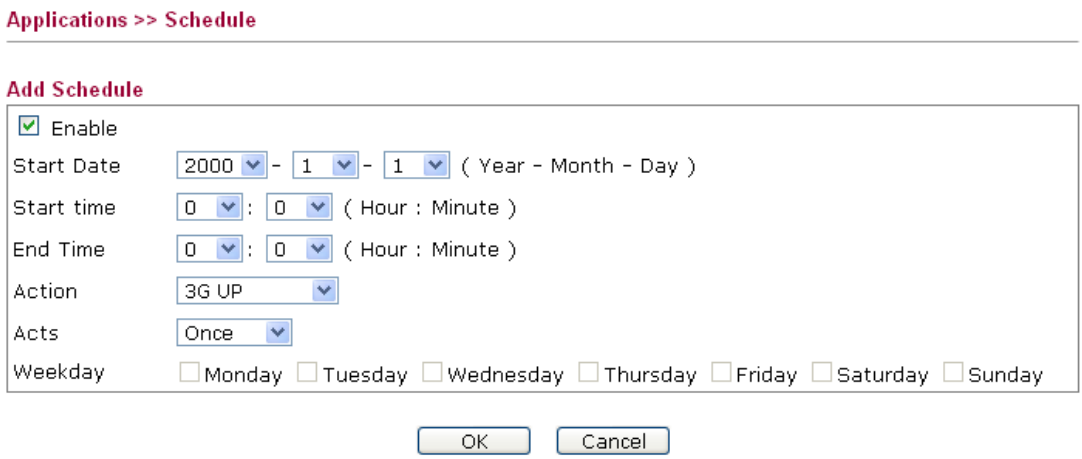
3.7.7 Schedule

The Vigor router has a built-in real time clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the router to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule is also applicable to other functions.

You have to set your time before set schedule. In **System Maintenance>> Time and Date** menu, press **Inquire Time** button to set the Vigor router's clock to current time of your PC. The clock will reset once if you power down or reset the router. There is another way to set up time. You can inquiry an NTP server (a time server) on the Internet to synchronize the router's clock. This method can only be applied when the WAN connection has been built up.

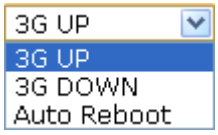
You can set up to 15 schedules.

To add a schedule, please click any index, say Index No. 1. The detailed settings of the call schedule with index 1 are shown below.



Available settings are explained as follows:

Item	Description
Enable	Check to enable the schedule.
Start Date	Specify the starting date of the schedule.
Start Time	Specify the starting time of the schedule.
End Time	Specify the ending time of the schedule.

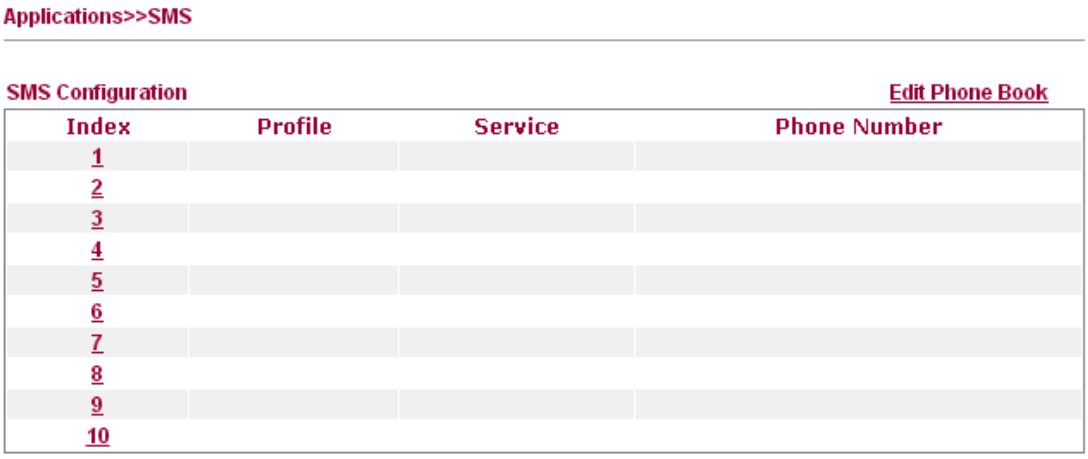
Item	Description
Action	Specify which action Call Schedule should apply during the period of the schedule. **3G UP -**Force the 3G connection to be always on. **3G Down -**Force the 3G connection to be always down. **Auto Reboot –** The vigor system will reboot automatically according to such schedule profile. 
Acts	Specify the duration (or period) for the schedule. **Once -**The schedule will be applied just once. **Routine -**Specify which days in one week should perform the schedule.

After finishing all the settings here, please click **OK** to save the configuration.

3.7.8 SMS

The function of SMS (Short Message Service) is that Vigor router sends a message to user's mobile or e-mail box through specified service provider to assist the user knowing the real-time abnormal situations or sending message to the user when backup WAN (WAN2) is on.

Vigor router allows you to set up to **10** SMS profiles which will be sent out according to different conditions.



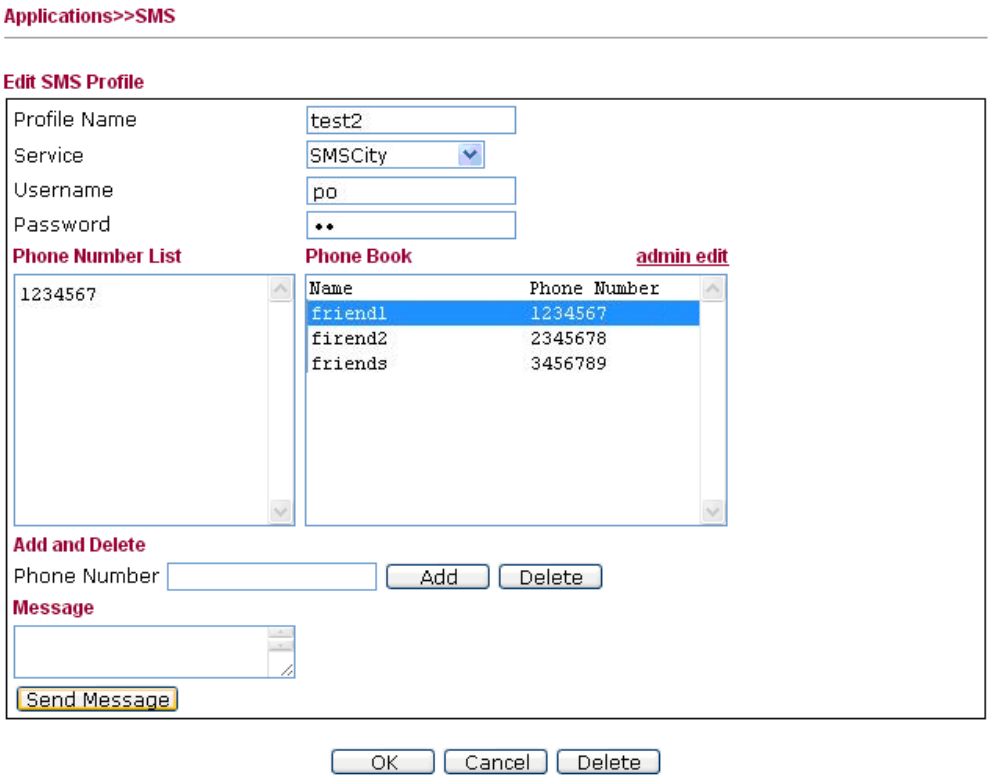
Each item will be explained as follows:

Item	Description
Edit Phone Book	Click it to open the phone book for modification.
Index	Display the index number (from 1 to 10) of the profile. Click the index number link to modify the selected profile.
Profile	Display the name of the profile.

Service	Display the name of the SMS provider.
Phone Number	Display the one who will receive the SMS.

To edit the SMS service profile:

1. Open **Applications>> SMS.**
2. Click one of the index numbers.
3. The following page will appear.



Available parameters are listed as follows:

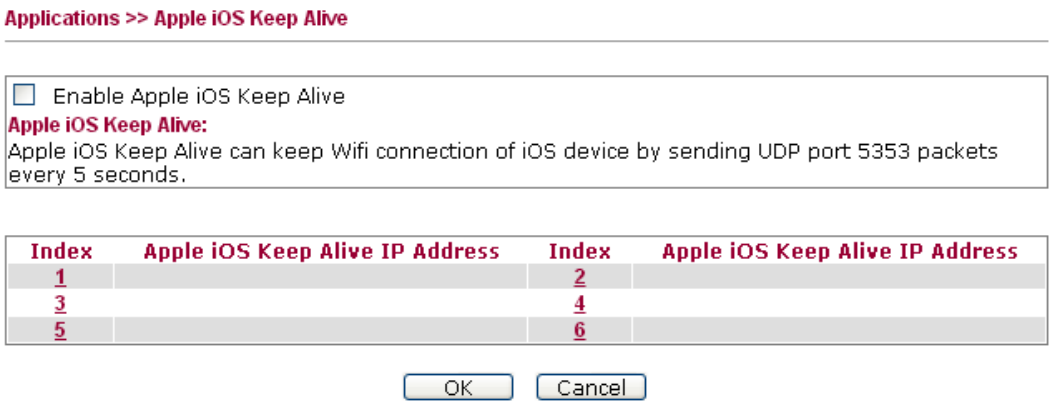
Item	Description
Profile Name	Type a name for such profile.
Service	Choose the SMS provider object profile from the drop down list.
Username	Type a user name that the sender can use to register to selected SMS provider. The maximum length of the name you can set is 31 characters.
Password	Type a password that the sender can use to register to selected SMS provider. The maximum length of the password you can set is 31 characters.
Phone Number List	Display the phone number created by clicking **Add**. The phone number displayed here will receive the message when such profile is selected for the access mode of **3G/4G USB Modem (PPP Mode)** under **WAN>>Internet Access**

	of WAN2.
Phone Book	Display all of the created names and phone numbers. When you double click on one of the existed names, the phone number related to that name will be selected and displayed on **Phone Number List**.
Admin edit	Click it to add new name with phone number. The result will be displayed on the **Phone Book** area.
Add and Delete	**Phone Number** – Type a phone number who will receive the SMS. **Add** – Click it to add the phone number. It will be displayed on the Phone Number List. **Delete** – Click it to remove the selected phone number that you don't want.
Message	Type the content of the SMS. **Send Message –** Click it to send a test message to the specified phone number.
OK	Click it to save the configuration and exit the page.
Cancel	Click it to return to the previous page without saving the configuration.
Delete	Delete current profile with the settings configuration.

4. Enter all the settings and click **OK**.

3.7.9 Apple iOS Keep Alive

To keep the wireless connection (via Wi-Fi) on iOS device in alive, VigorAP 710 will send the UDP packets with 5353 port to the specific IP every five seconds.



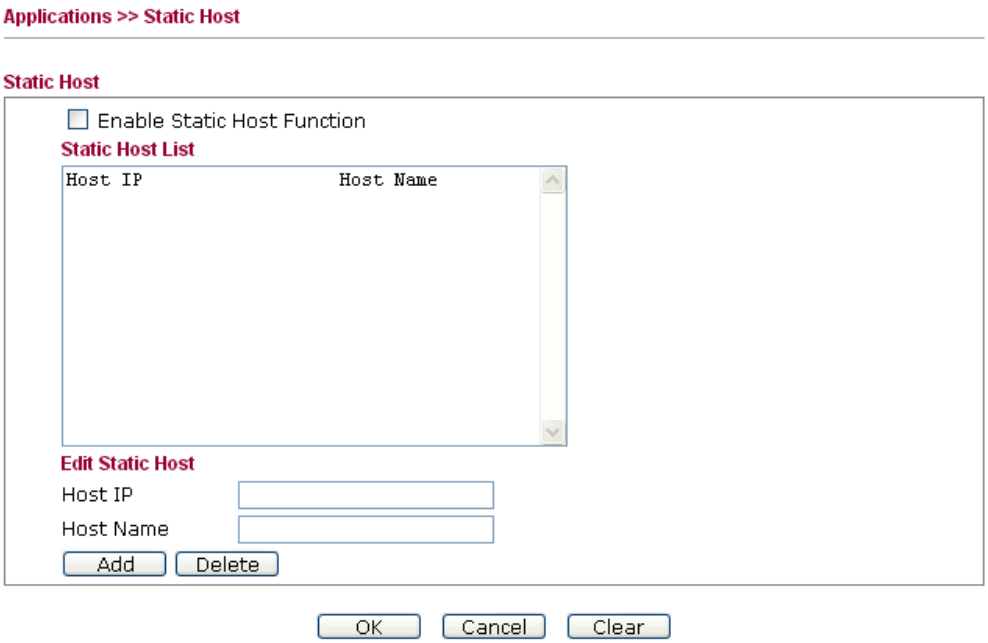
Available settings are explained as follows:

Item	Description
Enable Apple iOS Keep Alive	Check to enable the function.
Index	Display the setting link. Click the index link to open the configuration page for setting the IP address.

Item	Description
Apple iOS Keep Alive IP Address	Display the IP address.

3.7.10 Static Host

The host name on the list will be transferred into the IP address specified for that host.



Available settings are explained as follows:

Item	Description
Enable Static Host Function	Check the box to enable such function.
Static Host List	Display a list of the static hosts created.
Edit Static Host	**Host IP** – Type the IP address of the host that you want to add as a static host. **Host Name** – Type the name of the host. **Add** – Click it to add the new typed host IP with host name and display on the Static Host List. **Delete** – Remove the selected static host.
OK	Click it to save the configuration.
Cancel	Click it to discard the configuration.

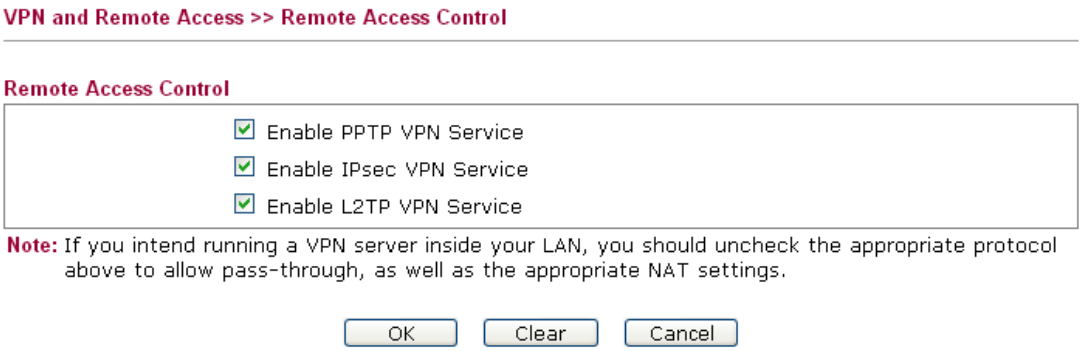
3.8 VPN and Remote Access

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

Below shows the menu items for VPN and Remote Access.

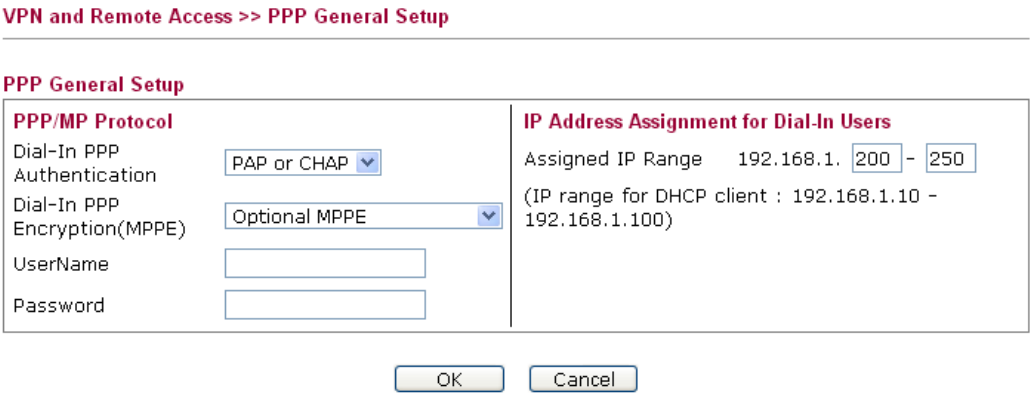
3.8.1 Remote Access Control

Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port.

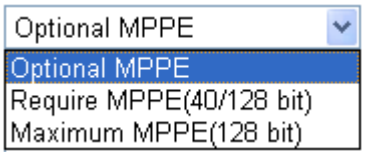


3.8.2 PPP General Setup

This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPSec.



Available settings are explained as follows:

Item	Description
Dial-In PPP Authentication	**PAP Only** - Select this option to force the router to authenticate dial-in users with the PAP protocol. **PAP or CHAP** - Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.
Dial-In PPP Encryption (MPPE)	This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data.  **Require MPPE (40/128bits) -** Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data. **Maximum MPPE -** This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.
UserName and **Password**	The mutual authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the **User Name** and **Password** of the mutual authentication peer.
IP Address Assignment for Dial-In Users	Enter a range of IP addresses for the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 as the Start IP Address.

3.8.3 IPSec General Setup

In **IPSec General Setup,** there are two major parts of configuration.

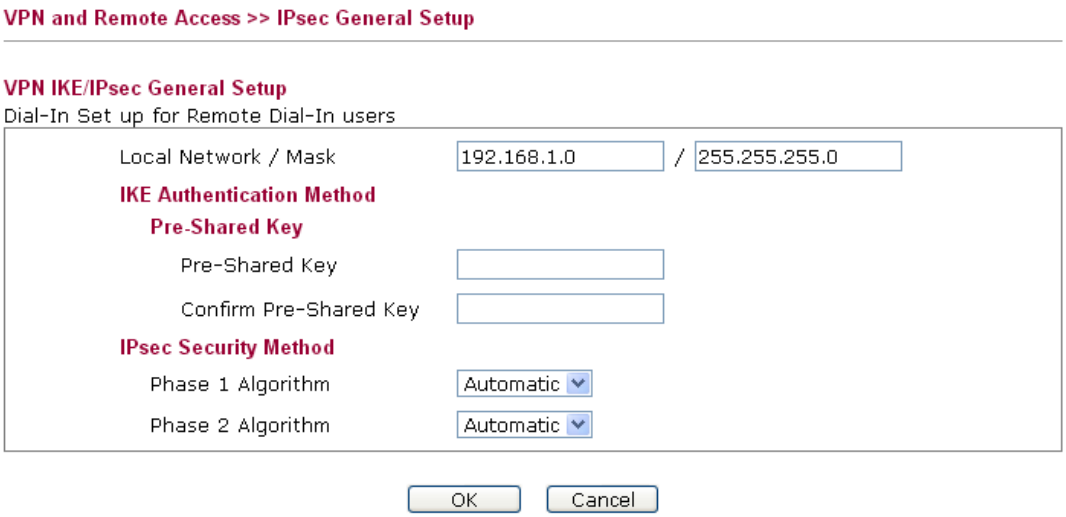
There are two phases of IPSec.

- Phase 1: negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using a Pre-Shared Key. The peer that starts the negotiation proposes all its policies to the remote peer and then remote peer tries to find a highest-priority match with its policies. Eventually to set up a secure tunnel for IKE Phase 2.
- Phase 2: negotiation IPSec security methods including Authentication Header (AH) or Encapsulating Security Payload (ESP) for the following IKE exchange and mutual examination of the secure tunnel establishment.

There are two encapsulation methods used in IPSec, **Transport** and **Tunnel**. The **Transport** mode will add the AH/ESP payload and use original IP header to encapsulate the data payload only. It can just apply to local packet, e.g., L2TP over IPSec. The **Tunnel** mode will not only add the AH/ESP payload but also use a new IP header (Tunneled IP header) to encapsulate the whole original IP packet.

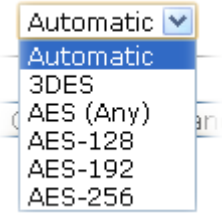
Authentication Header (AH) provides data authentication and integrity for IP packets passed between VPN peers. This is achieved by a keyed one-way hash function to the packet to create a message digest. This digest will be put in the AH and transmitted along with packets. On the receiving side, the peer will perform the same one-way hash on the packet and compare the value with the one in the AH it receives.

Encapsulating Security Payload (ESP) is a security protocol that provides data confidentiality and protection with optional authentication and replay detection service.



Available settings are explained as follows:

Item	Description
Local Network/Mask	Type the IP address with subnet mask of the host.
IKE Authentication Method	This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec and IPSec tunnel. **Pre-Shared Key-** Specify a key for IKE authentication.

	Confirm Pre-Shared Key- Retype the characters to confirm the pre-shared key.
IPSec Security Method	Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Triple DES (3DES) and AES. 

After finishing all the settings here, please click **OK** to save the configuration.

3.8.4 Remote Dial-in User

You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection. You may set parameters including specified connection peer ID, connection type (VPN connection - including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

The router provides **32** access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function. The following figure shows the summary table.

VPN and Remote Access >> Remote Dial-In User

Remote Access User Accounts

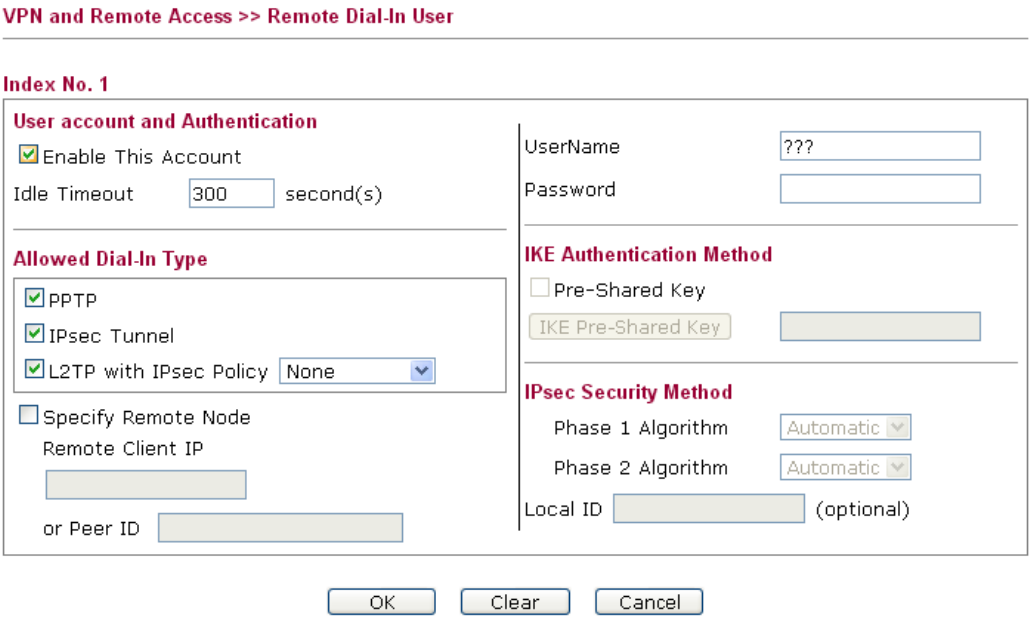
Index	User	Status	Index	User	Status
1	???	×	17	???	×
2	???	×	18	???	×
3	???	×	19	???	×
4	???	×	20	???	×
5	???	×	21	???	×
6	???	×	22	???	×
7	???	×	23	???	×
8	???	×	24	???	×
9	???	×	25	???	×
10	???	×	26	???	×
11	???	×	27	???	×
12	???	×	28	???	×
13	???	×	29	???	×
14	???	×	30	???	×
15	???	×	31	???	×
16	???	×	32	???	×

Each item is explained as follows:

Item	Description
Index	Click the number below Index to access into the setting page of Remote Dial-in User.

User	Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.
Status	Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.

Click each index to edit one remote user profile. **Each Dial-In Type requires you to fill the different corresponding fields on the right.** If the fields gray out, it means you may leave it untouched. The following explanation will guide you to fill all the necessary fields.



Available settings are explained as follows:

Item	Description
User account and Authentication	**Enable this account** - Check the box to enable this function. **Idle Timeout-** If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.
Allowed Dial-In Type	**PPTP** - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below. **IPSec Tunnel** - Allow the remote dial-in user to make an IPSec VPN connection through Internet. **L2TP with IPSec Policy** - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: ● **None -** Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. ● **Nice to Have -** Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in

Item	Description
	VPN connection becomes one pure L2TP connection. ● **Must -**Specify the IPSec policy to be definitely applied on the L2TP connection. **Specify Remote Node** **Check the checkbox-**You can specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode). **Uncheck the checkbox-**This means the connection type you select above will apply the authentication methods and security methods in the **general settings**. **User Name -** This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The maximum length for username is 19 characters. **Password -** This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The maximum length for password is 19 characters.
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. **Pre-Shared Key -** Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. **Phase 1/2 Algorithm -** It means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Triple DES (3DES) and AES. **Local ID (optional) -** Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.

3.8.5 LAN to LAN

Here you can manage LAN-to-LAN connections by maintaining a table of connection profiles. You may set parameters including specified connection direction (dial-in or dial-out), connection peer ID, connection type (VPN connection - including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

The router supports 2 VPN tunnels and provides up to **32** profiles simultaneously. The following figure shows the summary table.

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profile

Index	Name	Status	Index	Name	Status
1	???	X	17	???	X
2	???	X	18	???	X
3	???	X	19	???	X
4	???	X	20	???	X
5	???	X	21	???	X
6	???	X	22	???	X
7	???	X	23	???	X
8	???	X	24	???	X
9	???	X	25	???	X
10	???	X	26	???	X
11	???	X	27	???	X
12	???	X	28	???	X
13	???	X	29	???	X
14	???	X	30	???	X
15	???	X	31	???	X
16	???	X	32	???	X

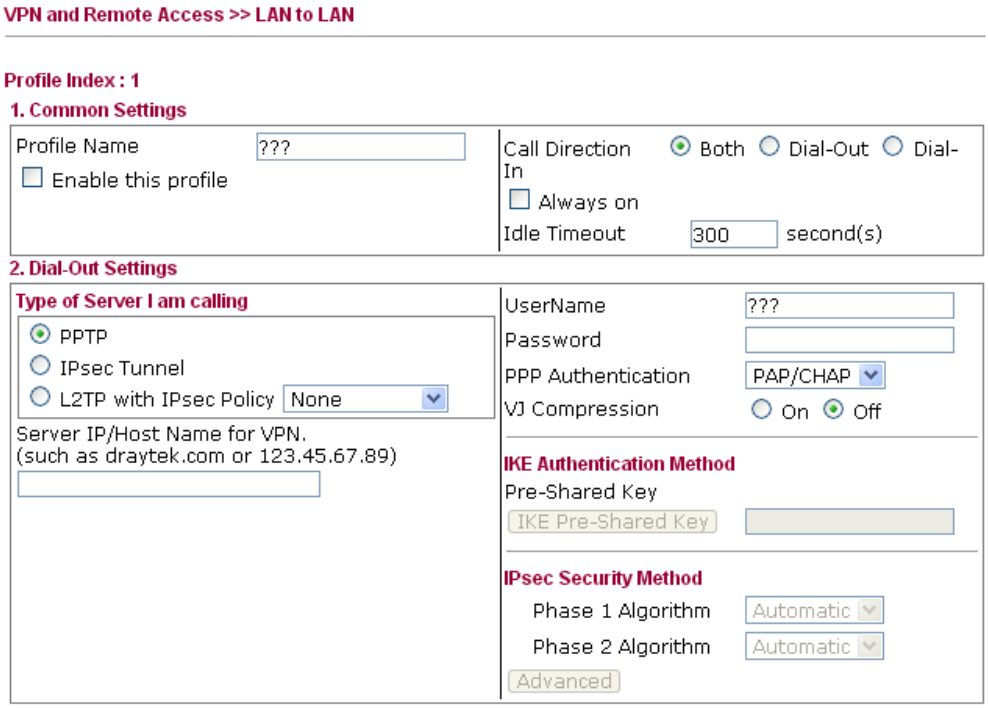
Each item is explained as follows:

Item	Description
Name	Indicate the name of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.
Status	Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

To edit each profile:

1. Click each index to edit each profile and you will get the following page. Each LAN-to-LAN profile includes 4 subgroups. If the fields gray out, it means you may leave it untouched. The following explanations will guide you to fill all the necessary fields.

   For the web page is too long, we divide the page into several sections for explanation.



Available settings are explained as follows:

Item	Description
Common Settings	**Profile Name -** Specify a name for the profile of the LAN-to-LAN connection. **Enable this profile -** Check here to activate this profile. **Call Direction -** Specify the allowed call direction of this LAN-to-LAN profile. ● **Both**:-initiator/responder ● **Dial-Out**- initiator only ● **Dial-In**- responder only. **Always On**-Check to enable router always keep VPN connection. **Idle Timeout:** The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.
Dial-Out Settings	**Type of Server I am calling –** **PPTP** - Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server. **IPSec Tunnel** - Build an IPSec VPN connection to the server through Internet. **L2TP with IPSec Policy -** Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: ● **None:** Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. ● **Nice to Have:** Apply the IPSec policy first, if it is

applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection.

- **Must:** Specify the IPSec policy to be definitely applied on the L2TP connection.

User Name - This field is applicable when you select, PPTP or L2TP with or without IPSec policy above. The maximum length for username is 49 characters.

Password - This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The maximum length for password is 15 characters.

PPP Authentication - This field is applicable when you select, PPTP or L2TP with or without IPSec policy above. PAP/CHAP is the most common selection due to wild compatibility.

VJ compression - This field is applicable when you select PPTP or L2TP with or without IPSec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to **Yes** to improve bandwidth utilization.

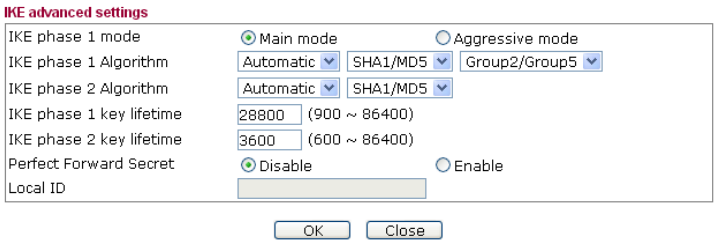
IKE Authentication Method - This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy.

- **Pre-Shared Key** - Input 1-63 characters as pre-shared key.

IPSec Security Method - This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.

Advanced - Specify mode, proposal and key life of each IKE phase, Gateway, etc.

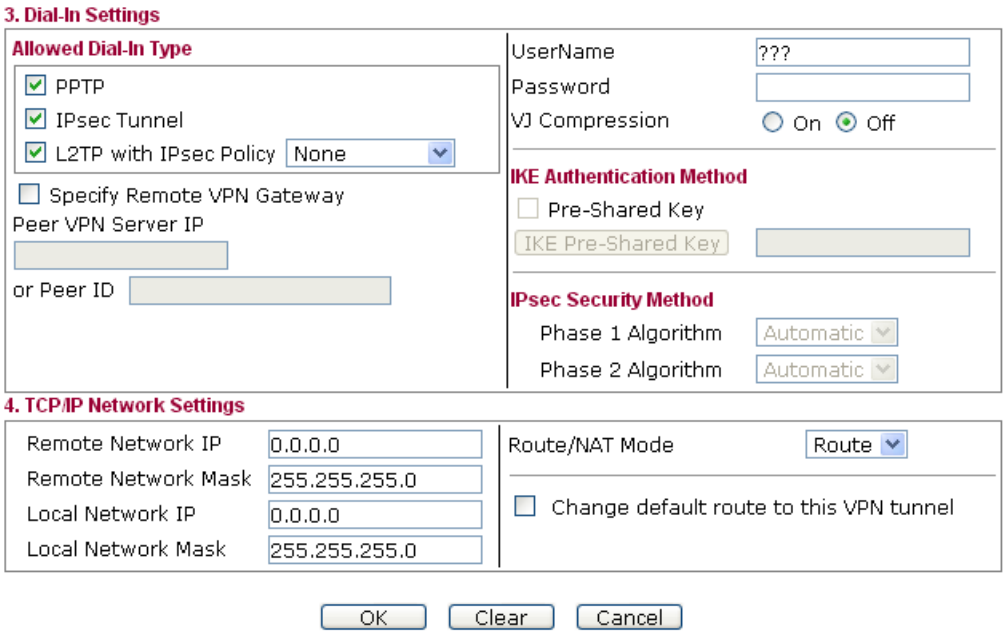
The window of advance setup is shown as below:



IKE phase 1 mode -Select from **Main** mode and **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPSec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode.

- **IKE phase 1 mode-**To propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match. Two combinations are available for Aggressive mode and nine for **Main** mode. We suggest you select the combination that covers the most schemes.
- **IKE phase 1 Algorithm** and **IKE phase 2 Algorithm -**To propose the local available algorithms to the VPN peers, and get its feedback to find a match. Three

	combinations are available for both modes. We suggest you select the combination that covers the most algorithms. ● **IKE phase 1 key lifetime**-For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds. ● **IKE phase 2 key lifetime**-For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds. ● **Local ID**-In **Aggressive** mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.



Available settings are explained as follows:

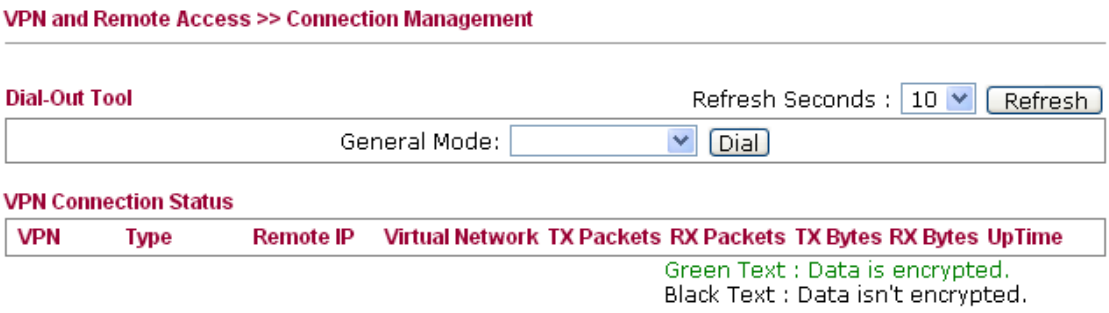
Item	Description
Allowed Dial-In Type	Determine the dial-in connection with different types. **PPTP -** Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below. **IPSec Tunnel-** Allow the remote dial-in user to trigger an IPSec VPN connection through Internet. **L2TP with IPSec Policy -** Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: ● **None -** Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. ● **Nice to Have -** Apply the IPSec policy first, if it is

	applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. ● **Must -** Specify the IPSec policy to be definitely applied on the L2TP connection. **Specify Remote VPN Gateway -** You can specify the IP address of the remote dial-in user or peer ID (should be the same with the ID setting in dial-in type) by checking the box. Also, you should further specify the corresponding security methods on the right side. If you uncheck the checkbox**,** the connection type you select above will apply the authentication methods and security methods in the general settings. **User Name -** This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The maximum length for both username is 11 characters. **Password -** This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The maximum length for both username is 11 characters. **VJ Compression -** VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP with or without IPSec policy above. **IKE Authentication Method -** This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. **Pre-Shared Key -** Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. **IPSec Security Method -** This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. **Phase 1/2 Algorithm-** Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Triple DES (3DES) and AES.
TCP/IP Network Settings	**Remote Network IP/ Remote Network Mask -** Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPSec, this is the destination clients IDs of phase 2 quick mode. **Local Network IP / Local Network Mask -** Add a static route to direct all traffic destined to Local Network IP Address/Local Network Mask through the VPN connection. **Route/NAT Mode -** If the remote network only allows you to dial in with single IP, please choose **NAT**, otherwise choose **Route**. **Change default route to this VPN tunnel -** Check this box to change the default route with this VPN tunnel. Note that this setting is available only for one WAN interface is enabled. It is not available when both WAN interfaces are enabled.

2. After finishing all the settings here, please click **OK** to save the configuration.

3.8.6 Connection Management

You can find the summary table of all VPN connections. You may disconnect any VPN connection by clicking **Drop** button. You may also aggressively Dial-out by using Dial-out Tool and clicking **Dial** button.



Available settings are explained as follows:

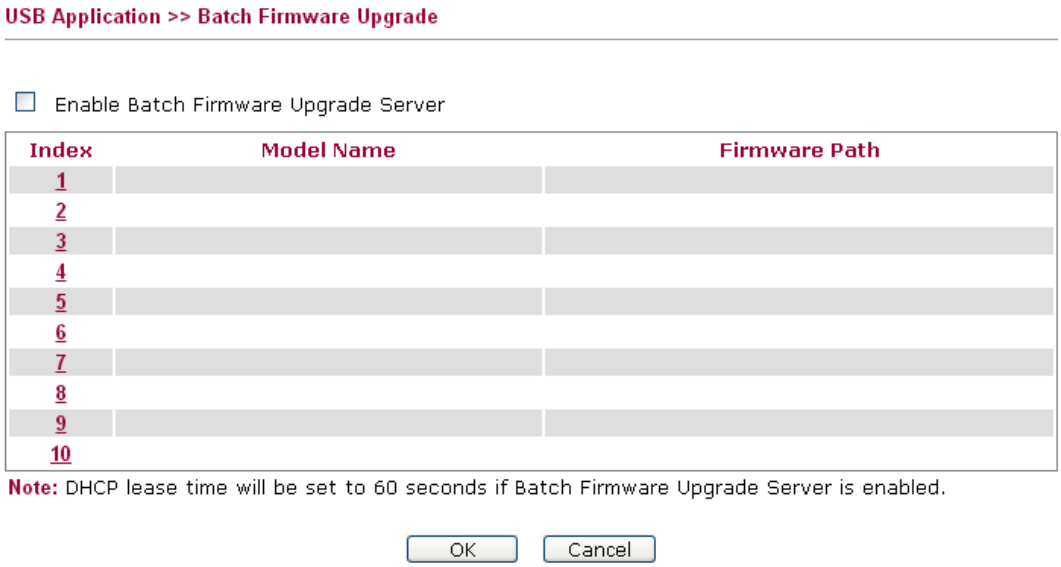
Item	Description
General Mode	This filed displays the profile configured in LAN-to-LAN (with Index number and VPN Server IP address).
Dial	Click this button to execute dial out function.
Refresh Seconds	Choose the time for refresh the dial information among 10, 20, and 30.
Refresh	Click this button to refresh the whole connection status.

3.9 USB Application

3.9.1 Batch Firmware Upgrade

Usually, the acknowledgement of firmware upgrade is that only the active router which connects to the host is allowed to have the firmware update for the at one time.

However, in real physical network connection, VigorFly 210 can be connected with other routers to satisfy different requests from users. Executing the firmware upgrade for others connected router might not be easy as done in VigorFly210. Fortunately, the new feature of Batch Firmware Upgrade can solve the problem. Not only it is easy to operate, but also it can save the time of firmware upgrade for other router(s).



Each item is explained as follows:

Item	Description
Enable Batch Firmware Upgrade Server	Check the box to enable such function and let VigorFly 210 acts as a firmware upgrade server.
Index	Display the number of the batch profile.
Model Name	Display the name of the profile.
Firmware Path	Display the path that the firmware is located.

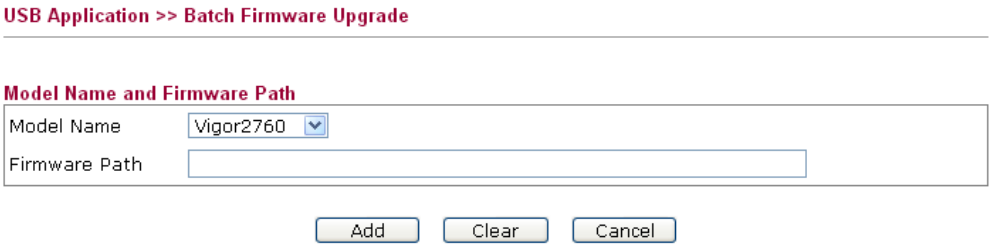
1. Insert a USB disk to the USB port on VigorFly 210.

2. Create a directory for storing firmware downloaded from DrayTek website on USB disk. For example, create a folder named “Vigor2860” which is ready to store the newly firmware for Vigor2860.

3. Open **USB Application>>Batch Firmware Upgrade** from the web user interface of VigorFly 210.

4. Check the box of **Enable Batch Firmware Upgrade Server**.

5. To create a firmware upgrade profile, simply click one of the index numbers to open the following web page.



Available settings are explained as follows:

Item	Description
Model Name	Use the drop down list to choose the model you want. For example, choose Vigor2860.
Firmware Path	Write down the location of the firmware including the name and the directory. In this case, type /fw/vigor2860/vigor2860.all.
Add	Click it to add the settings configuration and return to previous page. A new created profile will be displayed on the previous page.
Clear	Click it to cancel the settings configuration.
Cancel	Click it to cancel the settings configuration and return to last web page.

6. Choose the model name and specify the path of the firmware located. Click **Add**.

7. Press the Factory Reset button of VigorFly 210 for 10 or more seconds. Now, the firmware will be upgraded automatically.

3.10 Wireless LAN

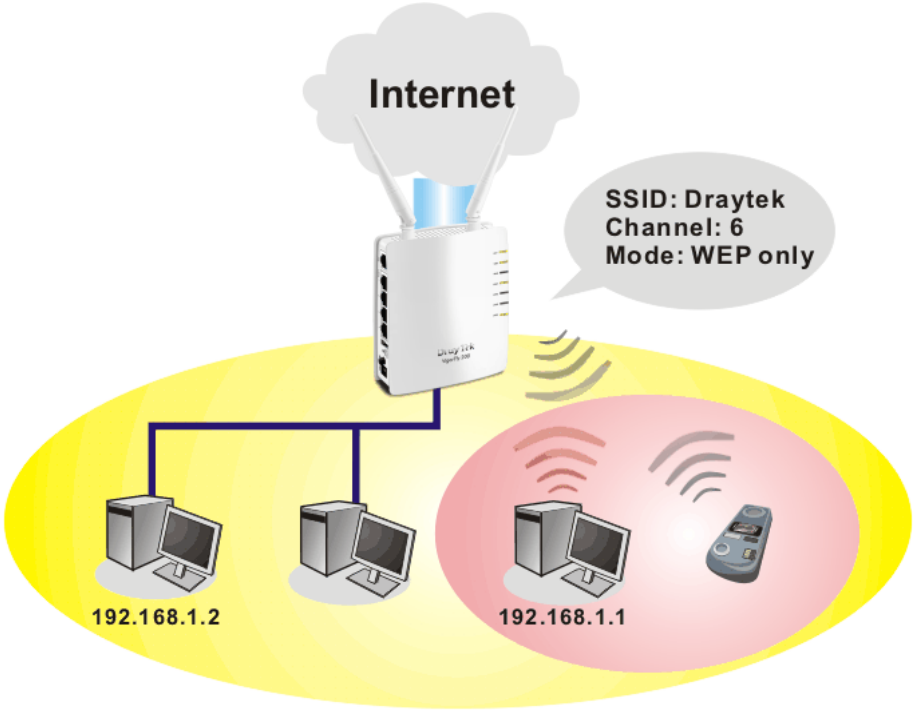
3.10.1 Basic Concepts

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.

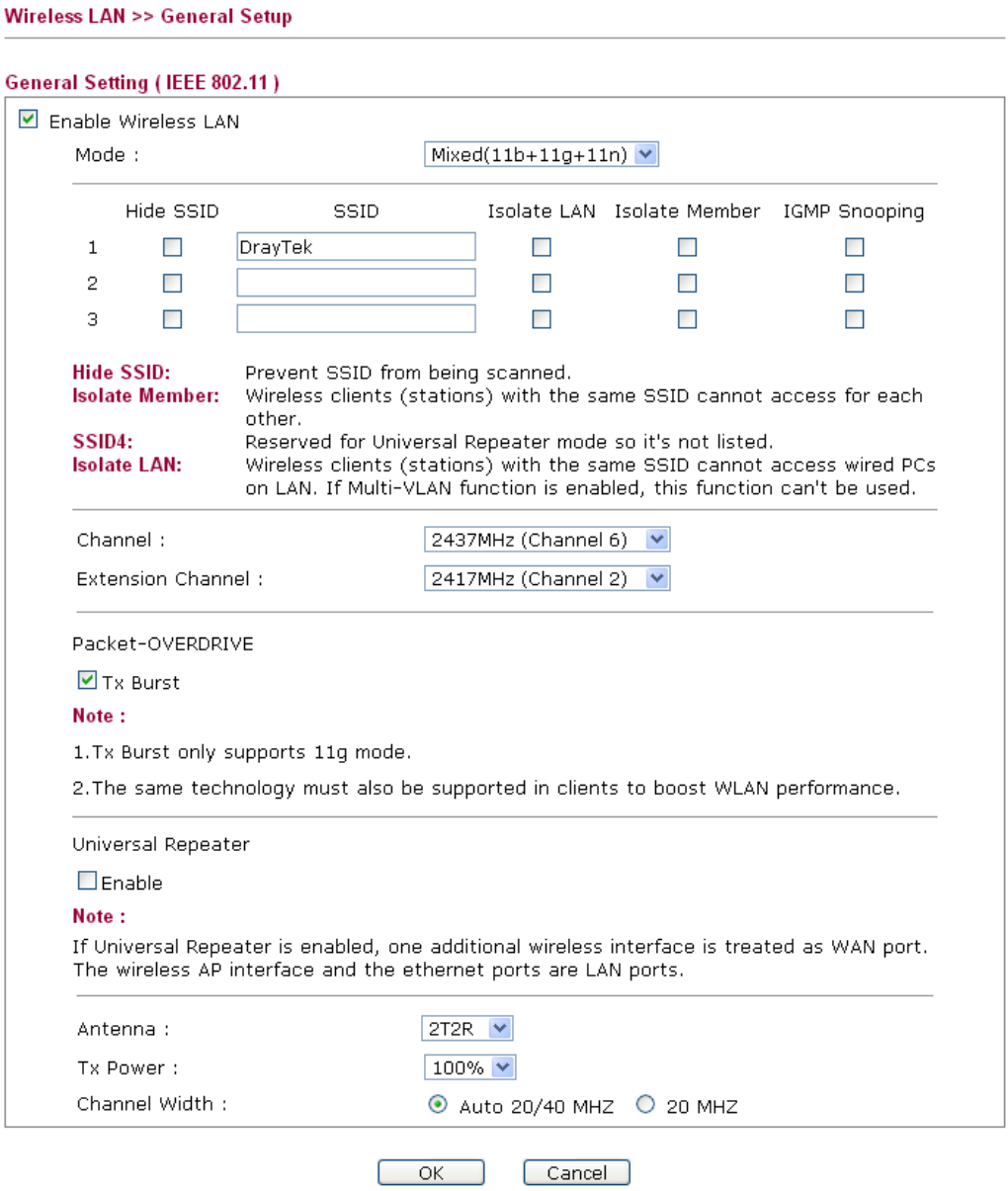
Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless 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.

3.10.2 General Setup

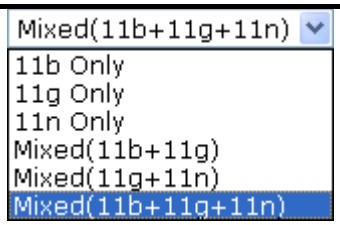
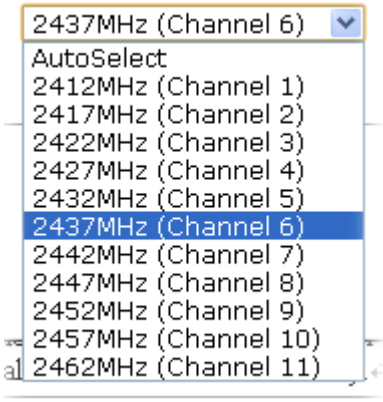
By clicking the **General Setup**, a new web page will appear so that you could configure the SSID and the wireless channel.

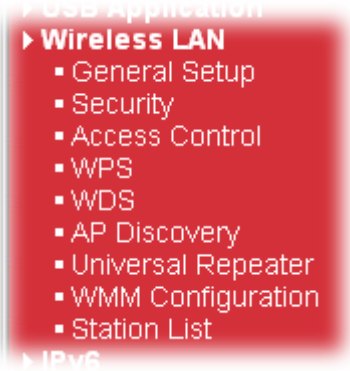
Please refer to the following figure for more information.



Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	At present, the router can connect to, 11g Only, 11b Only, 11n Only, Mixed (11g+11n), Mixed (11b+11g), 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 LAN	Wireless clients (stations) with the same SSID can access for each other through Access Point and access Internet via WAN interface; however, they cannot access wired PCs on LAN.
Isolate Member	Wireless clients (stations) with the same SSID cannot access for each other through Access Point; however, they can access wired PCs on LAN and access Internet via WAN interface.
IGMP Snooping	Check the box to activate IGMP snooping for the station which access into Internet through such SSID.
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. 
Extension Channel	Such channel will be brought out automatically when you determine the **Channel** selection. It can help to extend the bandwidth for wireless connection. Such value can be modified manually.
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.

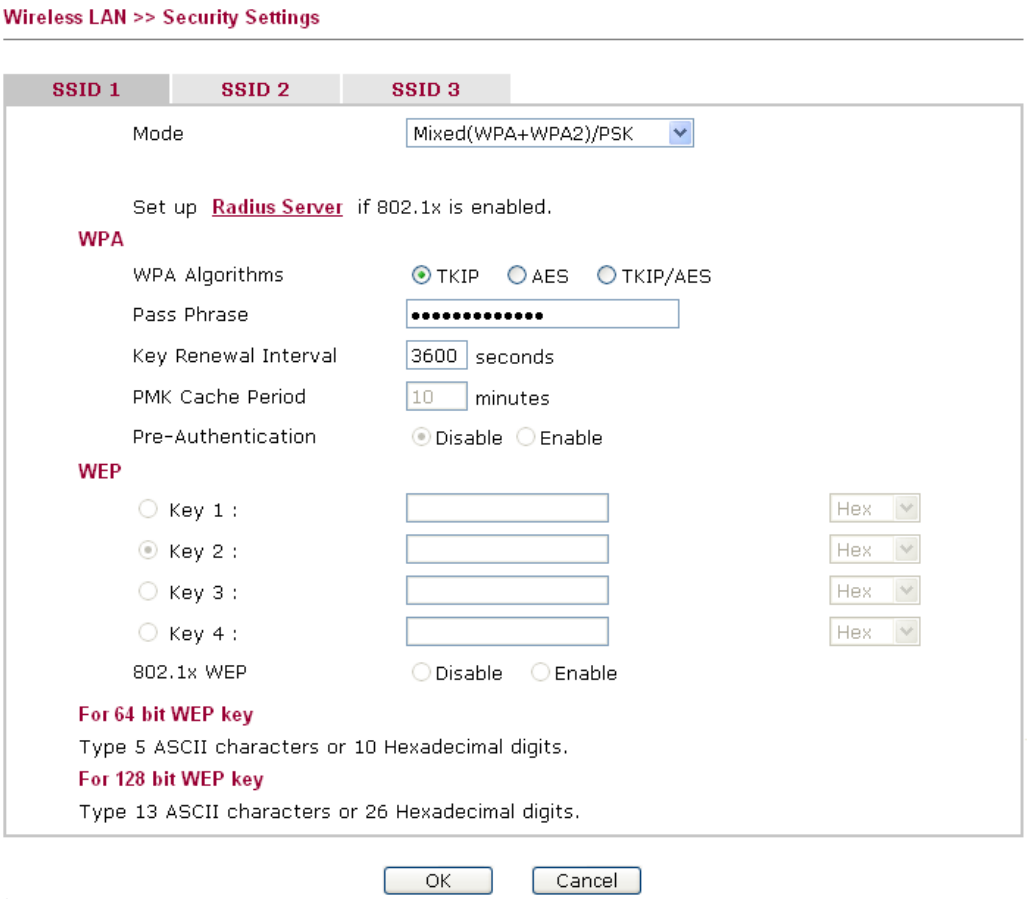
	That is, the wireless client must support this feature and invoke the function, too. **Note:** Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, 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 Repeate**r. Please refer to the corresponding section for detailed information.
Antenna	Specify the type of the antenna used for your router.
Tx Power	Set the power percentage for transmission signal of access point. The greater the value is, the higher intensity of the signal will be. 
Channel Width	**Auto 20/40 MHZ** - The router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transmission. **20 MHZ-** the router will use 20Mhz for data transmitting and receiving between the AP and the stations.

After finishing all the settings here, please click **OK** to save the configuration.

3.10.3 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.



Available settings are explained as follows:

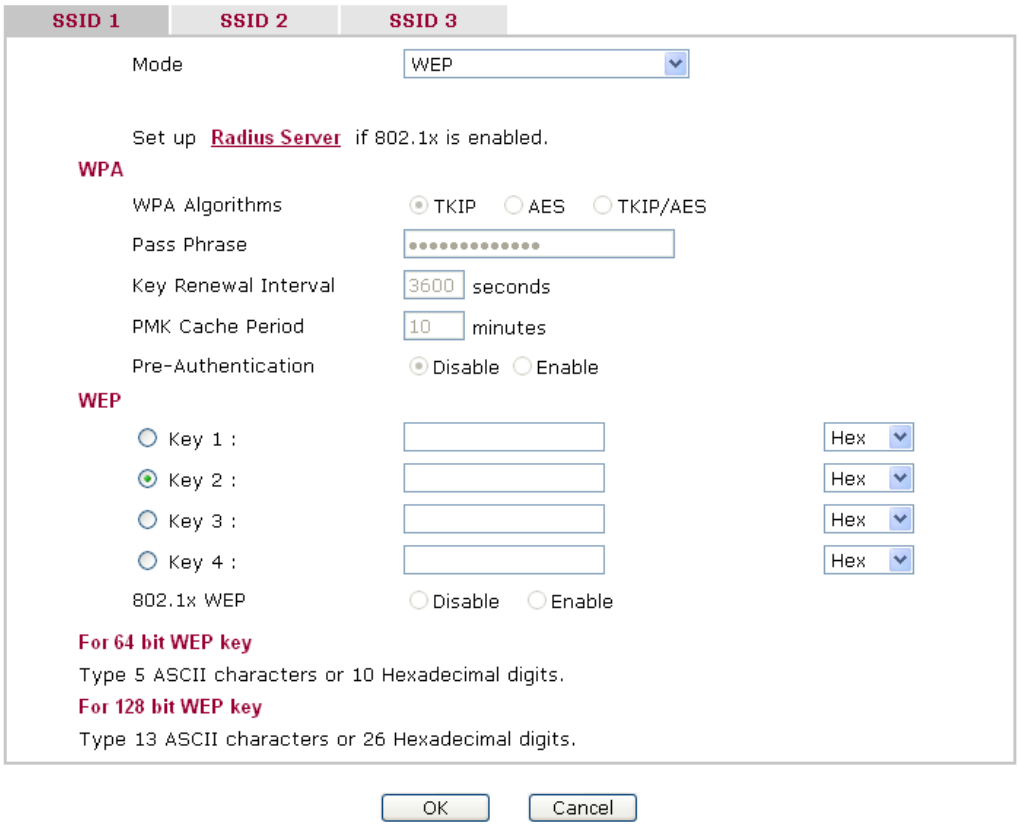
Item	Description
Mode	There are several modes provided for you to choose. Disable Disable WEP WPA/PSK WPA2/PSK Mixed(WPA+WPA2)/PSK WEP/802.1x WPA/802.1x WPA2/802.1x Mixed(WPA+WPA2)/802.1x

- **Disable**

  The encryption mechanism is turned off.

- **WEP**

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

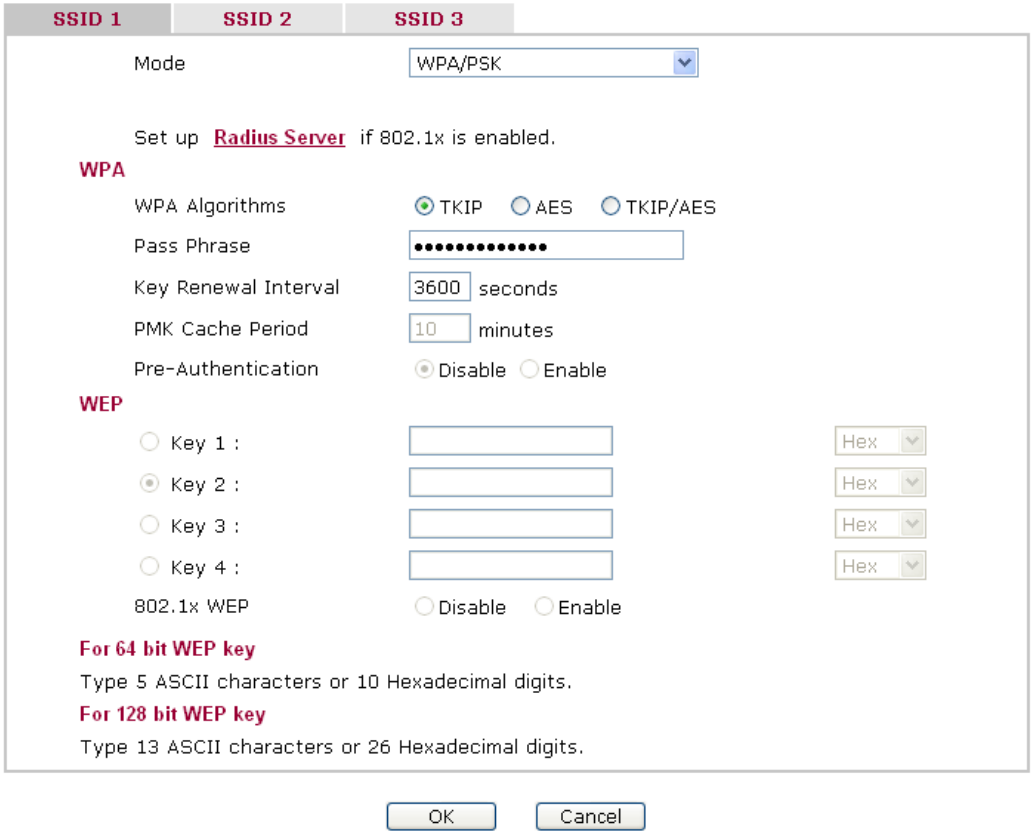


Available settings are explained as follows:

Item	Description
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.



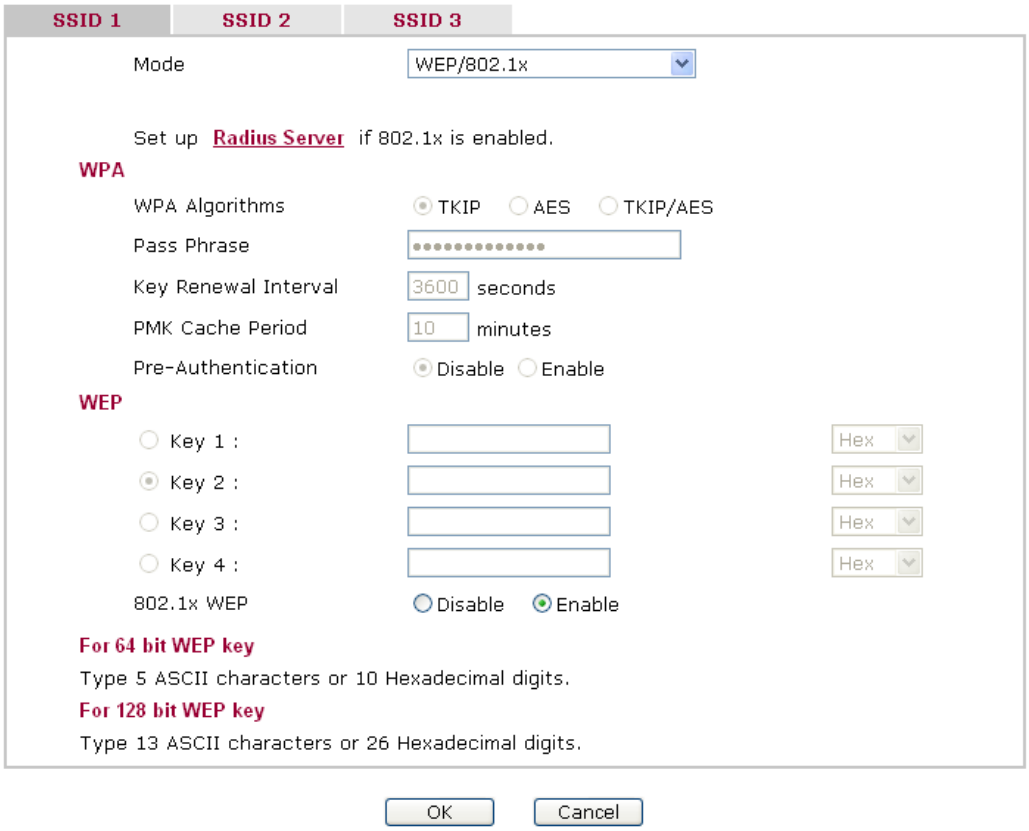
Available settings are explained as follows:

Item	Description
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.

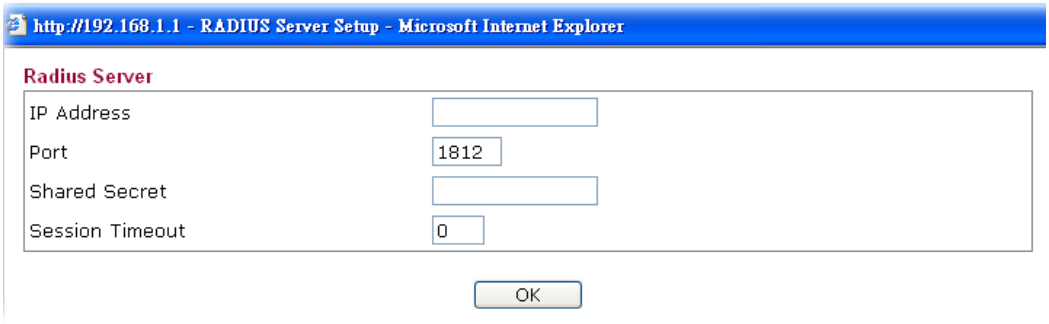
The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode.



Available settings are explained as follows:

Item	Description
802.1x WEP	**Disable** - Disable the WEP Encryption. Data sent to the AP will not be encrypted. **Enable** - Enable the WEP Encryption.
RADIUS Server	Guide you to access into next pop-up window to configure RADIUS server settings.

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



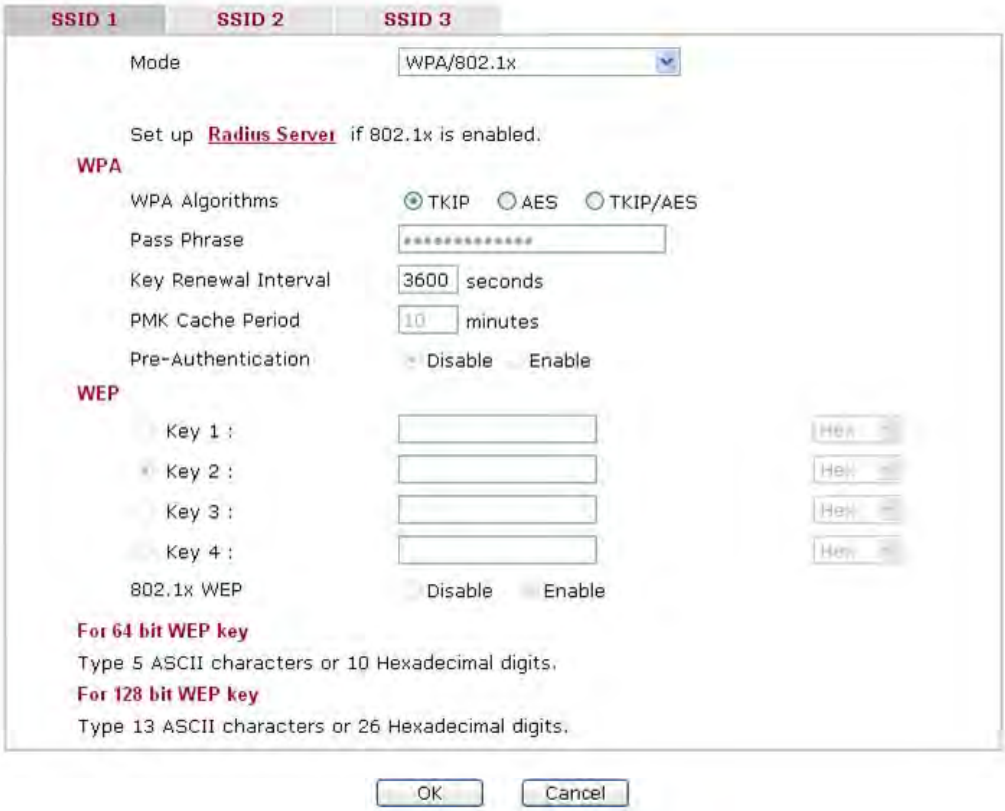
Available settings are explained as follows:

Item	Description
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.)

- **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.

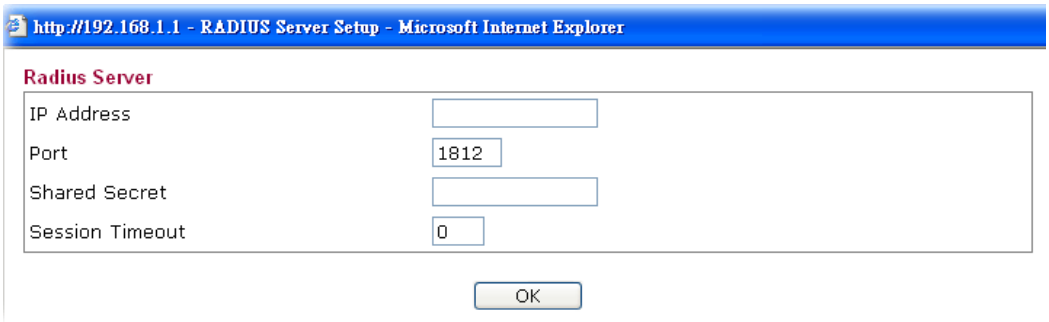


Available settings are explained as follows:

Item	Description
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.

RADIUS Server	Guide you to access into next pop-up window to configure RADIUS server settings.

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

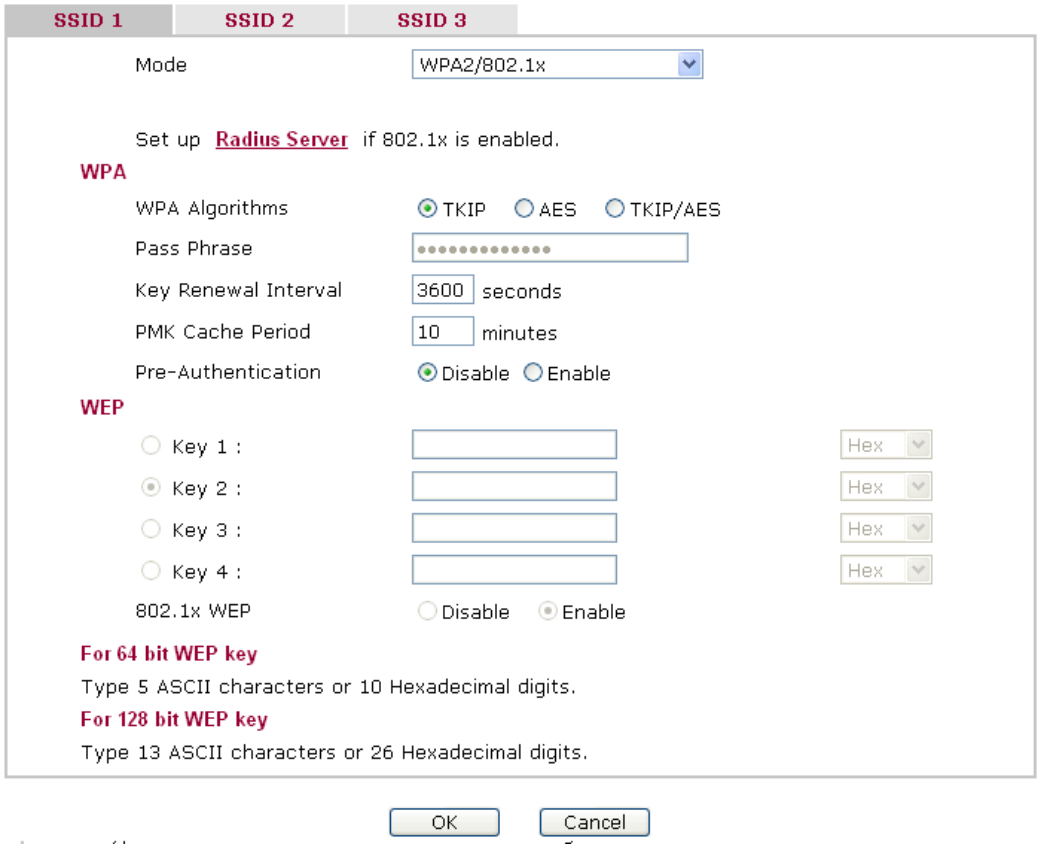


Available settings are explained as follows:

Item	Description
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.)

- **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.

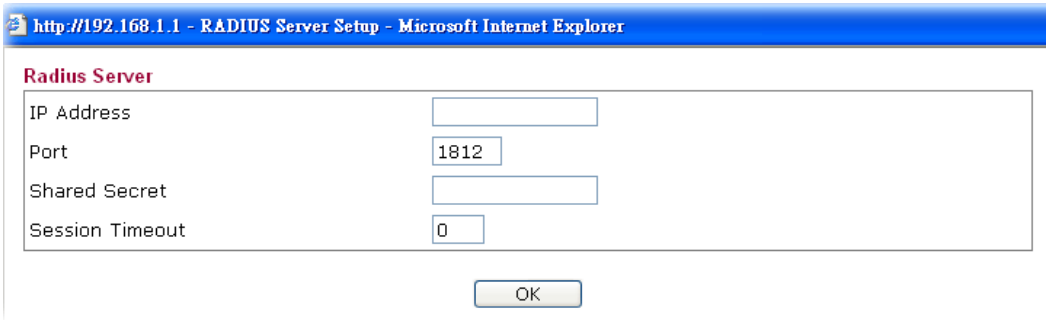


Available settings are explained as follows:

Item	Description
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.
RADIUS Server	Guide you to access into next pop-up window to configure RADIUS server settings.

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

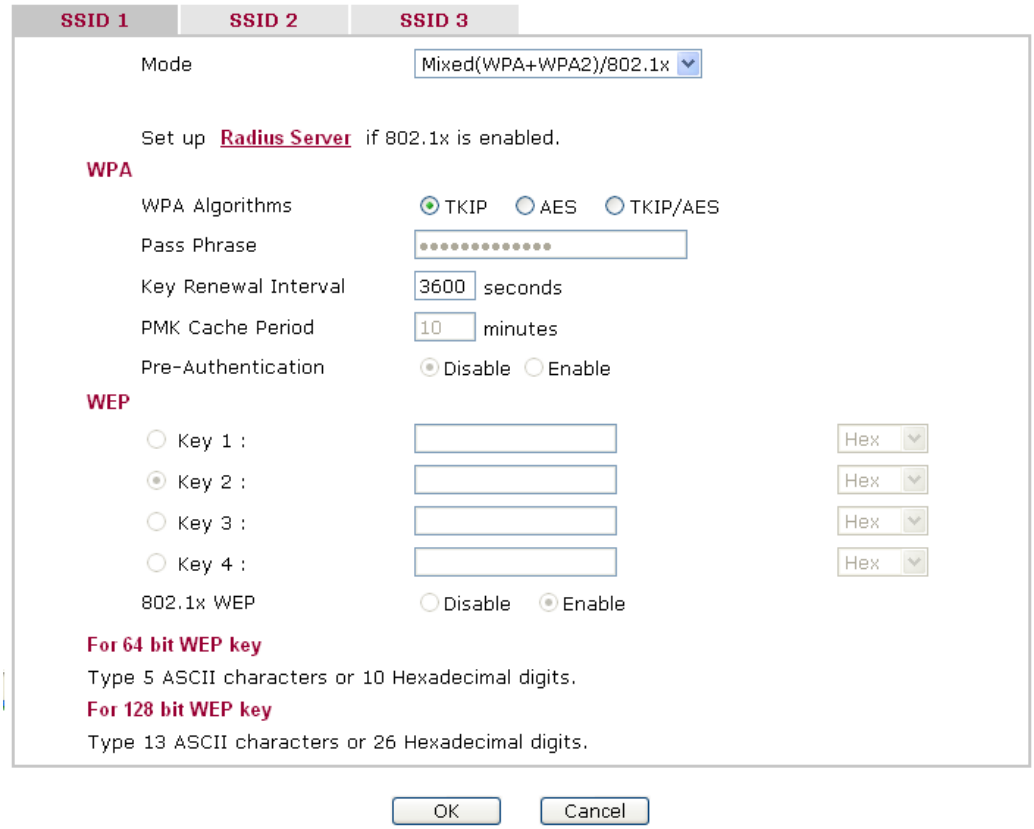


Available settings are explained as follows:

Item	Description
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.)

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

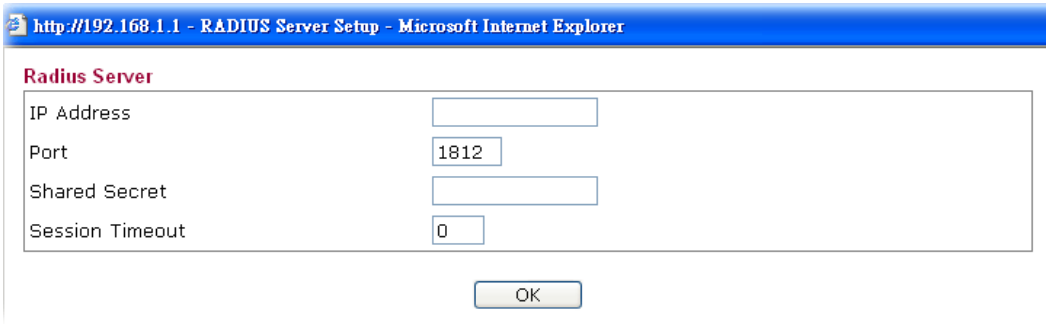
The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.



Available settings are explained as follows:

Item	Description
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.?
RADIUS Server	Guide you to access into next pop-up window to configure RADIUS server settings.

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

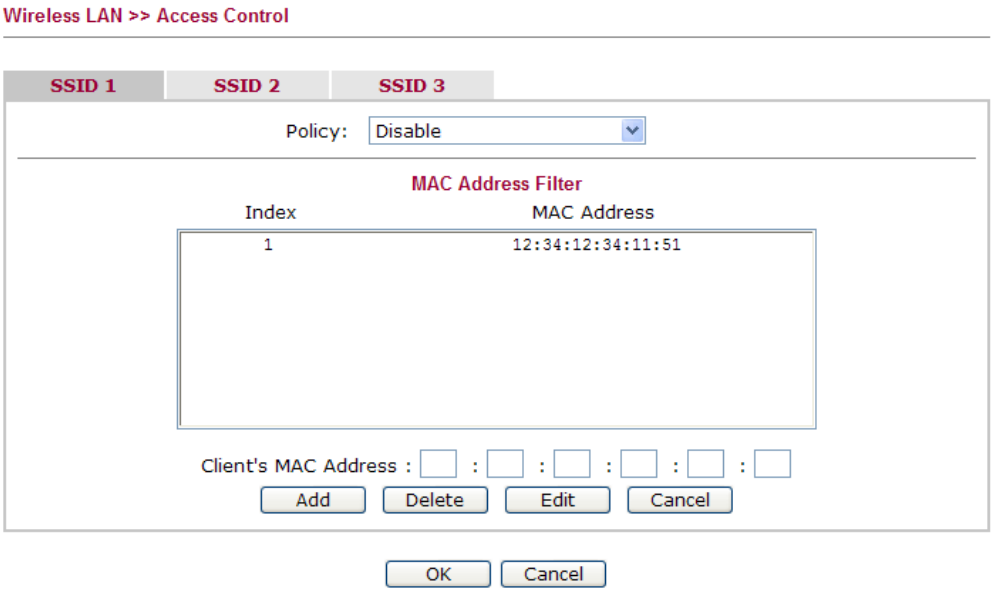


Available settings are explained as follows:

Item	Description
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.)

3.10.4 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).



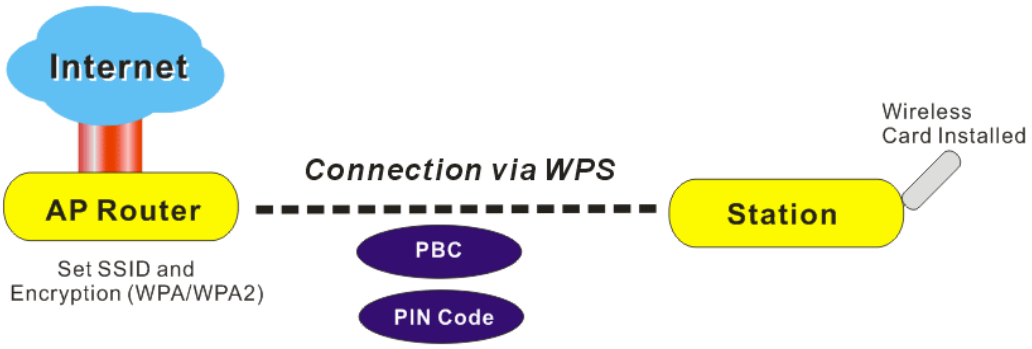
Available settings are explained as follows:

Item	Description
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. Activate MAC address filter Disable Activate MAC address filter Blocked MAC address filter
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.

3.10.5 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.

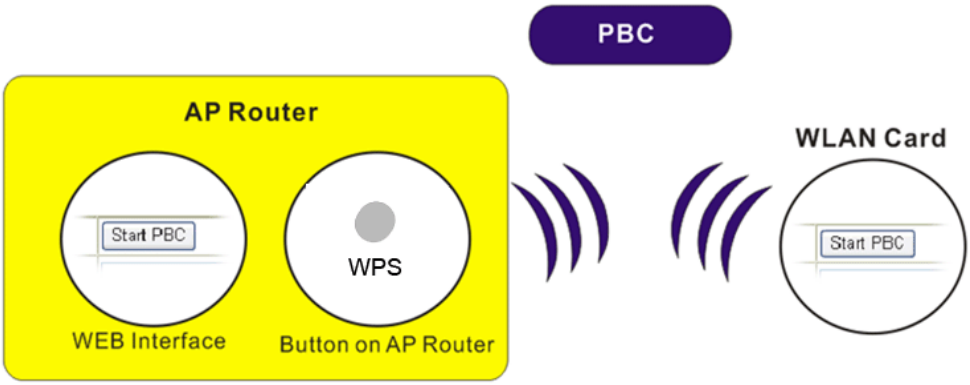


Note: Such function is available for the wireless station with WPS supported.

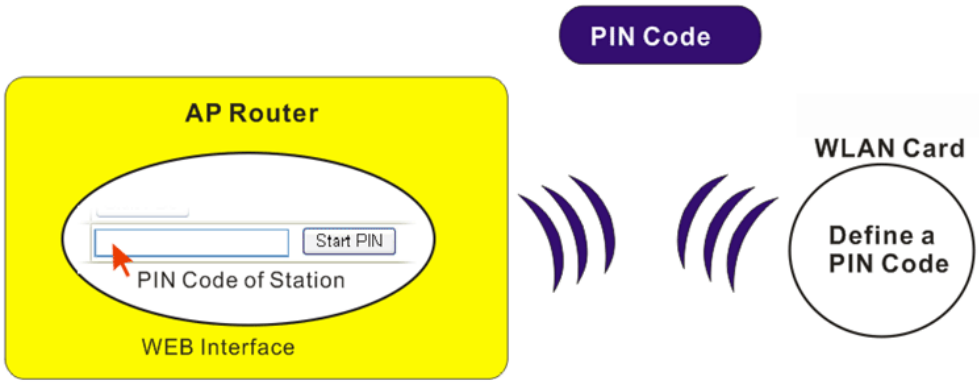
There are two methods to do network connection through WPS between AP and Stations: pressing the ***Start PBC*** button or using ***PIN Code***.

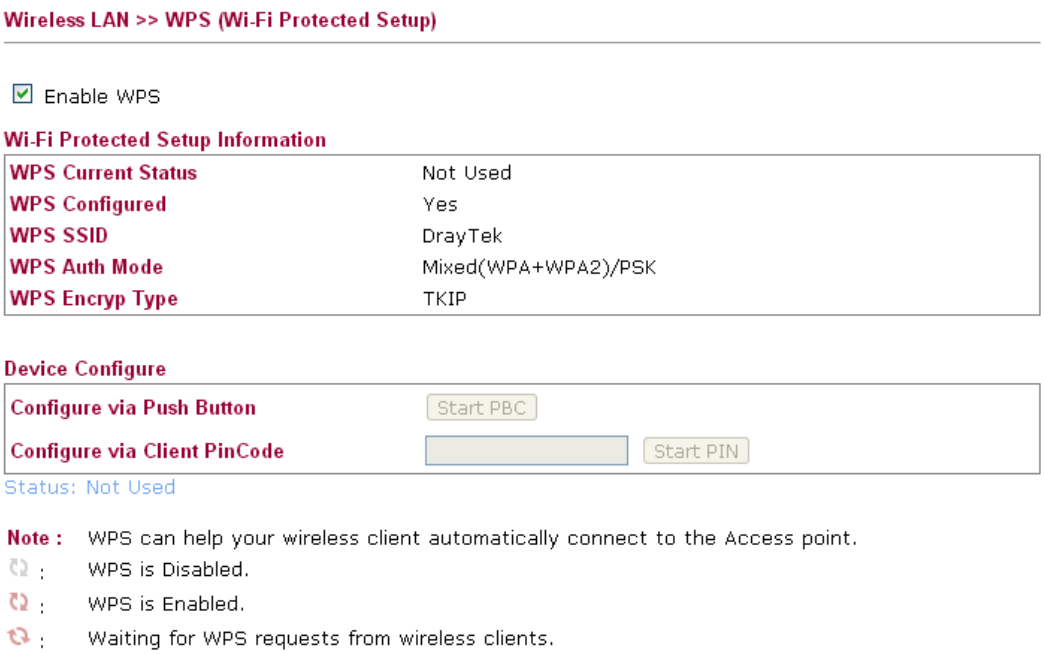
On the side of VigorFly 210 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a

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.





Available settings are explained as follows:

Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Current Status	Display related system information for WPS. If the wireless

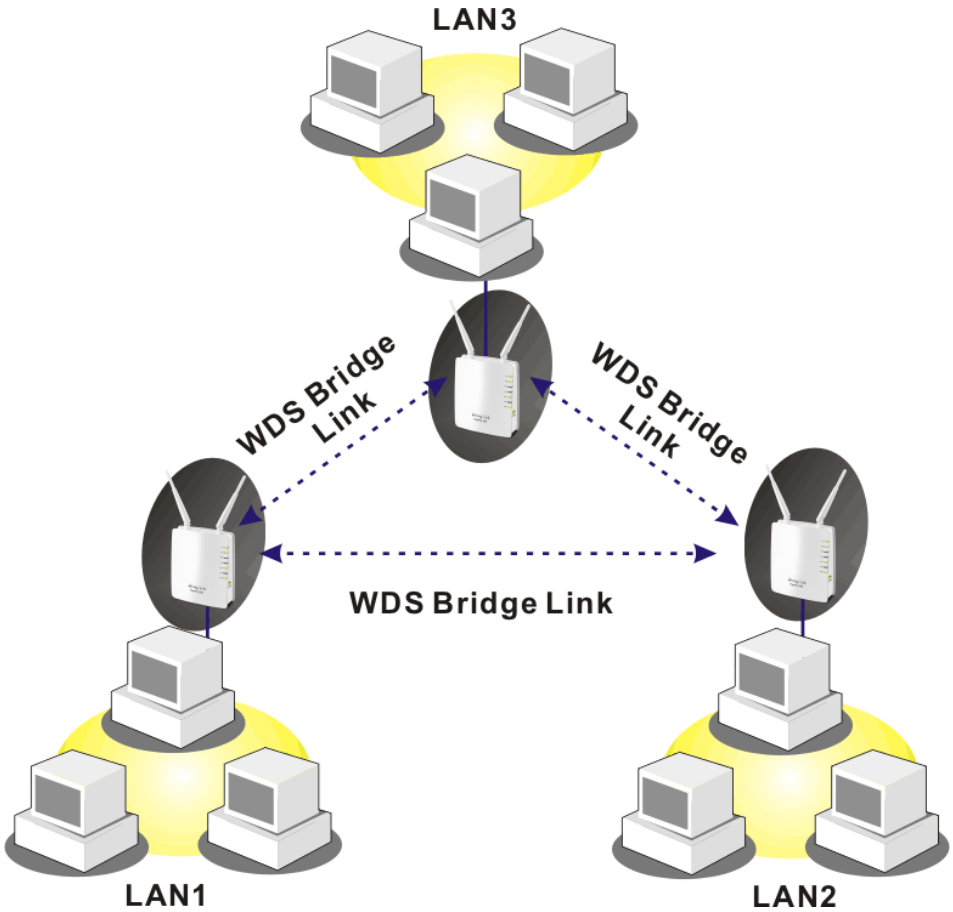
Item	Description
	security (encryption) function of the router is properly configured, you can see 'Configured' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encryp Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of the router.
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.

3.10.6 WDS

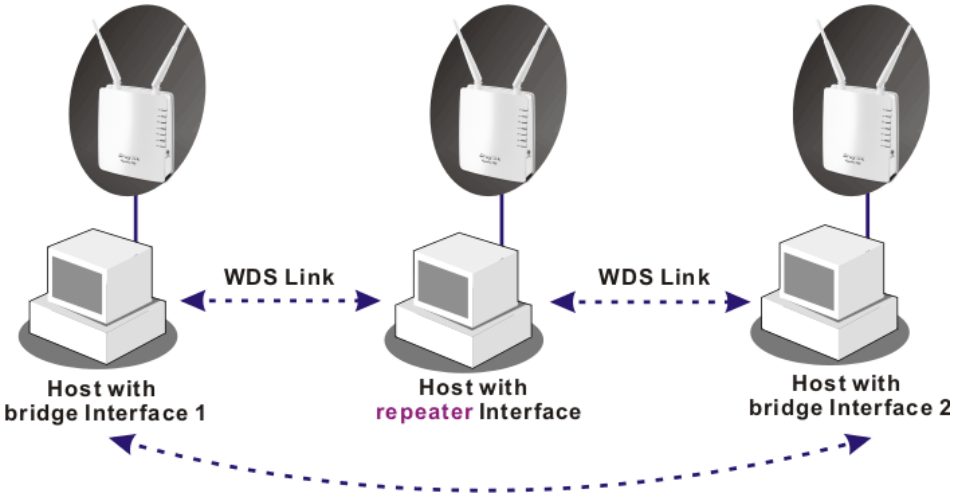
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- 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:

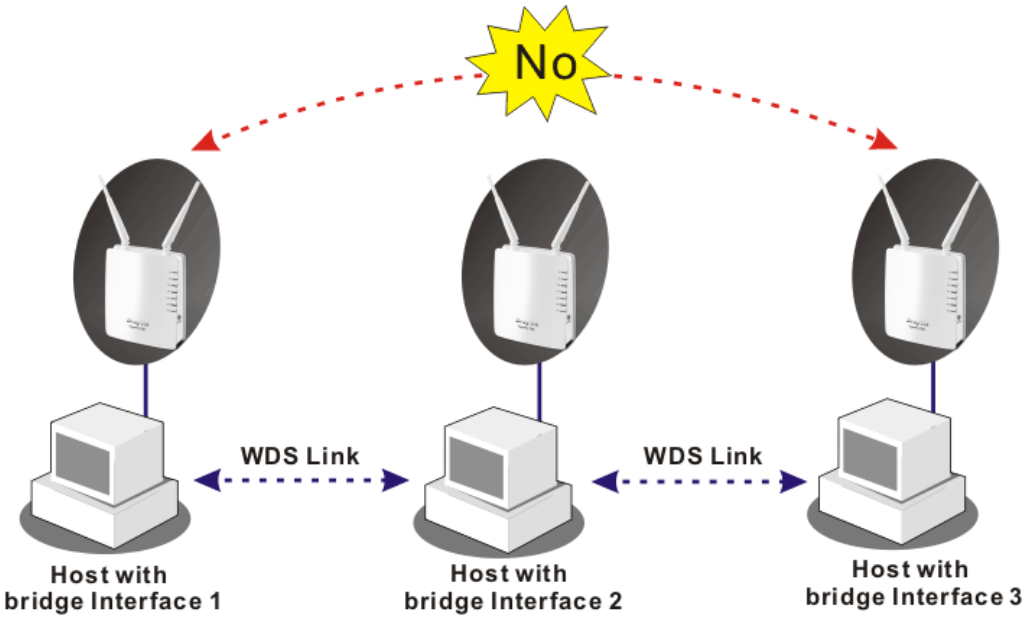


The application for the WDS-Repeater mode is depicted as below:

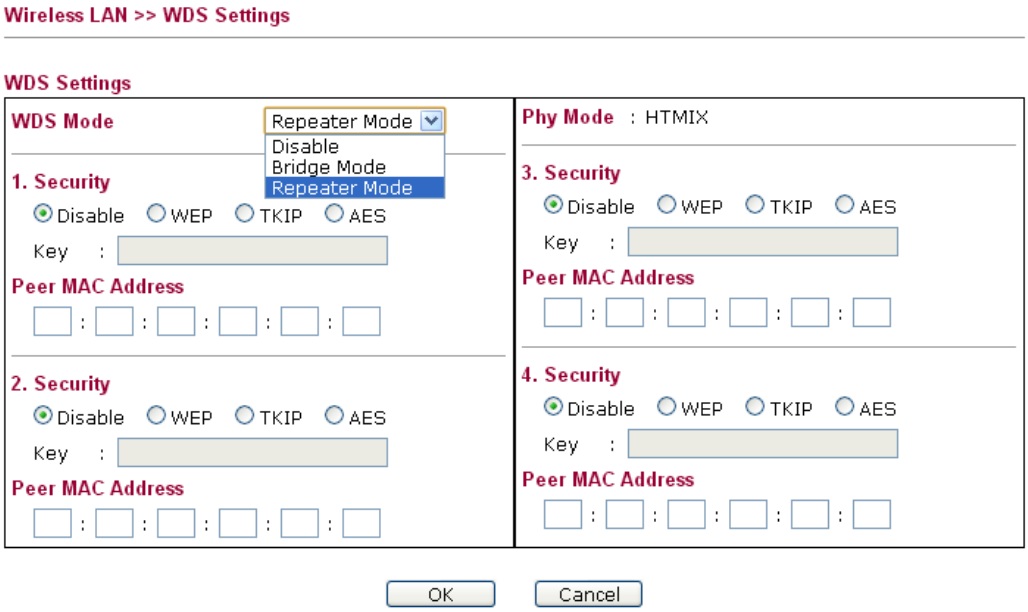


The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words,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



Available settings are explained as follows:

Item	Description
WDS 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. Bridge Mode Disable Bridge Mode Repeater Mode
Security	There are several types for security, **Disabled**, **WEP**, **TKIP, AES** and **Key** or **Peer Mac Address** field valid or not. Choose one of the types for the router. Please disable

Item	Description
	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	Display the transmission rates developed with **HTMIX**.

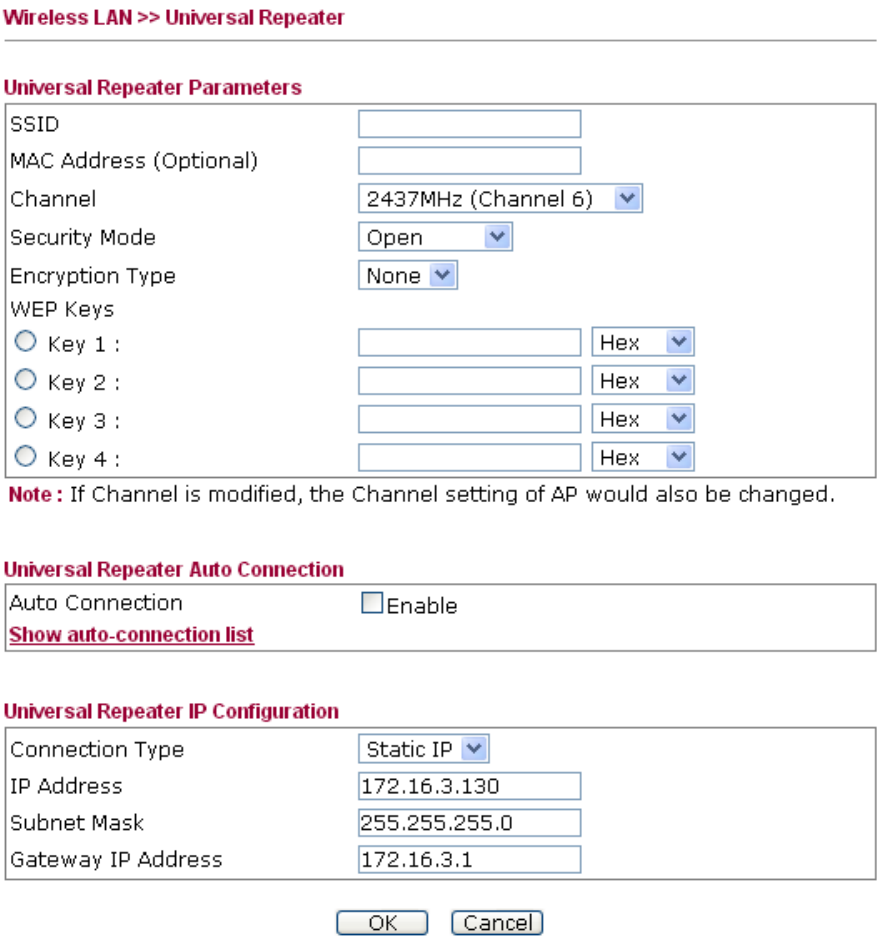
After finishing all the settings here, please click **OK** to save the configuration.

3.10.7 Universal Repeater

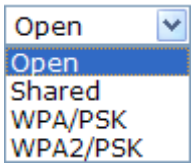
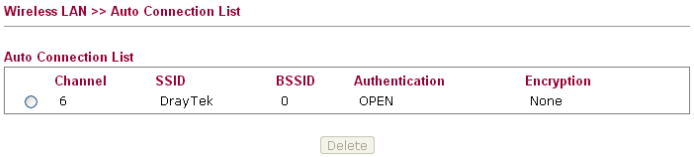
This menu is available only when it is enabled in **Wireless LAN>>General Setup**. It allows you to specify which AP that remote client can connect to.

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.

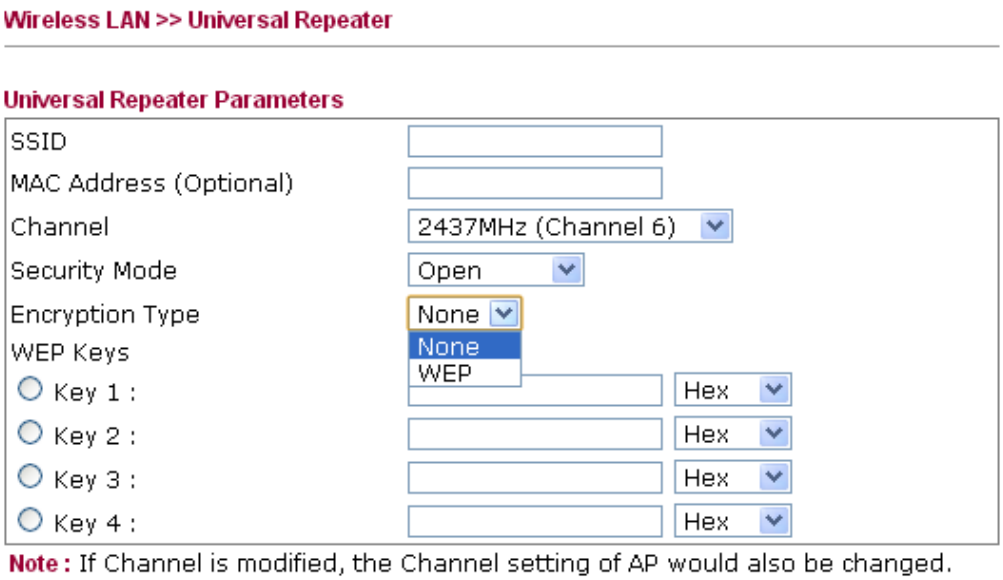


Available settings are explained as follows:

Item	Description
Universal Repeater Parameters	**SSID -** Set a name for the router to be identified. **MAC Address (Optional) -** Type the MAC address of the Access Point that VigorFly 210 wants to connect to. **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. **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. 
Universal Repeater Auto Connection	Before enabling such function, you have to manually type SSID, MAC Address, Channel, Security Mode and Encryption Type (if required) of the access point you want to use first, and click **OK** to save the settings. **Auto Connection –** Check the **Enable** box to perform the network connection automatically. **Show auto-connection list** – Click it to open another page which will display all the access point(s) available for Universal Repeater mode for automatic network connection.  If you have no idea about the SSID and MAC address of the access point you want to connect, simply go to **Wireless LAN>>Access Point Discovery.** Click **Scan** and wait for the scanned result. Choose one of the scanned devices you want and click the **Select** button on the bottom. The related information (including SSID, MAC address, Channel, Security mode, Encryption type, and so on) of that access point will be brought and displayed on this page automatically. Then, check **Enable** for Auto Connection and click **OK** to save the changes. VigorFly 210 will keep such information. Next time, it will make network connection for the computer(s) in LAN automatically when the computer is powered on.
Universal Repeater IP Configuration	Choose it to let current router (treated as a client) connecting to other Access Point. You have to specify connection type, IP address, Subnet Mask and Gateway IP address of this router. **Connection Type** – Choose Static IP or DHCP.

Item	Description
	IP Address – It is available when Static IP is selected. Type the IP address of VigorFly 210. **Subnet Mask** – It is available when Static IP is selected. Type the subnet mask for the IP address configured above. **Gateway IP Address** – It is available when Static IP is selected. Type an IP address of the gateway for VigorFly 210. **Router Name** – It is available when DHCP is selected. You can change the default name if required.

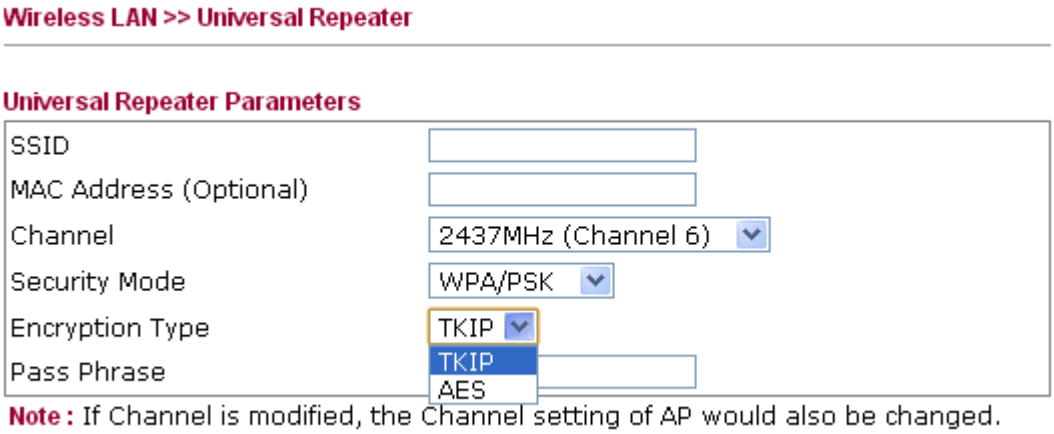
Open / Shared Mode



Available settings are explained as follows:

Item	Description
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 ','. Hex ASCII Hex

WPA/PSK Mode and WPA2/PSK Mode



Available settings are explained as follows:

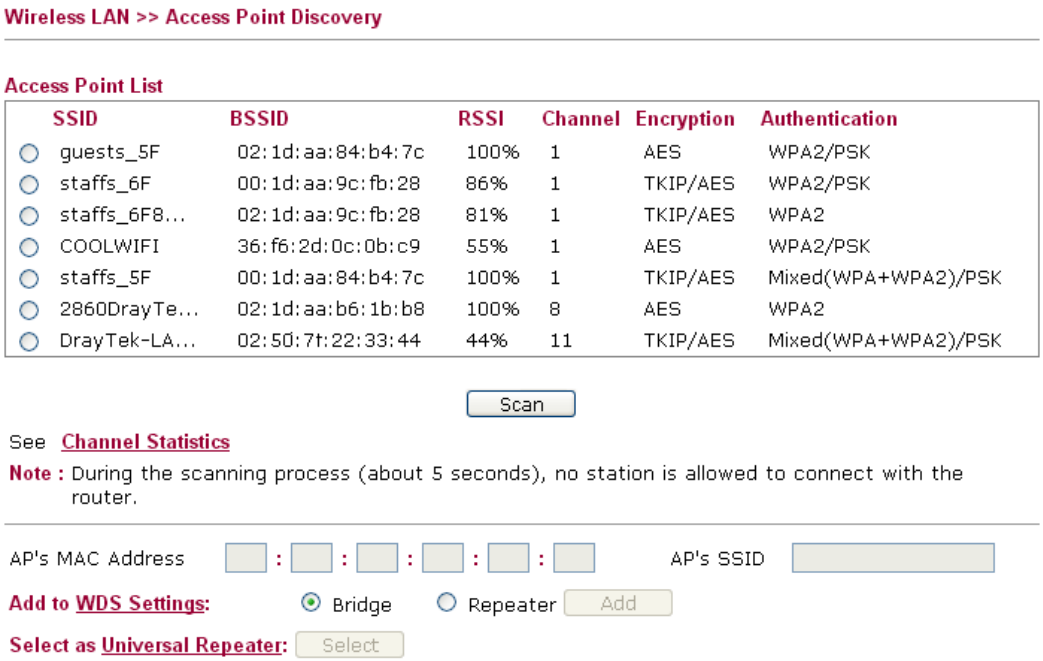
Item	Description
Encryption Type	Select TKIP or AES as the algorithm for WPA.
Pass Phrase	Either **8~63** ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

After finishing all the settings here, please click **OK** to save the configuration.

3.10.8 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.



Available settings are explained as follows:

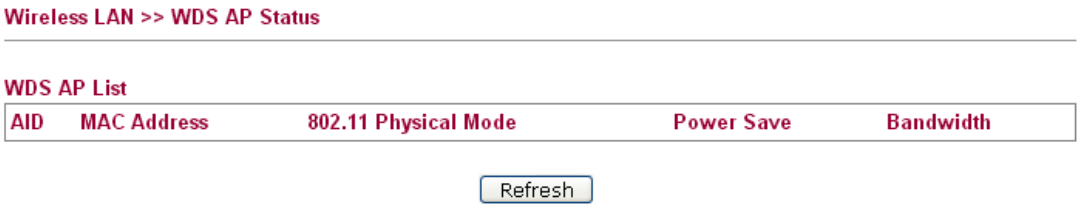
Item	Description
SSID	Display the SSID of the AP scanned by this router.
BSSID	Display the MAC address of the AP scanned by this router.
RSSI	Display the signal strength. RSSI is the abbreviation of Receive Signal Strength Indication.
Channel	Display the wireless channel used for the AP that is scanned 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
Channel 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.

Item	Description
Add to WDS Settings	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.
Select as Universal Repeater	Choose one of the above scanned AP and click **Select.** Corresponding settings of the selected AP will be displayed and applied on **Wireless LAN>>Universal Repeater** page.

After finishing all the settings here, please click **OK** to save the configuration.

3.10.9 WDS AP Status

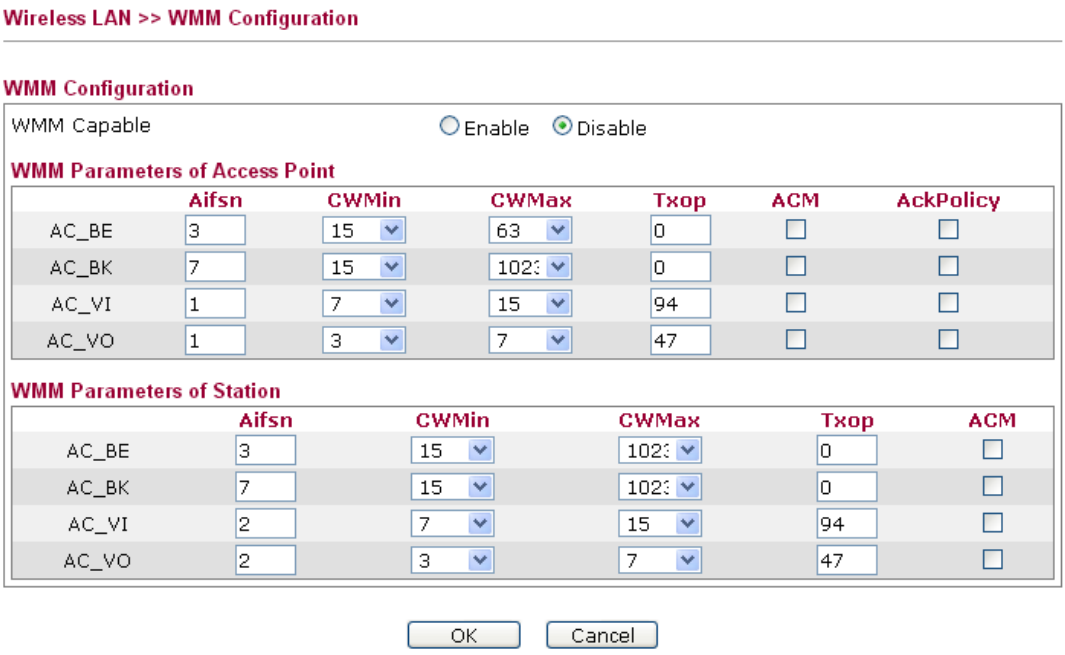
This page display current status for the Access Point



3.10.10 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.



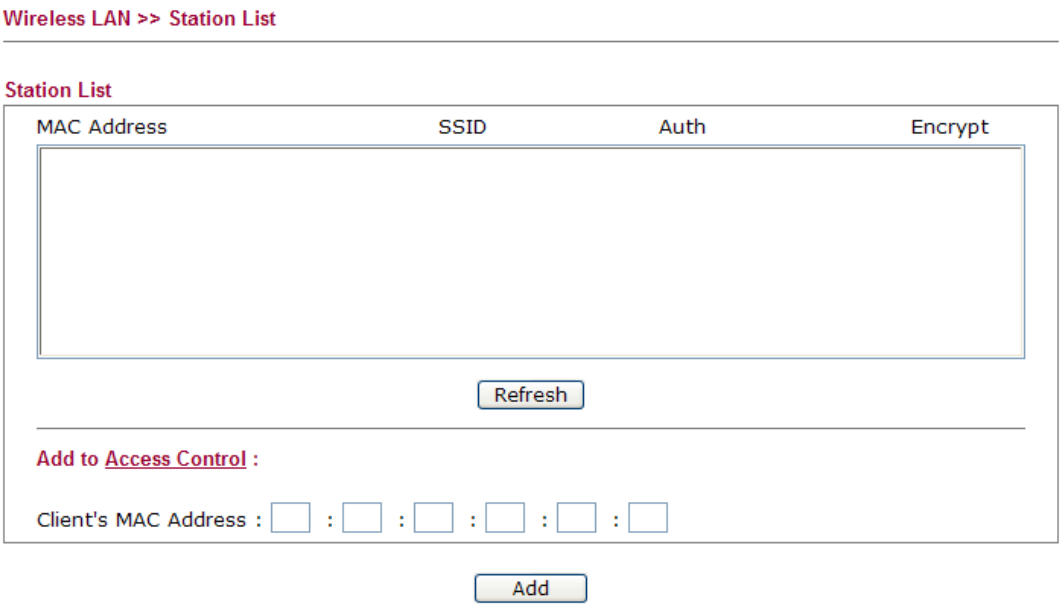
Available settings are explained as follows:

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

After finishing all the settings here, please click **OK** to save the configuration.

3.10.11 Station List

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

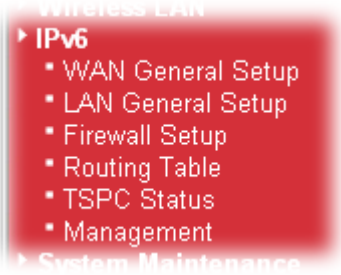


Available settings are explained as follows:

Item	Description
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 Control.**

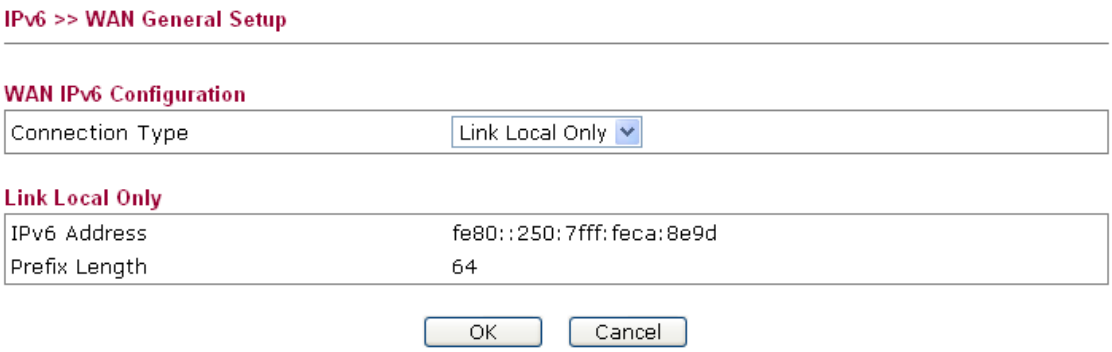
After finishing all the settings here, please click **OK** to save the configuration.

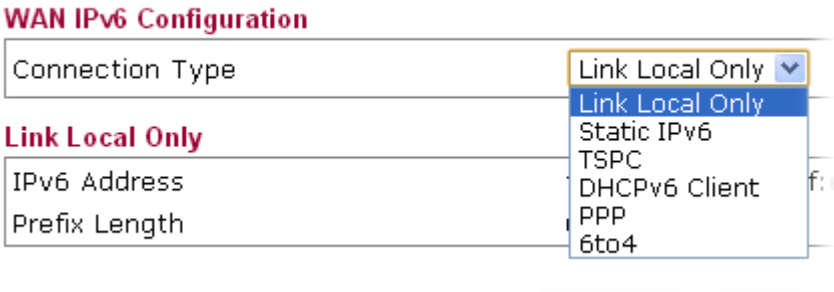
3.11 IPv6



3.11.1 WAN General Setup

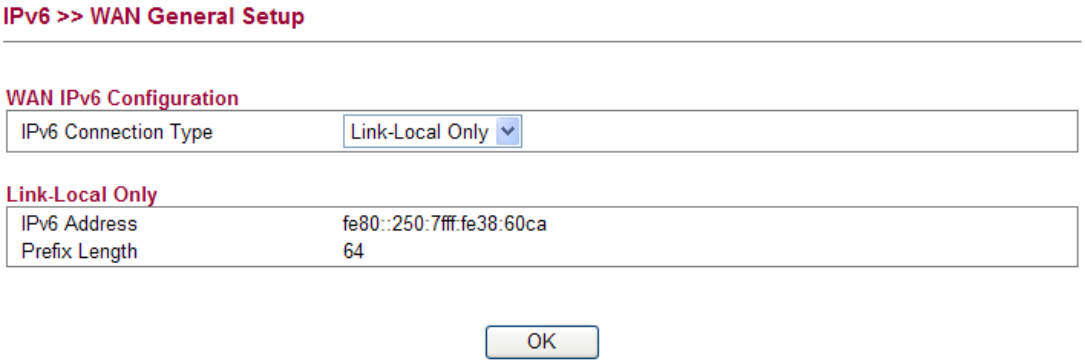
This page defines the IPv6 connection types for WAN interface. Possible types contain Link-Local only, Static IPv6 and TSPC. Each type requires different parameter settings.





Link Local Only

Link Local address is used for communicating with neighbouring nodes on the same link. It is defined by the address prefix **fe80::/10**. You don't need to setup Link-Local address manually for it is generated automatically according to your MAC Address.

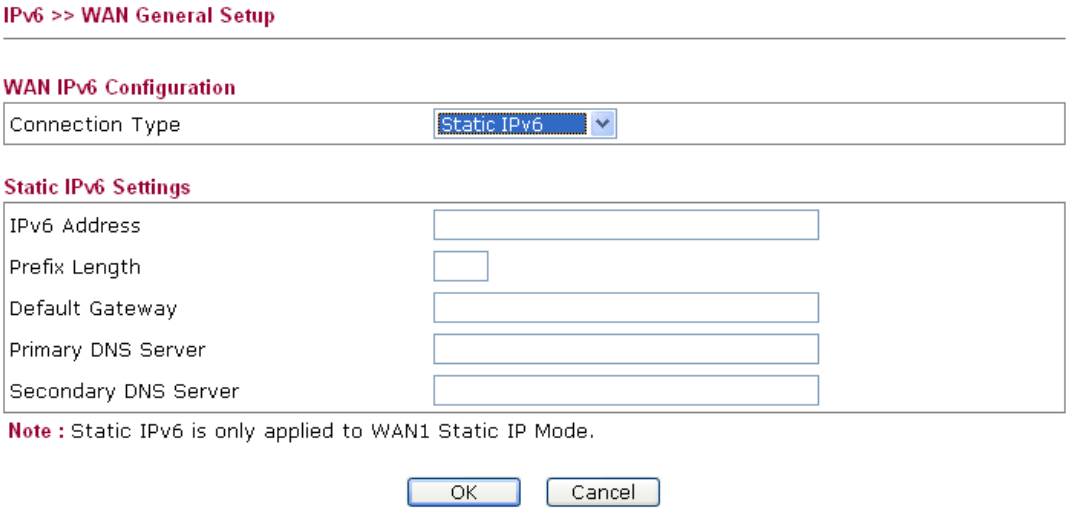


Available settings are explained as follows:

Item	Description
MAC Address	Display the MAC Address for the connecting client.
IPv6 Address	The least significant 64 bits are usually chosen as the interface hardware address constructed in modified EUI-64 format.
Prefix Length	Display the fixed value (64) for prefix length.

Static IPv6

This type allows you to setup static IPv6 address for WAN.



Available settings are explained as follows:

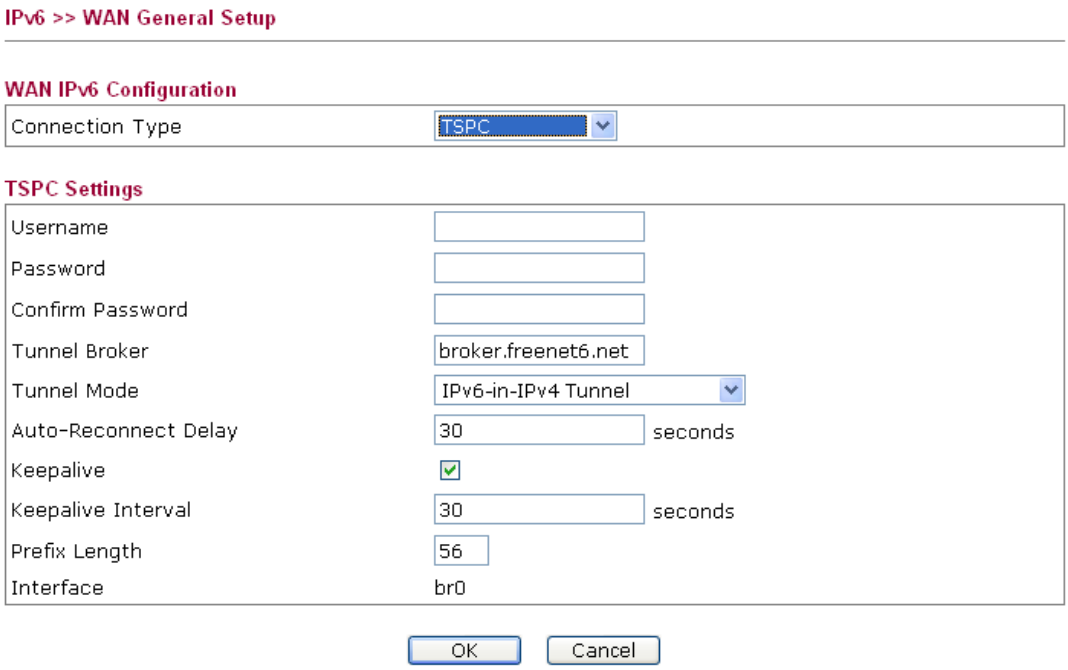
Item	Description
IPv6 Address	Type your IPv6 static IP here.
Prefix Length	Type your IPv6 address prefix length here.
Gateway IPv6 Server	Type your IPv6 gateway address here.
Primary DNS Server	Type your IPv6 primary DNS Server address here.
Secondary DNS Server	Type your IPv6 secondary DNS Server address here.

TSPC

Tunnel setup protocol client (TSPC) is an application which could help you to connect to IPv6 network easily.

Please make sure your IPv4 WAN connection is OK and apply one free account from hexage (http://gogonet.gogo6.com/page/freenet6-account) before you try to use TSPC for network connection. TSPC would connect to tunnel broker and requests a tunnel according to the specifications inside the configuration file. It gets a public IPv6 IP address and an IPv6 prefix from the tunnel broker and then monitors the state of the tunnel in background.

After getting the IPv6 prefix and starting router advertisement daemon (RADVD), the PC behind this router can directly connect to the Internet.



Available settings are explained as follows:

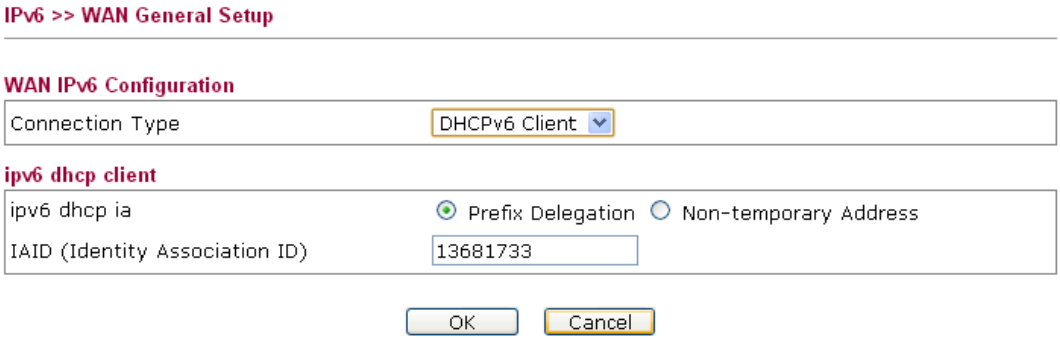
Item	Description
Username	Type the name obtained from the broker.
Password	Type the password assigned with the user name.
Confirm Password	Type the password again to make the confirmation.
Tunnel Broker	Type the address for the tunnel broker IP, FQDN or an optional port number.
Tunnel Mode	**IPv6-in-IPv4 Tunnel**- Let the broker chose the tunnel mode appropriate for the client. **IPv6-in-IPv4 (Native)** - Request an IPv6 in IPv4 tunnel. **IPv6-in-IPv4 (NAT Traversal** - Request an IPv6 in UDP of IPv4 tunnel (for clients behind a NAT). IPv6-in-IPv4 (NAT Traversal) IPv6-in-IPv4 Tunnel IPv6-in-IPv4 (Native) IPv6-in-IPv4 (NAT Traversal)
Auto-reconnect Delay	After passing the time set here, the client will retry to connect in case of failure or keepalive timeout. 0 means not retry.
Keepalive	Check the box to keep the connection between TSPC and tunnel broker always on. TSPC will send ping packet to make sure the connection between both ends is normal.
Keepalive Interval	Type the time for the interval between two keepalive messages transferring from the client to the broker.
Prefix Length	Type the required prefix length for the client network.

Interface	Display LAN interface name. The name of the OS interface that will be configured with the first 64 of the received prefix from the broker and the router advertisement daemon is started to advertise that prefix on the interface.

After finishing all the settings here, please click **OK** to save the configuration.

DHCPv6 Client

DHCPv6 client mode would use DHCPv6 protocol to obtain IPv6 address from server.



Available settings are explained as follows:

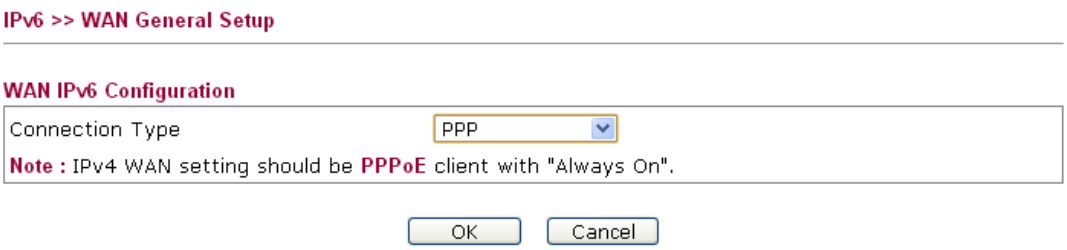
Item	Description
Ipv6 dhcp ia	Choose **Prefix Delegation** or **Non-temporary Address** as the identify association.
IAID	Type a number as IAID.

After finished the above settings, click **OK** to save the settings.

PPP

During the procedure of IPv4 PPPoE connection, we can get the IPv6 Link Local Address between the gateway and Vigor router through IPv6CP. Later, use DHCPv6 or Accept RA to acquire the IPv6 prefix address (such as: 2001:B010:7300:200::/64) offered by the ISP. In addition, PCs under LAN also can have the public IPv6 address for Internet access by means of the generated prefix.

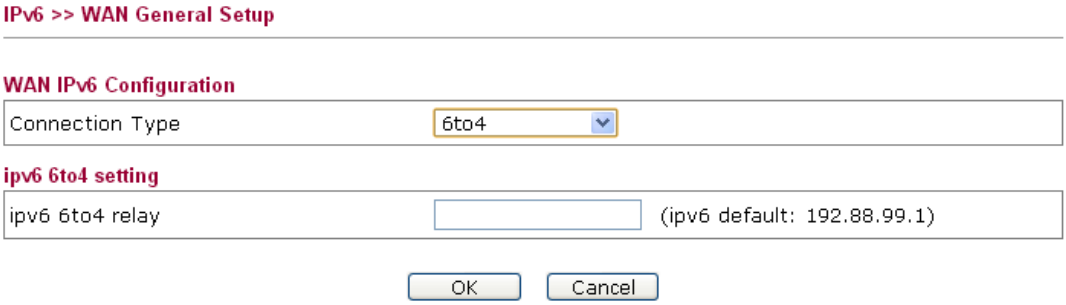
No need to type any other information for PPP mode.



6to4

6to4 is an IPv4 tunnel-based transition mechanism defined in RFC-3056(Connection of IPv6 Domains via IPv4 Clouds).

It is designed to allow different IPv6 domains to communicate with others through IPv4 clouds without explicit IPv4 tunnels.

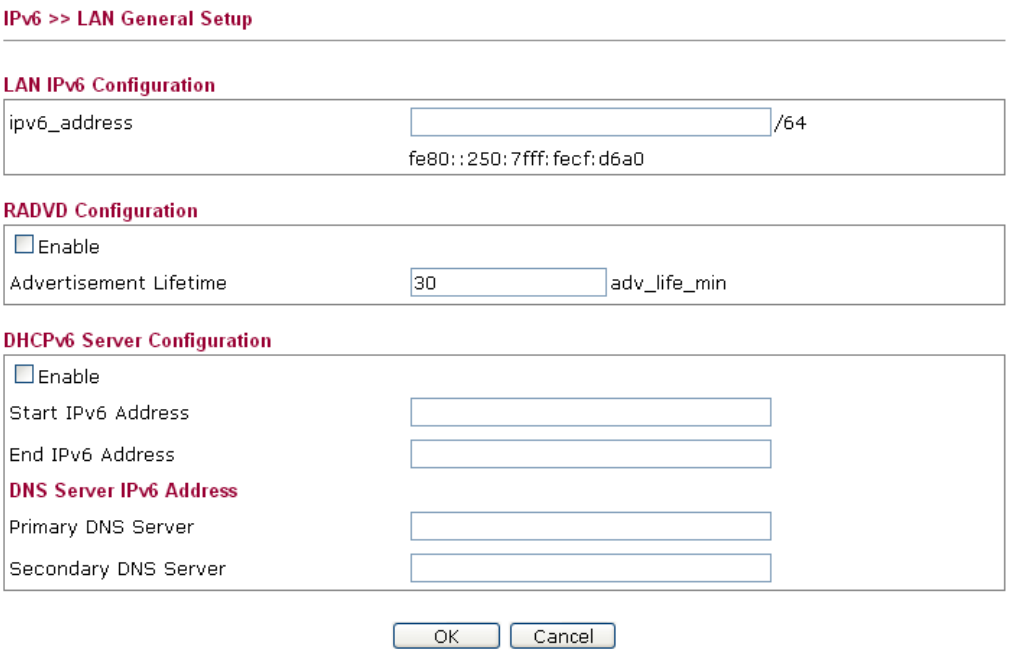


Available settings are explained as follows:

Item	Description
Ipv6 6to4 relay	Type an IP address of 6to4 relay router which connected an IPv4 network and an IPv6 network.

3.11.2 LAN General Setup

This page defines the IPv6 connection types for LAN interface. Possible types contain DHCPv6 Server and RADVD. Each type requires different parameter settings.



Available settings are explained as follows:

Item	Description
LAN IPv6 Configuration	**IPv6 Address -** Type static IPv6 address for LAN.
RADVD Configuration	The router advertisement daemon (radvd) sends Router

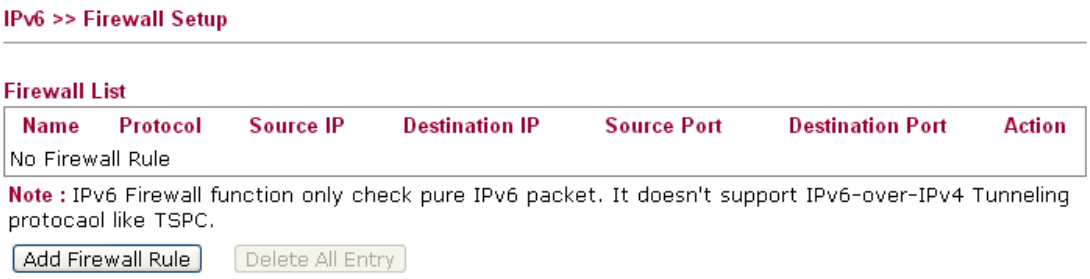
Item	Description
	Advertisement messages, specified by RFC 2461, to a local Ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless auto-configuration. **Enable** – Check the box to enable RADVD server. **Advertisement Lifetime** - The lifetime associated with the default router in units of seconds. It's used to control the lifetime of the prefix. The maximum value corresponds to 18.2 hours. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router list.
DHCPv6 Server Configuration	**Enable –** Check it to enable such setting. **Start IPv6 Address/ End IPv6 Address** - Type the start and end address for IPv6 server.
DNS Server IPv6 Address	**Primary DNS Server -** Type in the primary IP address for the DNS Server. **Secondary DNS Server -** Type in secondary IP address for the primary DNS Server.

After finishing all the settings here, please click **OK** to save the configuration.

3.11.3 Firewall Setup

This page allows users to set firewall rules for IPv6 packets.

Note: Section 3.4 **Firewall** is configured for IPv4 packets only.



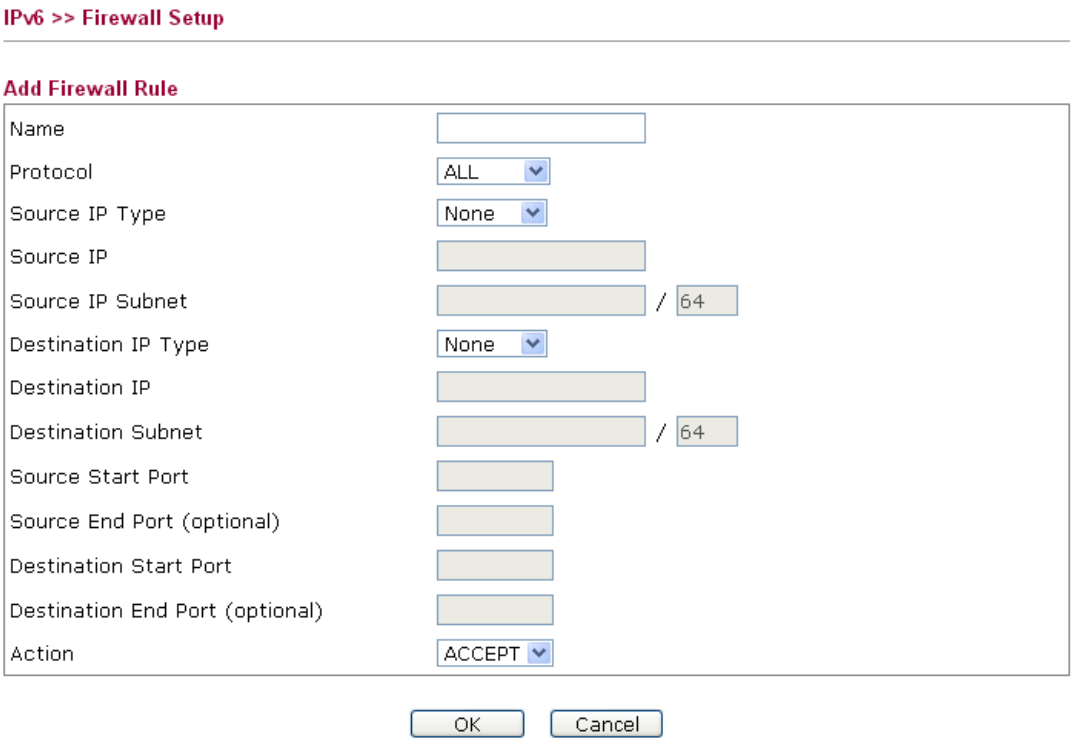
Each item is explained as follows:

Item	Description
Name	Display the name of the rule.
Protocol	Display the protocol (TCP/UDP/ICMPv6) the rule uses.
Source IP	Display the source IP address of such rule.
Destination IP	Display the destination IP address of such rule.
Source Port	Display the source port number of such rule.
Destination Port	Display the destination port number of such rule
Action	Display the status (accept or drop) of such rule.

Adding a New Rule

Click **Add New Rule** to configure a new rule for IPv6 Firewall.

Note: You can set up to 20 sets of IPv6 rules.



Available settings are explained as follows:

Item	Description
Name	Type a name for the rule.
Protocol	Specify a protocol for this rule. ALL ALL TCP UDP ICMPv6
Source IP Type	Determine the IP type as the source. None None Single Subnet
Source IP	Type the IPv6 address here if you choose **Single** as **Source IP Type**.
Source IP Subnet	Type the subnet mask here if you choose **Subnet** as **Source IP Type**.
Destination IP Type	Determine the IP type as the destination.

Item	Description
	None None Single Subnet
Destination IP	Type the IP address here if you choose **Single** as **Destination IP Type**.
Destination Subnet	Type the subnet mask here if you choose **Subnet** as **Destination IP Type**.
Source Start Port	Type a value as the source start port. Such value will be available only TCP/UDP is selected as the protocol.
Source End Port (optional)	Type a value as the source end port. Such value will be available only TCP/UDP is selected as the protocol.
Destination Start Port	Type a value as the destination start port. Such value will be available only TCP/UDP is selected as the protocol.
Destination End Port (optional)	Type a value as the destination end port. Such value will be available only TCP/UDP is selected as the protocol.
Action	Set the action that the router will perform for the packets through the protocol of IPv6. ACCEPT ACCEPT DROP **ACCEPT –** If the IPv6 packets fit the condition listed in this page, the router will let it pass through. **DROP-** If the IPv6 packets fit the condition listed in this page, the router will block it.

3.11.4 Routing Table

This page displays the routing table for the protocol of IPv6.

IPv6 >> Routing Table

Routing Table | Refresh |

Destination	Gateway	Flags	Interface
2000::/64	::	U	eth2.2
fe80::/64	::	U	eth2
fe80::/64	::	U	ra0
fe80::/64	::	U	eth2.1
fe80::/64	::	U	eth2.3
fe80::/64	::	U	eth2.4
fe80::/64	::	U	eth2.5
fe80::/64	::	U	br0
fe80::/64	::	U	eth2.2
ff02::1:2/128	ff02::1:2	U	eth2.2

Note : Flags may include U (route is up), H (target is a host), G (use gateway).

Available settings are explained as follows:

Item	Description
Destination	Display the IPv6 routing destination address and prefix length.
Gateway	Display the IPv6 gateway address.
Flags	Display the routing status.
Interface	Display the interface name (eth0, eth1, fp, etc..) that used to transfer packets with addresses matching the prefix.

After finishing all the settings here, please click **OK** to save the configuration.

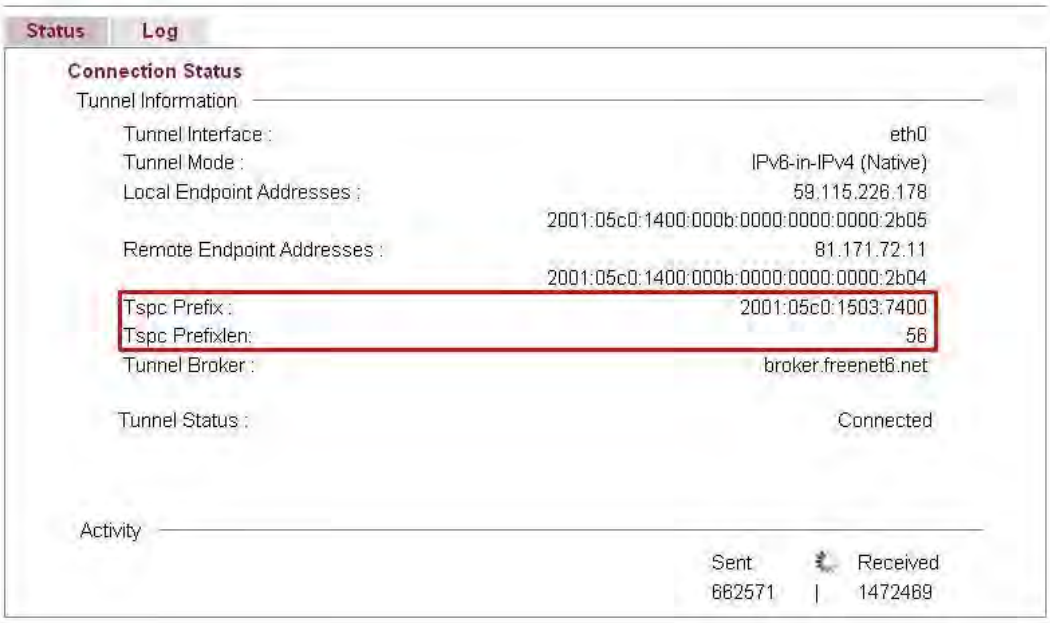
3.11.5 TSPC Status

IPv6 TSPC status web page could help you to diagnose the connection status of TSPC. TSPC log contains some debug information from program.

If TSPC has not configured properly, the router will display the following page when the user tries to connect through TSPC connection.

When TSPC configuration has been done, the router will start to connect. The connecting page will be shown as below:

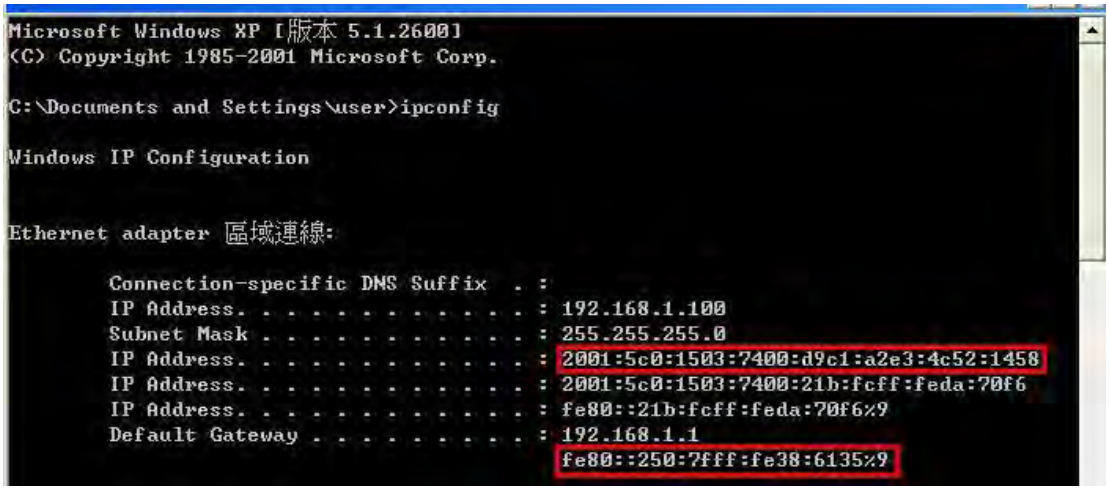
When the router detects all the information, the screen will be shown as follows. One set of **TSPC prefix** and **prefix length** will be obtained after the connection between TSPC and Tunnel broker built.



Each item is explained as follows:

Item	Description
Connection Status	It will bring out different pages to represent IPv6 disconnection, connecting and connected.
Tunnel Information	Display interface name (used to send TSPC prefix), tunnel mode, local endpoint addresses, remote endpoint address, TSPC Prfix, TSPC Prefixlen (prefix length), tunnel broker and so on.
Tunnel Status	**Disconnected** - The remote client doesn't connect to the tunnel server. **Connecting** - The remote client is connecting to the tunnel server. **Connected** – The remote client has been connected to the tunnel server.
Activity	**Sent** - sent to the tunnel (RX bytes). **Received** - received from the tunnel (RX bytes).

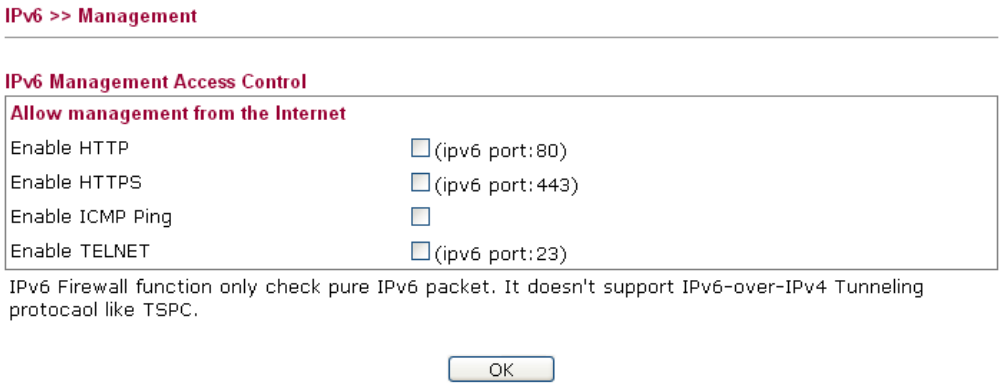
When the router connects to the tunnel broker, the router will use RADVD to transmit the prefix to the PC on LAN. Next, the PC will generate one set of IPv6 public IP (see the figure below). Users can use such IP for connecting to IPv6 network.



When your PC obtains the IPv6 address, please connect to http://www.ipv6.org. If your PC access Internet via IPv6 connection, your IPv6 address will be shown on the web page immediately. Refer to the following figure.

3.11.6 Management

This page allows you to manage the settings for IPv6 access control including settings of HTTP, HTTPs, ICMP Ping and TELNET by using IPv6 protocol. Check the box and type the port number respectively to enable the remote management of services.



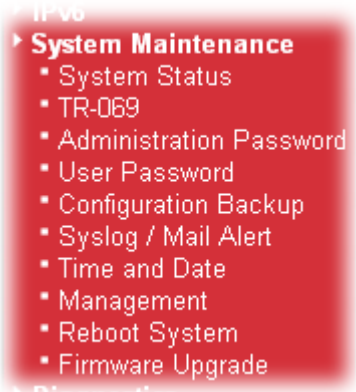
Available settings are explained as follows:

Item	Description
Allow management from the Internet	**Enable HTTP/HTTPS/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 the service.

3.12 System Maintenance

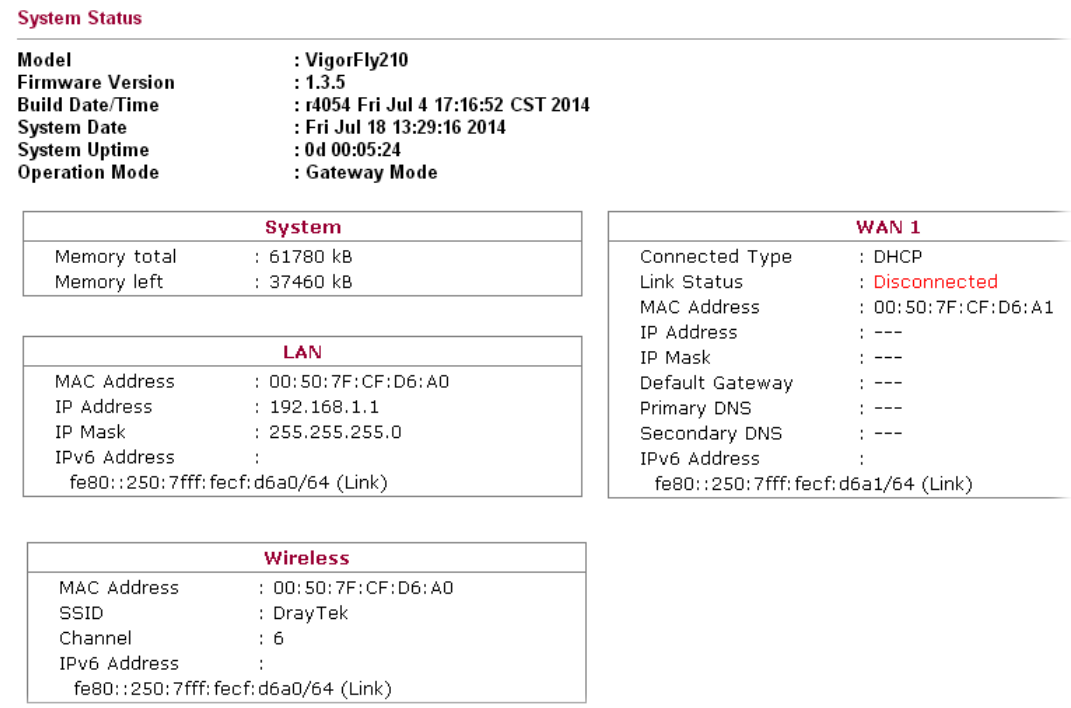
For the system setup, there are several items that you have to know the way of configuration: System Status, Administrator Password, Configuration Backup, Syslog/Mail Alert, Time and Date, Management, Reboot System, and Firmware Upgrade.

Below shows the menu items for System Maintenance.



3.12.1 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.



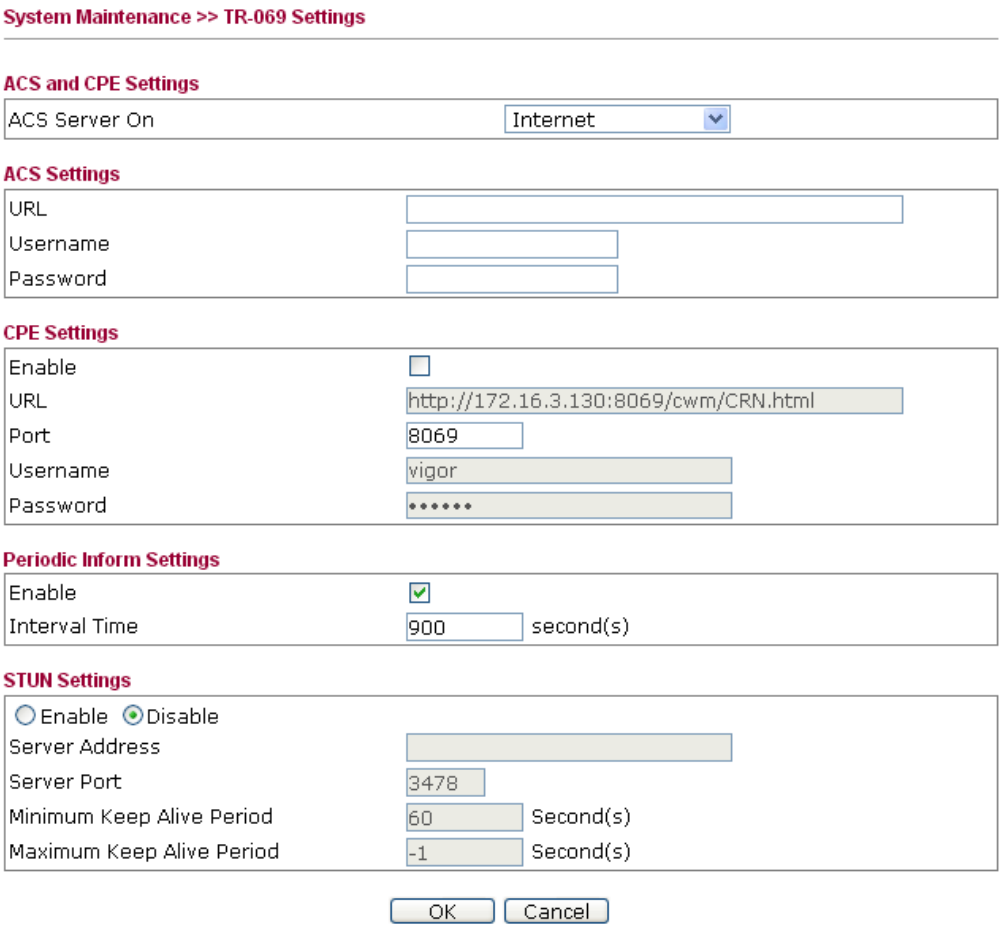
Each item is explained as follows:

Item	Description
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.

Item	Description
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.
System	**Memory total -** Display the total dynamic RAM size for the whole system. **Memory left -** Display the remaining RAM size for the whole system.
LAN	**MAC Address -** Display the MAC address of the LAN Interface. **IP Address -** Display the IP address of the LAN Interface. **IP Mask -** Display the subnet mask address of the LAN interface. **IPv6 Address** - Display the IPv6 address of the LAN Interface.
Wireless	**MAC Address -** Display the MAC address of the WLAN Interface. **SSID -** Display the SSID of this router. **Channel -** Display the channel that wireless LAN used. **IPv6 Address** - Display the IPv6 address of the wireless LAN Interface.
WAN 1	**Connected Type** - Display the network connection type for this router. **Link Status -** Display if current network is connected or not. **MAC Address -** Display the MAC address of the WAN Interface. **IP Address -** Display the IP address of the WAN Interface. **IP Mask -** Display the subnet mask address of the WAN interface. **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. **IPv6 Address** - Display the IPv6 address of the WAN1.

3.12.2 TR-069

Vigor router with TR-069 is available for matching with VigorACS server. Such page provides VigorACS and CPE settings under TR-069 protocol. All the settings configured here is for CPE to be controlled and managed with VigorACS server. Users need to type URL, username and password for the VigorACS server that such device will be connected. However URL, username and password under CPE client are fixed that users cannot change it. The default CPE username and password are "vigor" and "password". You will need it when you configure VigorACS server.



Available parameters are explained as follows:

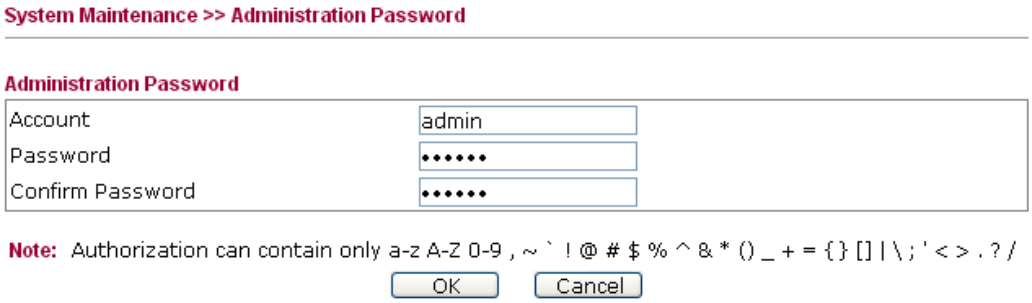
Item	Description
ACS Settings	Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to VigorACS user's manual for detailed information. **URL** - Type the URL for VigorACS server. If the connected CPE needs to be authenticated, please set URL as the following and type username and password for VigorACS server: ***http://{IP address of VigorACS}:8080/ACSServer/services/ACSServlet*** If the connected CPE does not need to be authenticated please set URL as the following: ***http://{IP address of***

	VigorACS}:8080/ACSServer/services/UnAuthACSServlet **Username/Password** - Type username and password for ACS Server for authentication. For example, if you want to use such CPE with VigorACS, you can type as the following: **Username*: acs*** **Password*: password***
CPE Settings	Such information is useful for Auto Configuration Server. **Enable/Disable** – Allow/Deny the CPE Client to connect with Auto Configuration Server. **Port** – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.
Periodic Inform Settings	**Disable –** The system will not send inform message to ACS server. **Enable –** The system will send inform message to ACS server periodically (with the time set in the box of interval time). The default setting is **Enable**. Please set interval time or schedule time for the router to send notification to CPE. Or click **Disable** to close the mechanism of notification.
STUN Settings	The default is **Disable**. If you click **Enable**, please type the relational settings listed below: **Server IP –** Type the IP address of the STUN server. **Server Port –** Type the port number of the STUN server. **Minimum Keep Alive Period –** If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is “60 seconds”. **Maximum Keep Alive Period –** If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of “-1” indicates that no maximum period is specified.

After finishing all the settings here, please click **OK** to save the configuration.

3.12.3 Administration Password

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



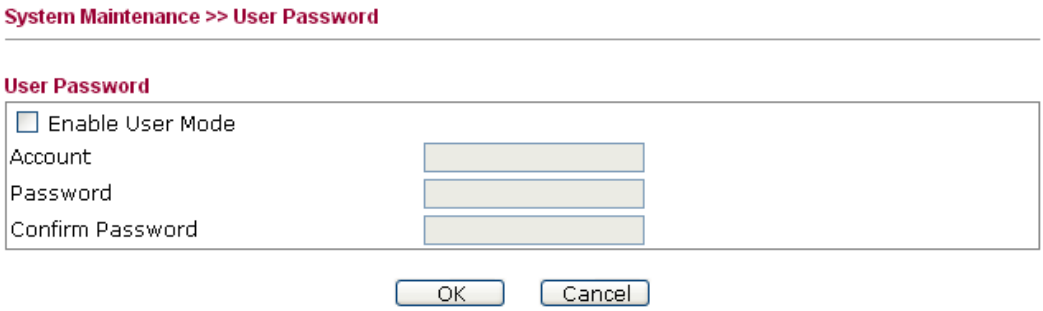
Available parameters are explained as follows:

Item	Description
Account	Type in the name for login.
Password	Type in new password in this filed.
Confirm Password	Type in the new password again.

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

3.12.4 User Password

Sometimes, you may want to access into User Mode to configure the web settings for some reason. Vigor router allows you to set new user password to login into the WUI to fit your request. Simply open **System Maintenance>>User Password**.



Available parameters are explained as follows:

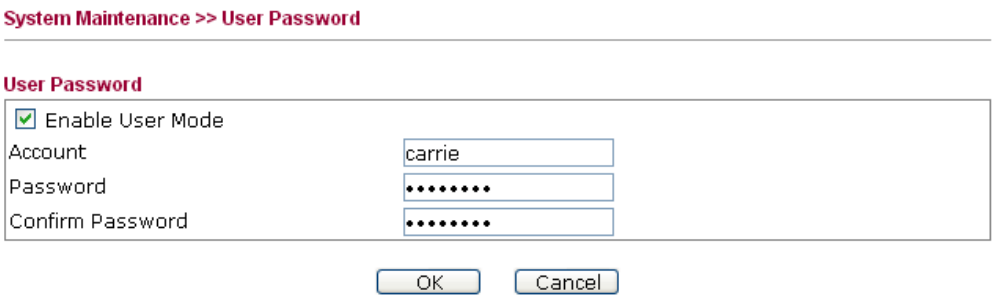
Item	Description
Enable User Mode	Check this box to enable user mode operation. If you do not check this box, you cannot access into the user mode operation even if you enter user password in login page.
Account	Type in a new account as the username for accessing into user mode for simple web configuration.
Password	Type in new password in this field.
Confirm Password	Type in the new password again.

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

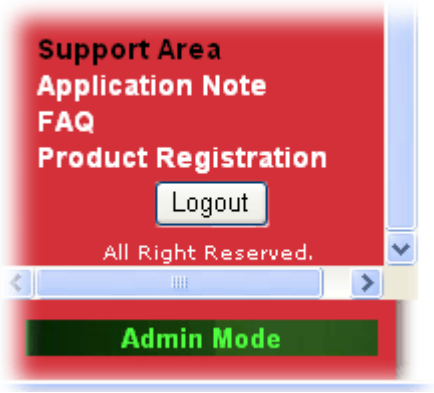
Below shows an example for accessing into User Operation with User Password.

1. Open **System Maintenance>>User Password**.

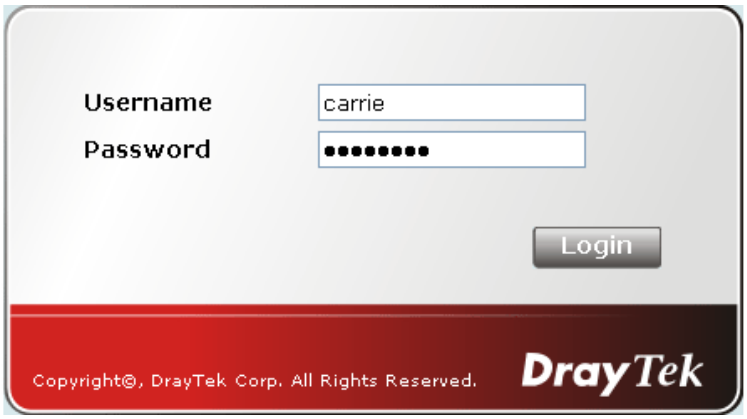
2. Check the box of **Enable User Mode for simple web configuration** to enable user mode operation. Type a new password in the field of New Password and click **OK**.



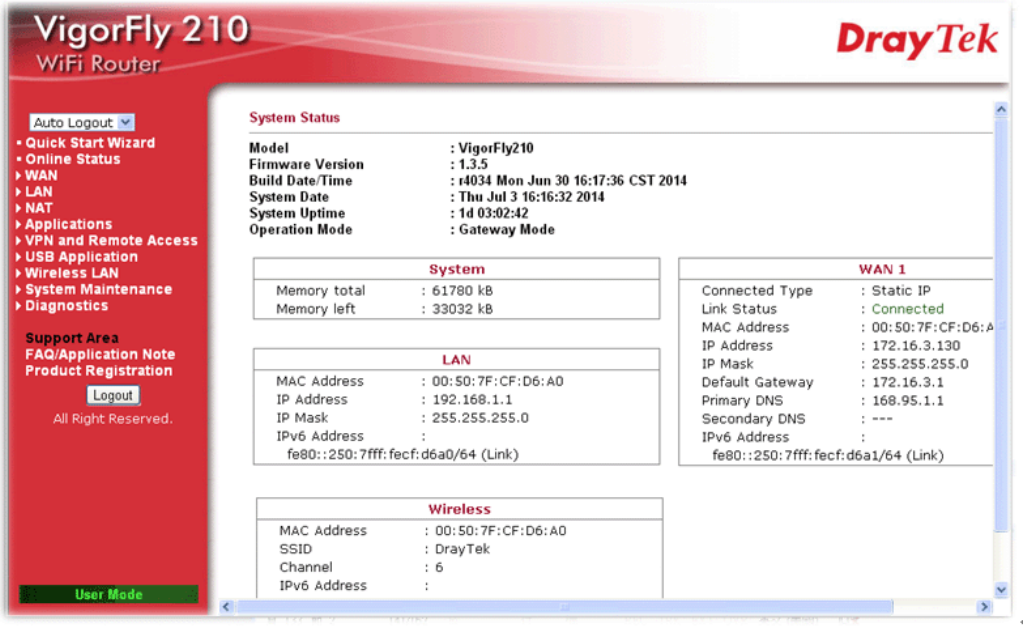
3. Log out Vigor router web user interface.



4. The following window will be open to ask for username and password. Type the new user password in the filed of **Password** and click **Login**.



5. The main screen with User Mode will be shown as follows.



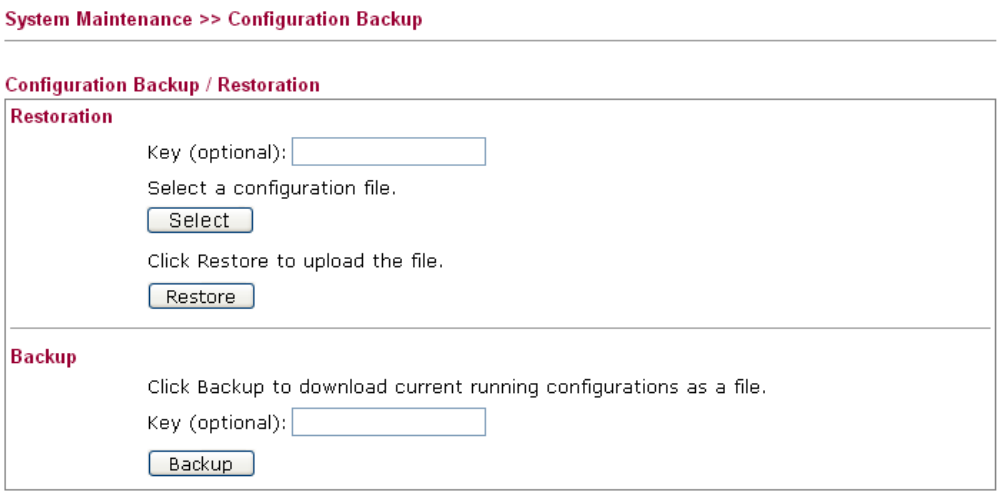
Settings to be configured in User Mode will be less than settings in Admin Mode. Only basic configuration settings will be available in User Mode.

3.12.5 Configuration Backup

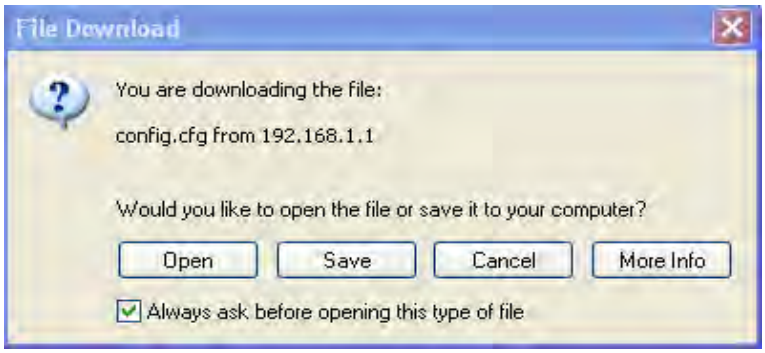
Backup the Configuration

Follow the steps below to backup your configuration.

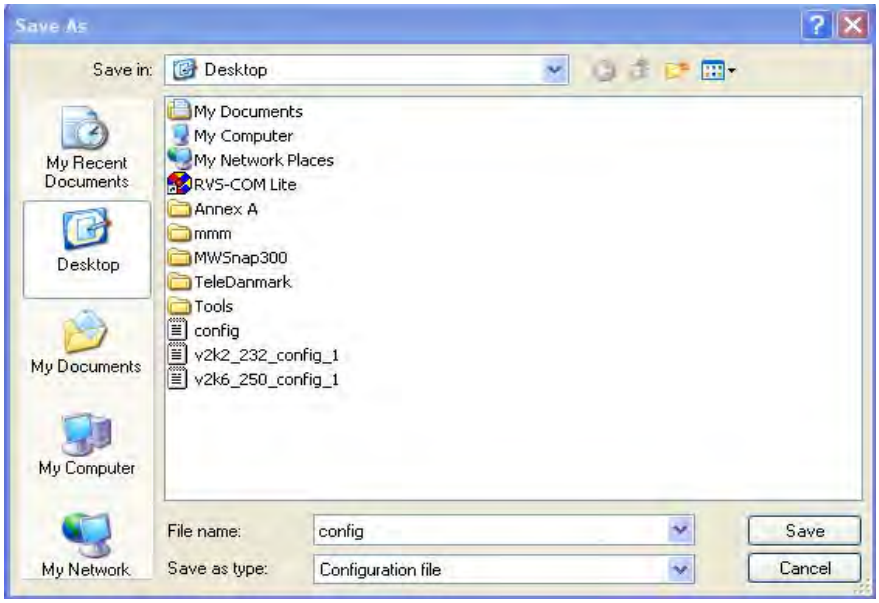
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.



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.



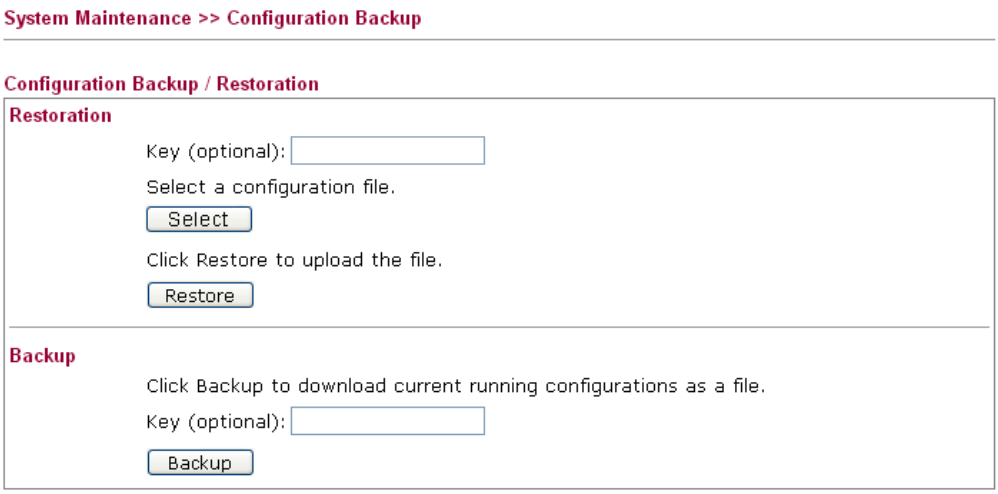
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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.

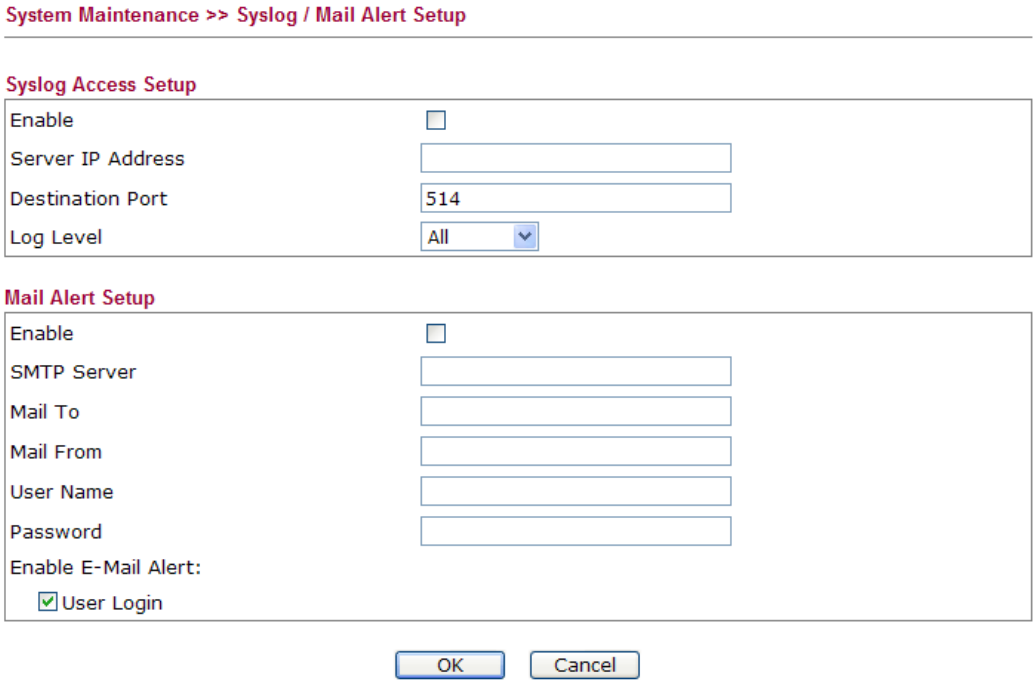


2. Click **Select** button to choose the correct configuration file for uploading to the router.
3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

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

3.12.6 Syslog/Mail Alert

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



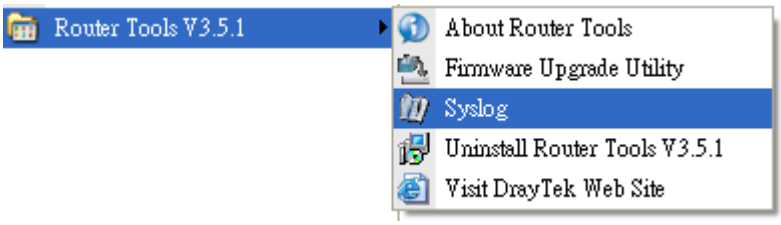
Available parameters are explained as follows:

Item	Description
Syslog Access Setup	**Enable** - 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. All All Info Warning Error
Mail Alert Setup	**Enable** - 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.

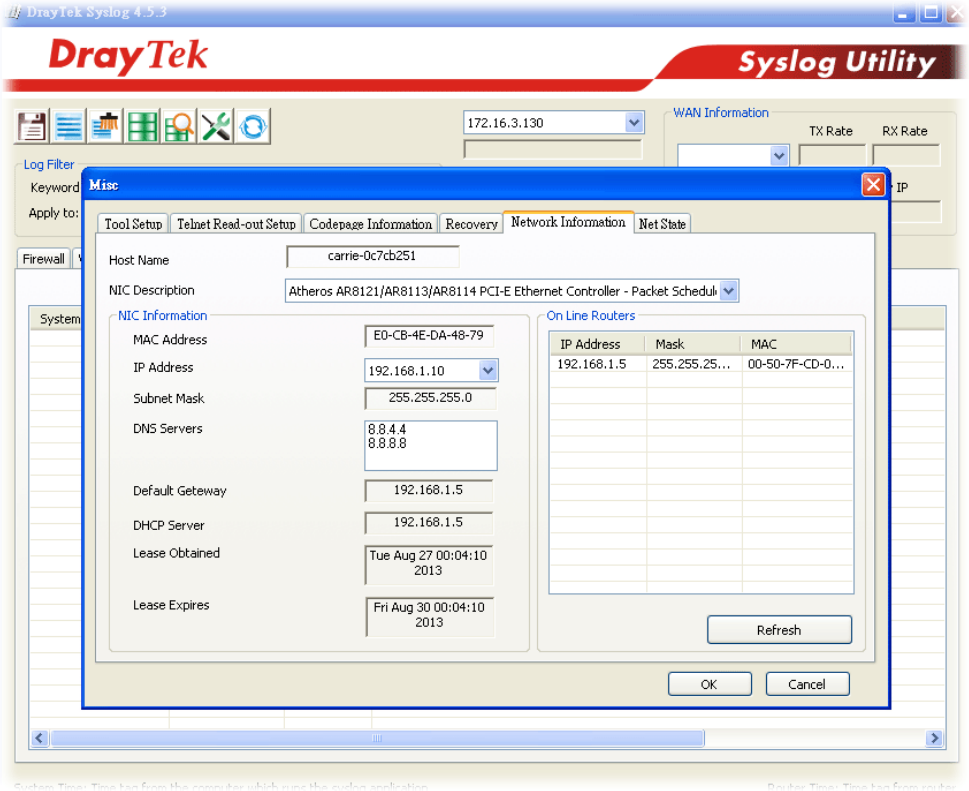
Click **OK** to save these settings.

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.

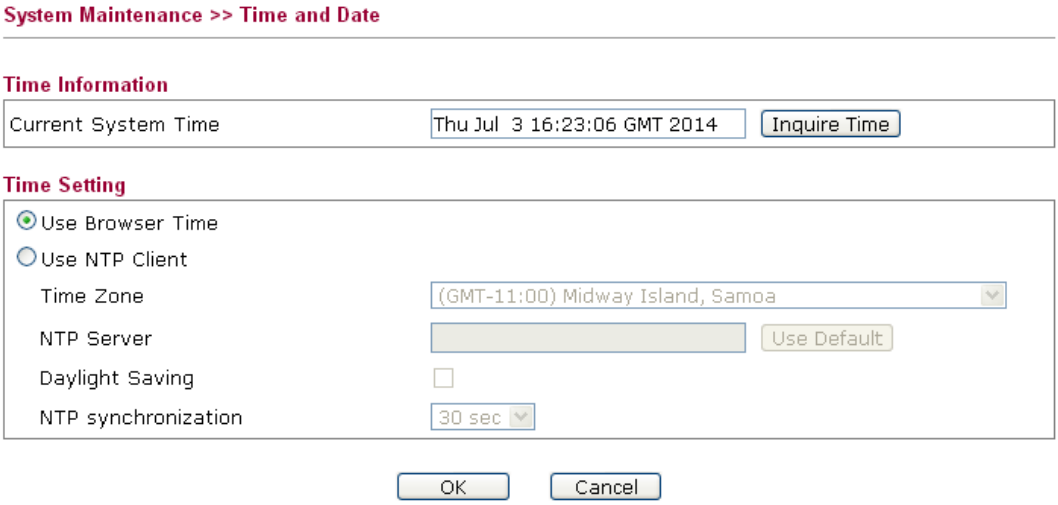


3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.



3.12.7 Time and Date

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



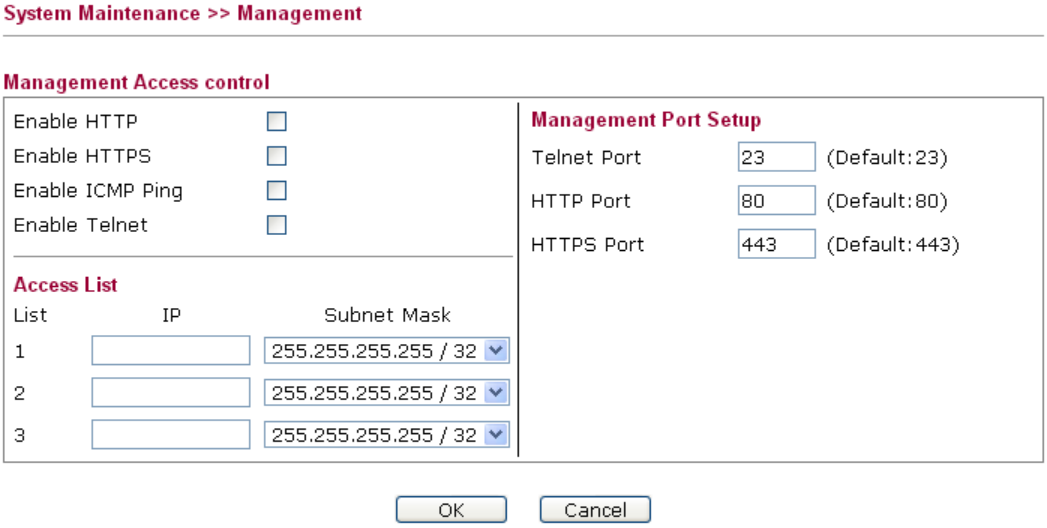
Available parameters are explained as follows:

Item	Description
Current System Time	Click **Inquire Time** to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use NTP Client	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time Zone	Select the time zone where the router is located.
NTP Server	Type a new NTP server.
Daylight Saving	Check the box to enable the daylight saving. Such feature is available for certain area.
NTP synchronization	Select a time interval for updating from the NTP server.

After finishing all the settings here, please click **OK** to save the configuration.

3.12.8 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.



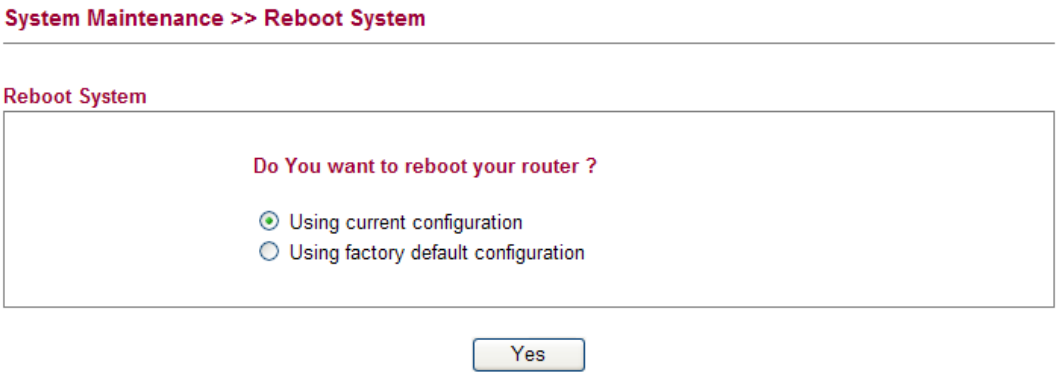
Available parameters are explained as follows:

Item	Description
Enable HTTP/HTTPS/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.
Management Port Setting	Specify user-defined port numbers for the Telnet, HTTP and HTTPS servers.

After finishing all the settings here, please click **OK** to save the configuration.

3.12.9 Reboot System

The web user interface 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.

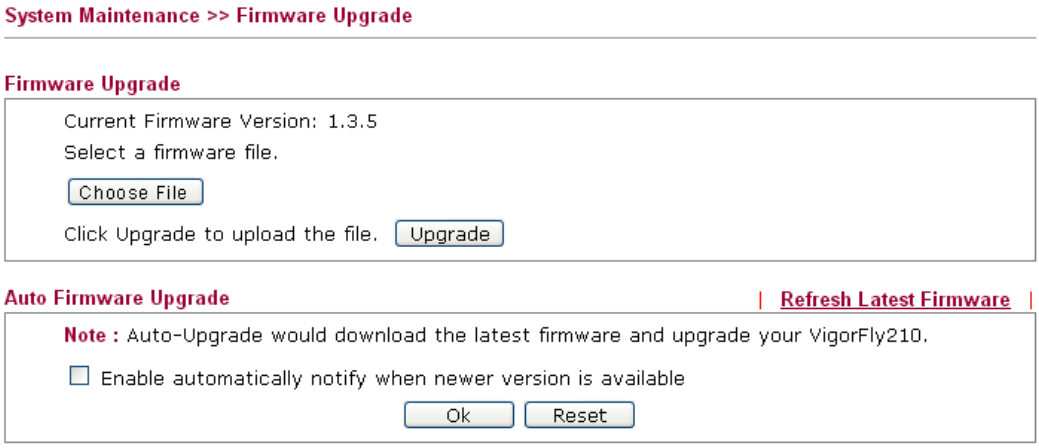
Note: When the system pops up Reboot System web page after you configure web settings, please click **Yes** to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

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

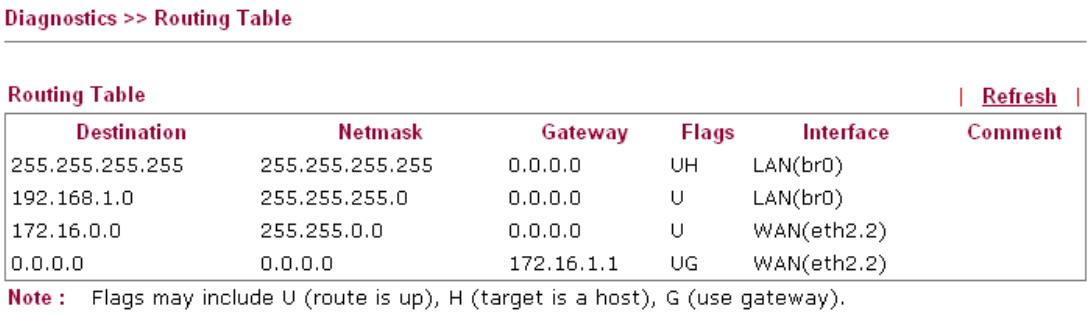
3.13 Diagnostics

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

Below shows the menu items for Diagnostics.

3.13.1 Routing Table

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

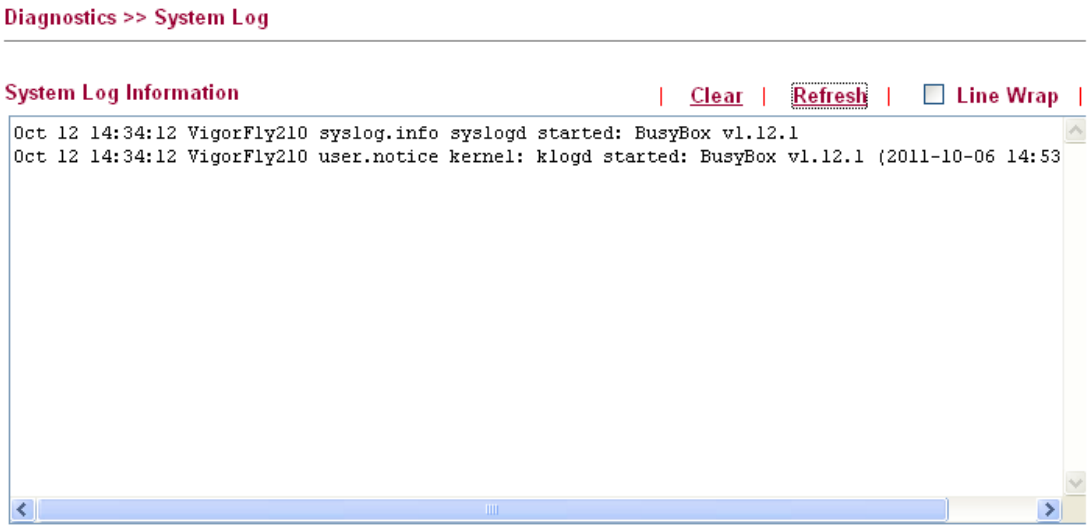


Each item is explained as follows:

Item	Description
Destination	Display the IP address of the routing.
Netmask	Display the subnet mask of the routing.
Gateway	Display the gateway IP address of the routing.
Flags	Display the routing status.
Interface	Display the interface name (eth0, eth1, fp, etc..) that used to transfer packets with addresses matching the prefix.
Comment	Display the brief explanation for the routing.

3.13.2 System Log

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



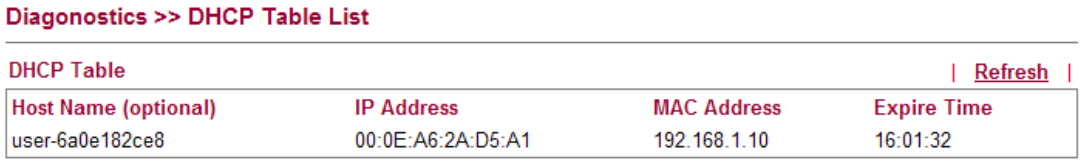
Each item is explained as follows:

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

3.13.3 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.



Each item is explained as follows:

Item	Description
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.

3.13.4 Data Flow Monitor

This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds.

Click **Diagnostics** and click **Data Flow Monitor** to open the web page. You can click **IP Address**, **TX rate**, **RX rate** or **Session** link for arranging the data display.

Diagnostics >> Data Flow Monitor

Page: 1 Auto-refresh: | Refresh |

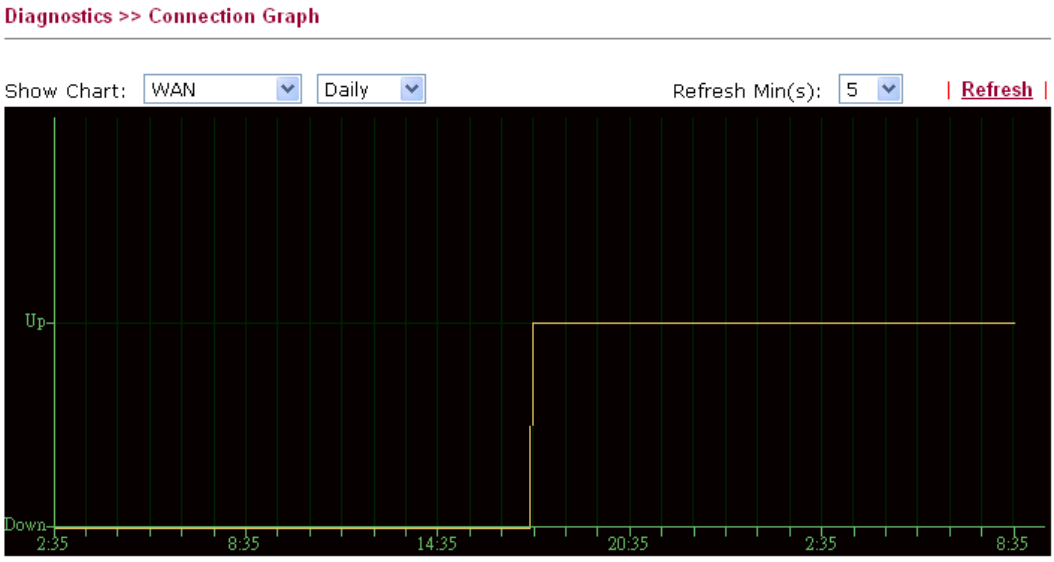
Index	IP Address	TX rate(Kbps)	RX rate(Kbps)	Sessions
1	192.168.1.10	1	0	31
Total		1	0	31

Each item is explained as follows:

Item	Description
Auto-refresh	Check this box to let the system automatically refresh this page.
Refresh	Click this link to refresh this page manually.
Index	Display the number of the data flow.
IP Address	Display the IP address of the monitored device.
TX rate (kbps)	Display the transmission speed of the monitored device.
RX rate (kbps)	Display the receiving speed of the monitored device.
Sessions	Display the session number.

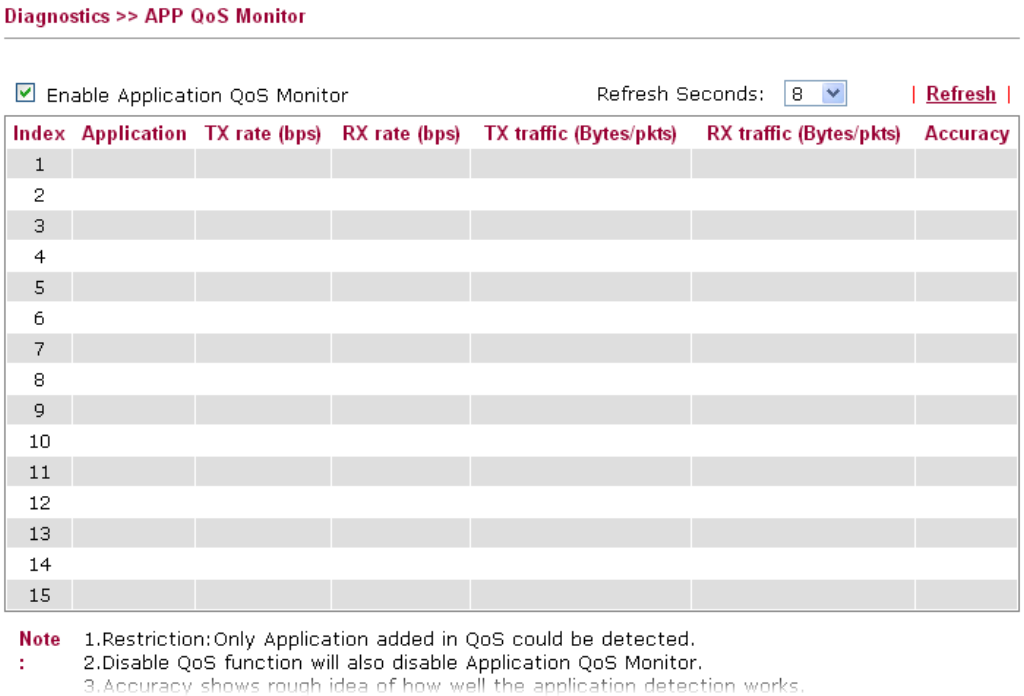
3.13.5 Connection Graph

Click **Diagnostics** and click **Connection Graph** to open the web page. Choose WAN or Backup WAN for viewing different connection graph. Click **Refresh** to renew the graph at any time.



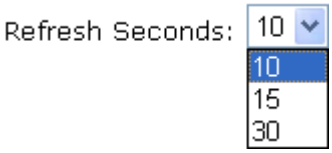
3.13.6 APP QoS Monitor

This page displays the APP QoS monitoring status.



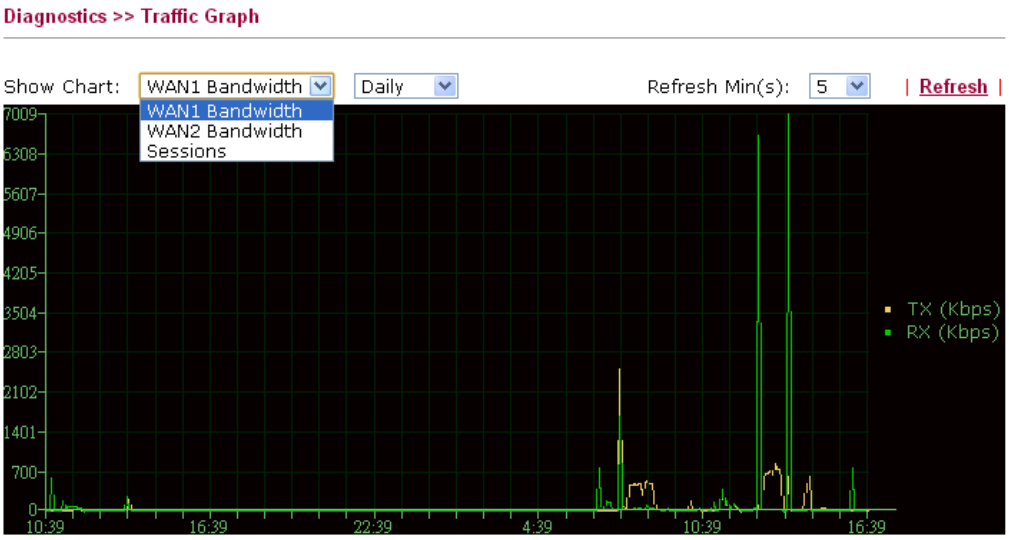
Each item is explained as follows:

Item	Description
Enable Application QoS Monitor	Check the box to perform the application QoS monitoring.

Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically. 
Refresh	Click this link to refresh this page manually.
Application	Display the name of the application.
TX rate (kbps)	Display the transmission speed of the monitored application.
RX rate (kbps)	Display the receiving speed of the monitored application.
TX traffic (kbps)	Display the transmission traffic of the monitored application.
RX traffic (kbps)	Display the receiving traffic of the monitored application.
Accuracy	Display how well the application detection works.

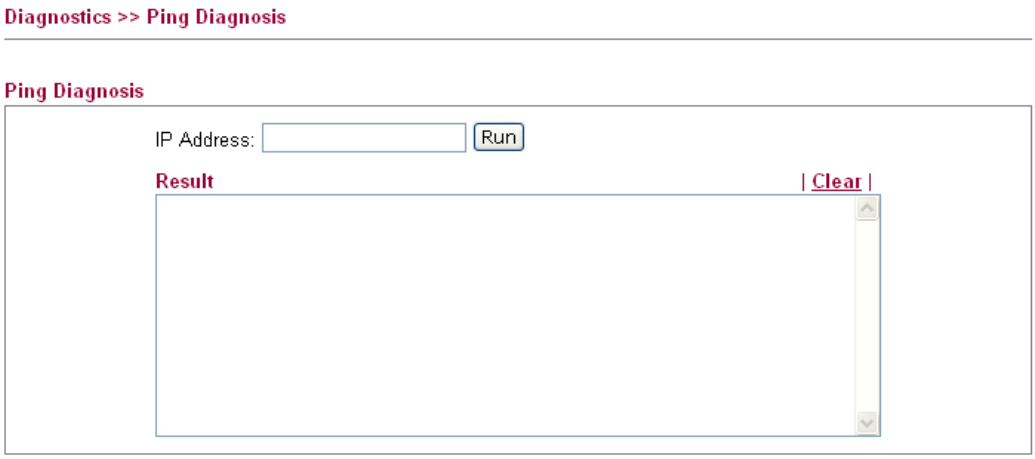
3.13.7 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1/WAN2 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Refresh** to renew the graph at any time.



3.13.8 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to pen the web page.



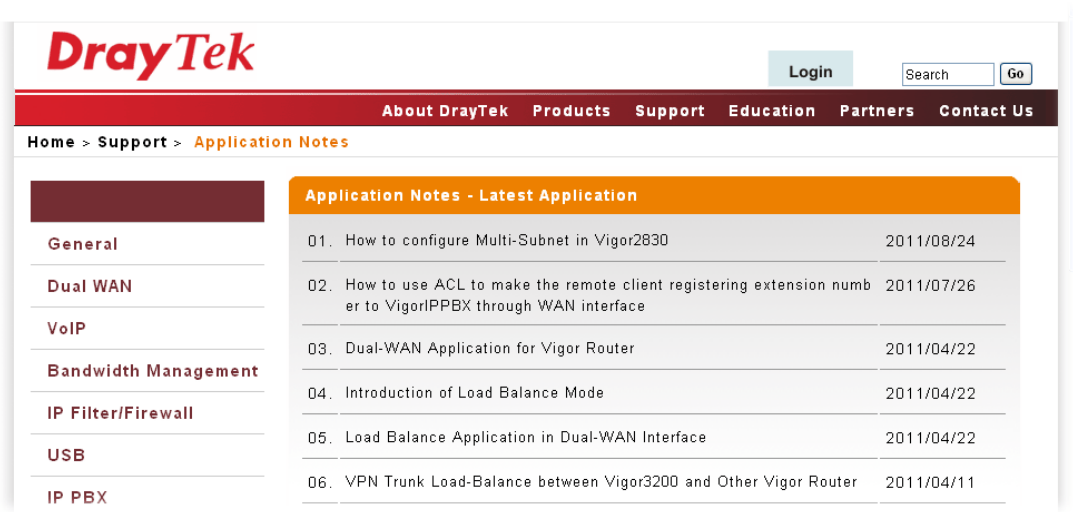
Each item is explained as follows:

Item	Description
IP Address	Type in the IP address of the Host/IP that you want to ping.
Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

3.14 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.

Refer to **section 2.6 Registering Vigor Router** for detailed information.

This page is left blank.

4 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.

4.1 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.

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

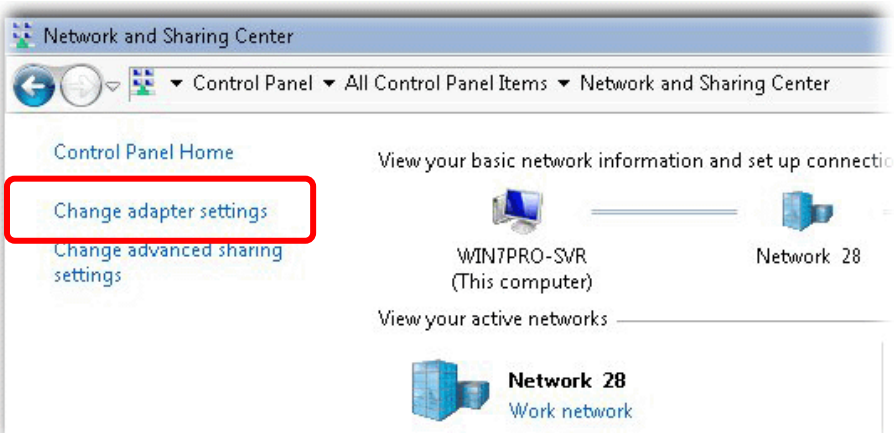
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

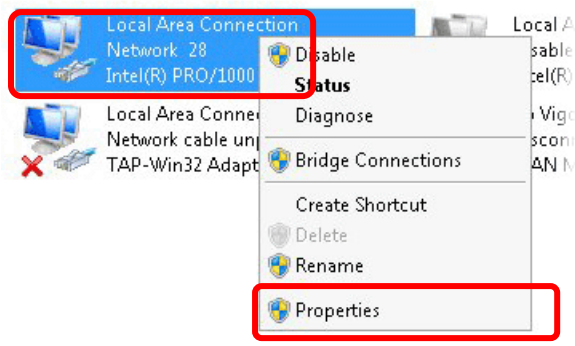
The example is based on Windows 7 (Professional Edition). As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.DrayTek.com**.

1. Open **All Programs>>Getting Started>>Control Panel.** Click **Network and Sharing Center.**

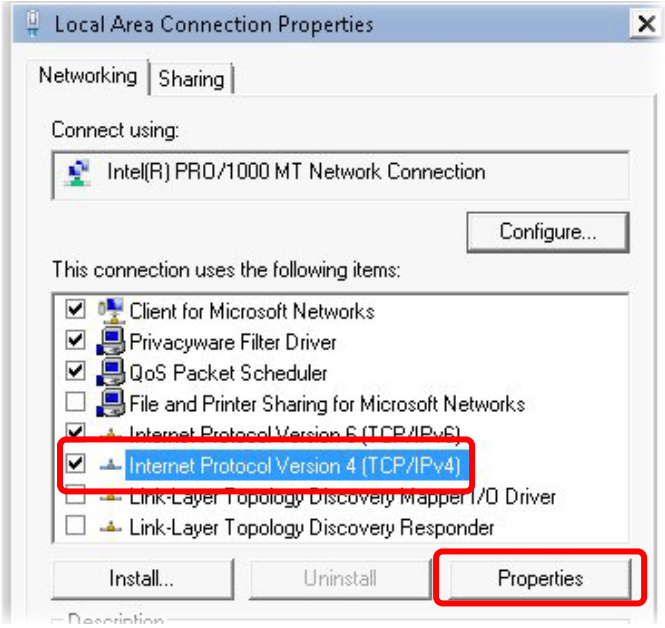
2. In the following window, click **Change adapter settings**.



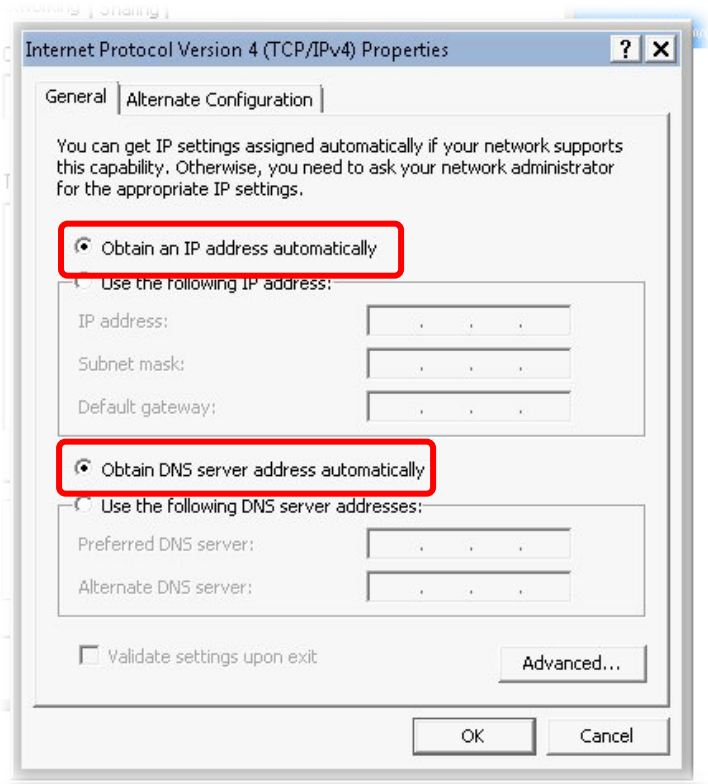
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



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

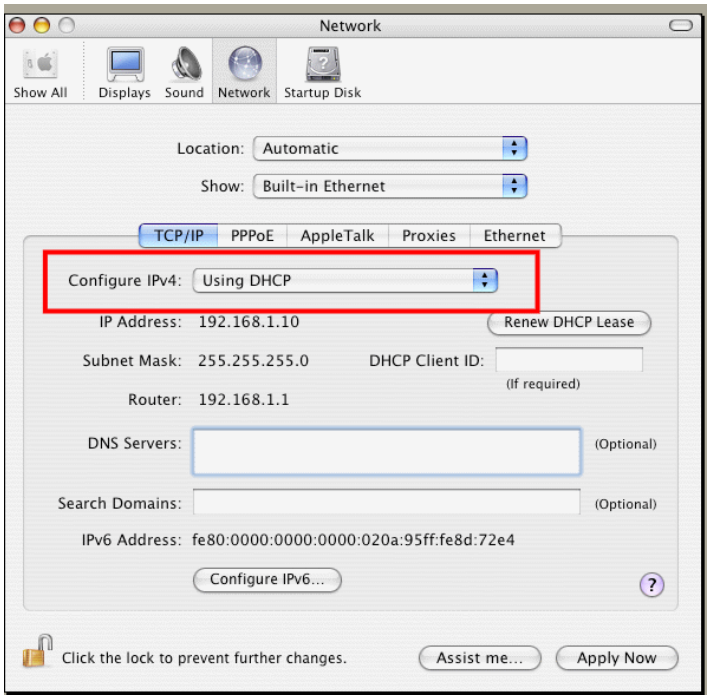


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



For Mac OS

1. Double click on the current used Mac OS 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.


Network
Show All
Displays
Sound
Network
Startup Disk
Location: Automatic
Show: Built-in Ethernet
TCP/IP
PPPoE
AppleTalk
Proxies
Ethernet
Configure IPv4: Using DHCP
IP Address: 192.168.1.10
Renew DHCP Lease
Subnet Mask: 255.255.255.0
DHCP Client ID:
(If required)
Router: 192.168.1.1
DNS Servers:
(Optional)
Search Domains:
(Optional)
IPv6 Address: fe80:0000:0000:0000:020a:95ff:fe8d:72e4
Configure IPv6...
Click the lock to prevent further changes.
Assist me...
Apply Now

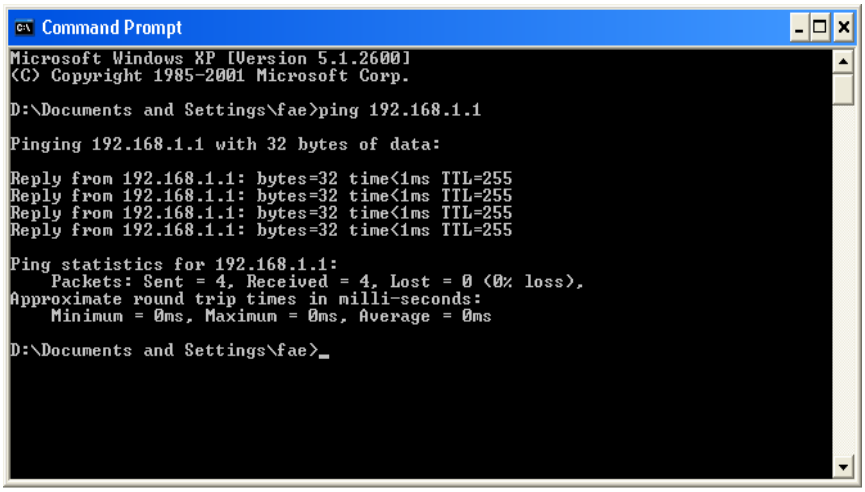
4.3 Pinging the Router from Your Computer

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 4.2)

Please follow the steps below to ping the router correctly.

For Windows

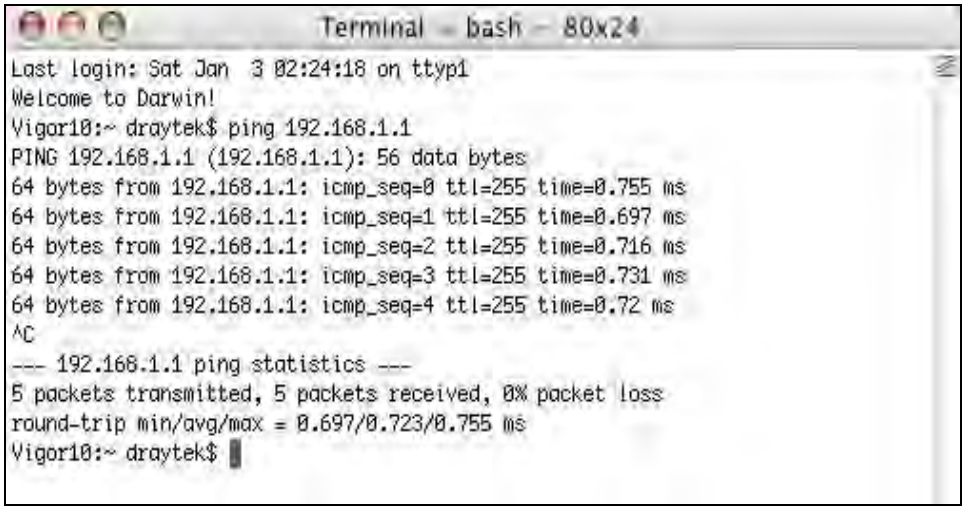
1. Open the **Command** Prompt window (from **Start menu**> **Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista/7). The DOS command dialog will appear.



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.

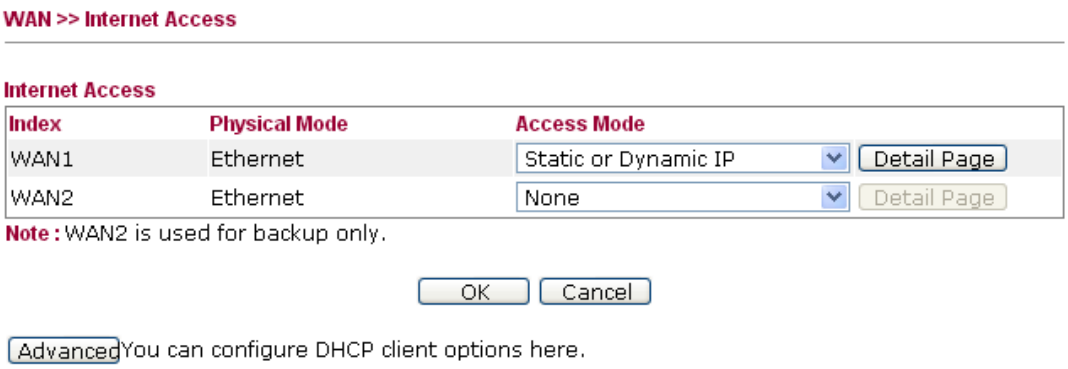
For Mac OS (Terminal)

1. Double click on the current used Mac OS 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.



4.4 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/ PPPoE/PPTP/L2TP/3G/4G for reviewing the settings that you configured previously.



4.5 Backing to Factory Default Setting If Necessary

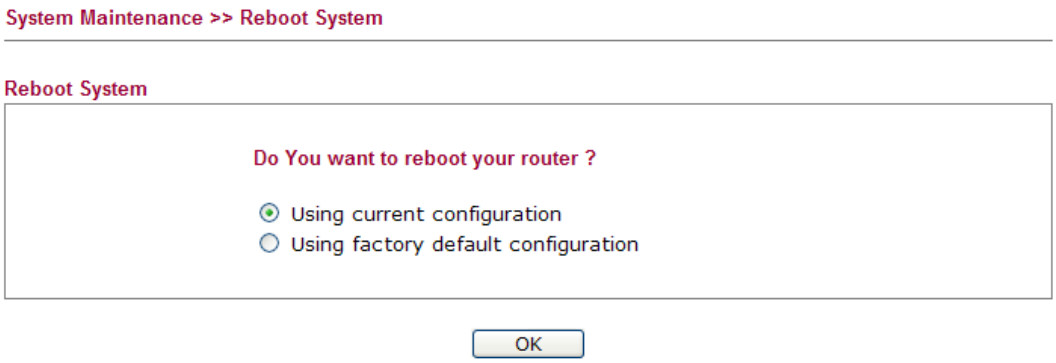
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

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.

4.6 Contacting DrayTek

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.