DrayTek

VigorPro 5510 Series
Unified Security Firewall
User's Guide

Version: 1.0

Date: 2007/10/16

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

Please consult the DrayTek web site for more information on newest firmware, tools and documents. For more detailed information, please refer to http://www.draytek.com

Parts of the anti-virus features are powered by Kaspersky Lab ZAO. For more detailed information, please refer to http://www.kaspersky.com.

European Community Declarations

Manufacturer: DrayTek Corp.
Address: No. 26, Fu Shing Road, HuKou County, HsinChu Industrial Park, Hsin-Chu, Taiwan 303
Product: VigorPro 5510

DrayTek Corp. declares that VigorPro 5510 Series is in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

The product conforms to the requirements of Electro-Magnetic Compatibility (EMC) Directive 89/336/EEC by complying with the requirements set forth in EN55022/Class A and EN55024/Class A.

The product conforms to the requirements of Low Voltage (LVD) Directive 73/23/EEC by complying with the requirements set forth in EN60950.

Regulatory Information

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A 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 use 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 form 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.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

Warning: This device might cause interference of radio frequency under the environment of dwelling. In such condition, the users might be asked to adopt some proper strategies.

Please visit “www.draytek.com/about_us/Regulatory.php”

Table of Contents

1 Preface

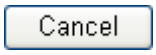
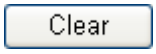
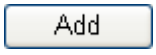
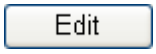
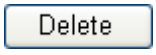
VigorPro 5510 is a UTM router with dual-WAN interface. It provides policy-based load-balance, fail-over and BoD (Bandwidth on Demand), also it integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

By adopting hardware-based VPN platform, hardware encryption of AES/DES/3DS and hardware key hash of SHA-1/MD5, the router increases the performance of VPN greatly, and offers several protocols (such as IPSec/PPTP/L2TP) with up to 200 VPN tunnels.

The object-originated design used in SPI (Stateful Packet Inspection) firewall allows users to set firewall policy with ease. CSM (Content Security Management) provides users control and management in IM (Instant Messenger), P2P (Peer to Peer), Web Content Filter and URL Content Filter more efficiency than before. By the way, DoS/DDoS prevention and URL/Web content filter strengthen the security outside and control inside.

1.1 Web Configuration Buttons Explanation

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

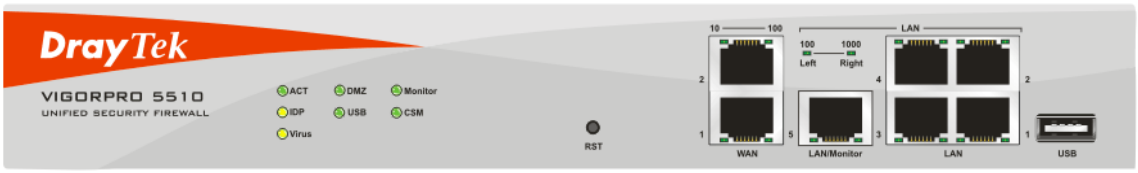
	Save and apply current settings.
	Cancel current settings and recover to the previous saved settings.
	Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings.
	Add new settings for specified item.
	Edit the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

Note: For the other buttons shown on the web pages, please refer to Chapter 3 for detailed explanation.

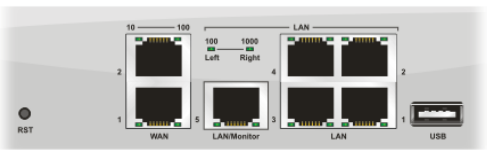
1.2 LED Indicators and Connectors

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

1.2.1 For VigorPro 5510



LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
		Off	The router is powered off.
IDP (Intrusion Detection and Prevention)		On (Yellow)	The anti-intrusion function is enabled.
Virus		On (Yellow)	The anti-virus function is enabled.
DMZ		On	DMZ Host is specified in certain site.
USB		On	A USB device is connected and active.
		Blinking	The data is transmitting.
Monitor		On	LAN traffic monitor is active.
CSM		On	The profile(s) for IM/P2P, Web Content Filter, and/or URL Content Filter application has been activated. (It is enabled from **Firewall >> General Setup**).
		Off	No IM/P2P, Web Content Filter, and/or URL Content Filter application has been activated.
LED on Connector			
WAN	10 (left LED)	On	The port is connected with 10Mbps.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	100 (right LED)	On	The port is connected with 100Mbps.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
LAN/Monitor LAN	100 (left LED)	On	The port is connected with 100Mbps.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	1000 (right LED)	On	The port is connected with 1000Mbps.
		Off	The port is disconnected.
		Blinking	The data is transmitting.

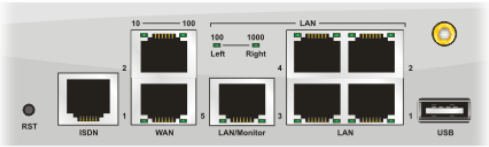


Interface	Description
RST (Factory Reset)	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.

WAN(1/2)	Connecter for remote networked devices.
LAN/Monitor	Connecter for local networked devices.
LAN (1-4)	Connecter for local networked devices.
USB	Connecter for a USB device.
	Connecter for a power cord with 100-240VAC (inlet).
	Power Switch. “1” is ON; “0” is OFF.

1.2.2 For VigorPro 5510Gi

LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
		Off	The router is powered off.
IDP (Intrusion Detection and Prevention)		On (Yellow)	The anti-intrusion function is enabled.
Virus		On (Yellow)	The anti-virus function is enabled.
DMZ		On	DMZ Host is specified in certain site.
USB		On	A USB device is connected and active.
		Blinking	The data is transmitting.
WLAN		On	Wireless access point is ready.
		Blinking	Ethernet packets are transmitting over wireless LAN.
		Off	The WLAN function is inactive.
Monitor		On	LAN traffic monitor is active.
CSM		On	The profile(s) for IM/P2P, Web Content Filter, and/or URL Content Filter application has been activated. (It is enabled from **Firewall** >> **General Setup**).
		Off	No IM/P2P, Web Content Filter, and/or URL Content Filter application has been activated.
ISDN		On	The ISDN service function is active.
		Blinking	A successful connection on the ISDN BRI B1/B2 channel.
LED on Connector			
WAN	10 (left LED)	On	The port is connected with 10Mbps.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	100 (right LED)	On	The port is connected with 100Mbps.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
LAN/Monitor LAN	100 (left LED)	On	The port is connected with 100Mbps.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	1000 (right LED)	On	The port is connected with 1000Mbps.
		Off	The port is disconnected.
		Blinking	The data is transmitting.



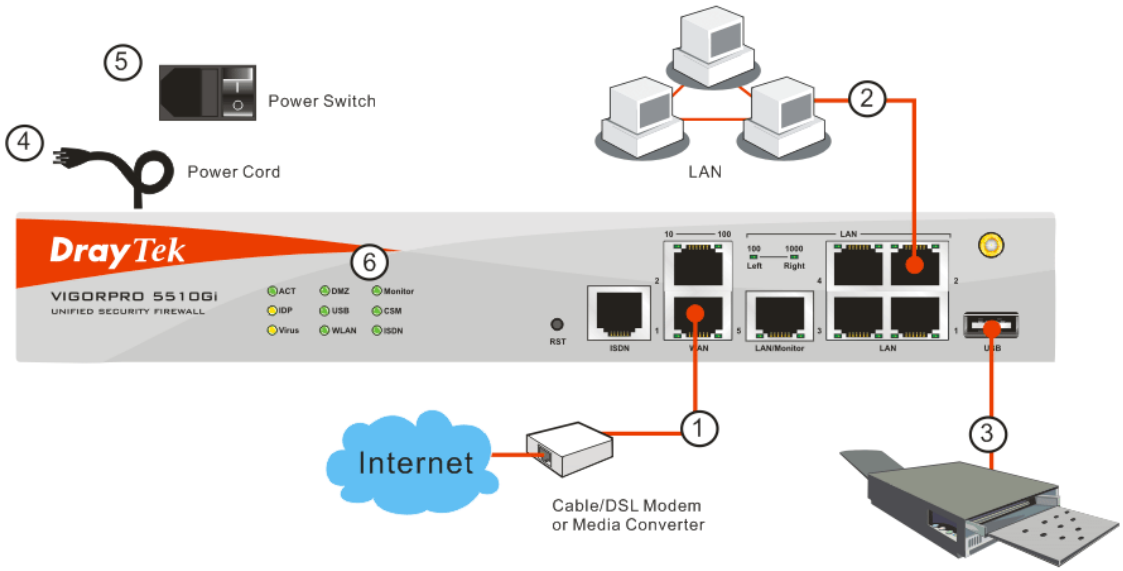
Interface	Description
RST (Factory Reset)	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default

	configuration.
ISDN	Connecter for ISDN line.
WAN(1/2)	Connecter for remote networked devices.
LAN/Monitor	Connecter for local networked devices.
LAN (1-4)	Connecter for local networked devices.
USB	Connecter for a USB device.
	Connecter for a power cord with 100-240VAC (inlet).
	Power Switch. “1” is ON; “0” is OFF.

1.3 Hardware Installation

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

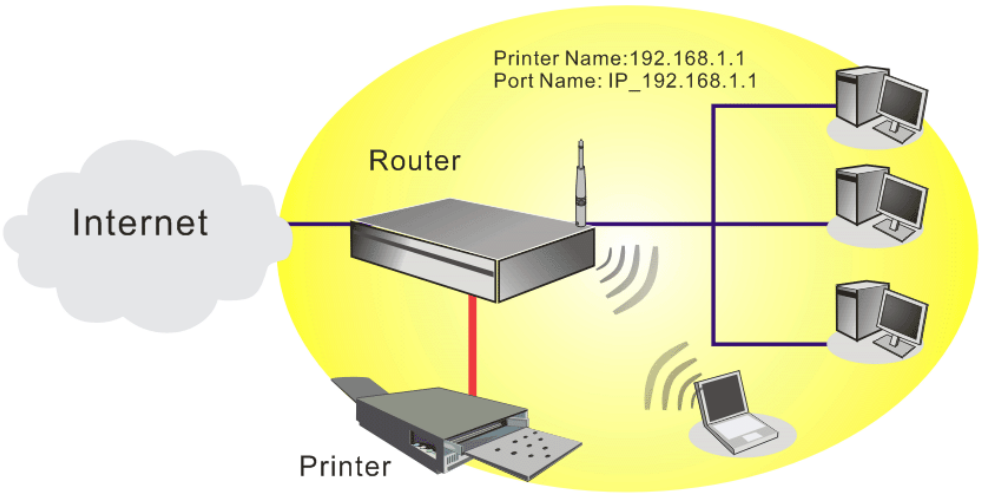
1. Connect a cable Modem/DSL Modem/Media Converter (depends on your requirement) to any WAN port of router with Ethernet cable (RJ-45). The **WAN1/WAN2** LED (Left or Right) will light up according to the speed (100 or 10) of the device that it connected.
2. Connect one end of an Ethernet cable (RJ-45) to one of the **LAN** ports of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer. The **LAN** LED (Left or Right) will light up according to the speed (100 or 10) of the device that it connected.
3. Connect one end of the power adapter to the router's power port on the rear panel, and the other side into a wall outlet.
4. Power on the device by pressing down the power switch on the rear panel.
5. The system starts to initiate. After completing the system test, the **ACT** LED will light up and start blinking.



(For the detailed information of LED status, please refer to section 1.2.)

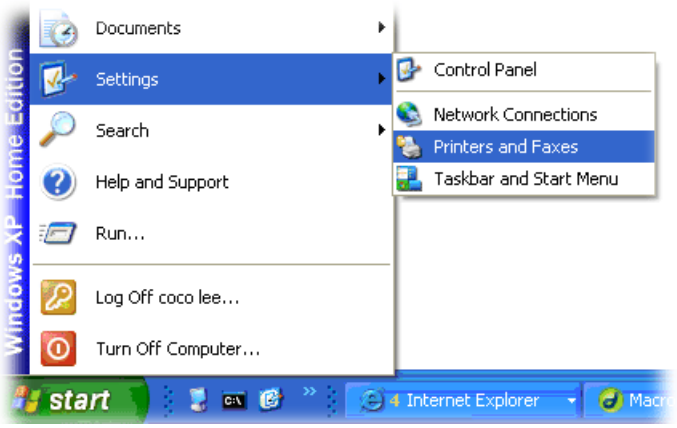
1.4 Printer Installation

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

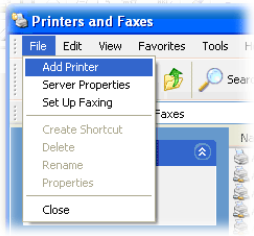


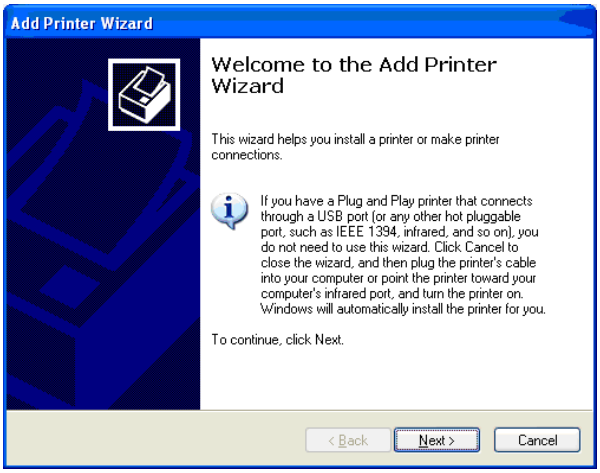
Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

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

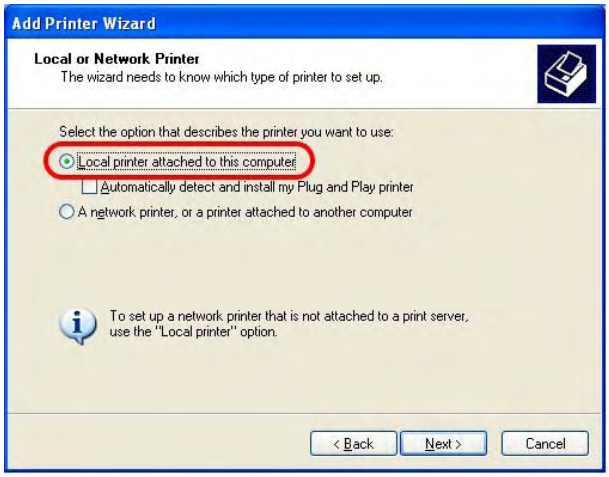


3. Open **File->Add a New Computer**. A welcome dialog will appear. Please click **Next**.



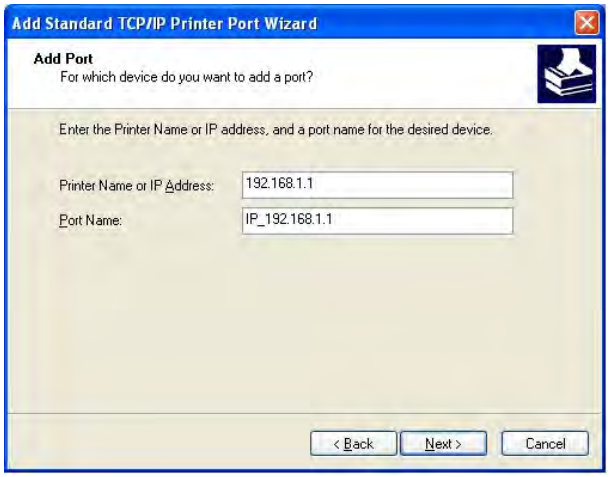


4. Click Local printer attached to this computer and click Next.



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

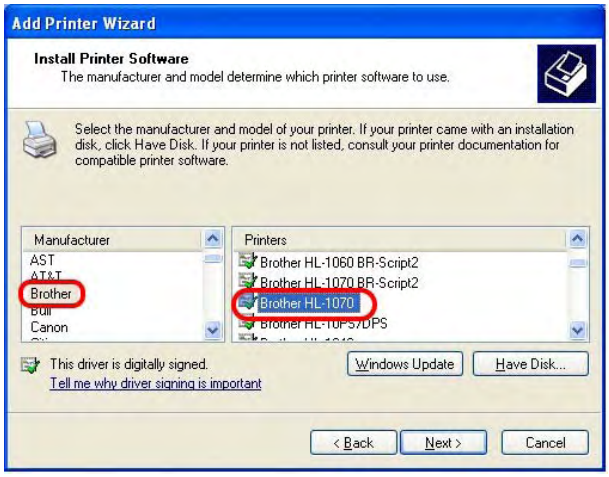
6. In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Printer Name or IP Address** and type **IP_192.168.1.1** as the port name. Then, click **Next**.



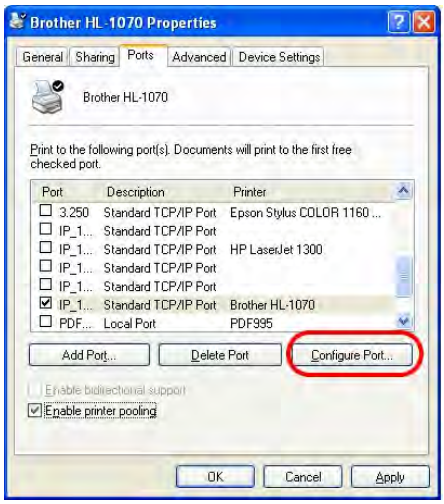
7. Click Standard and choose Generic Network Card.

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

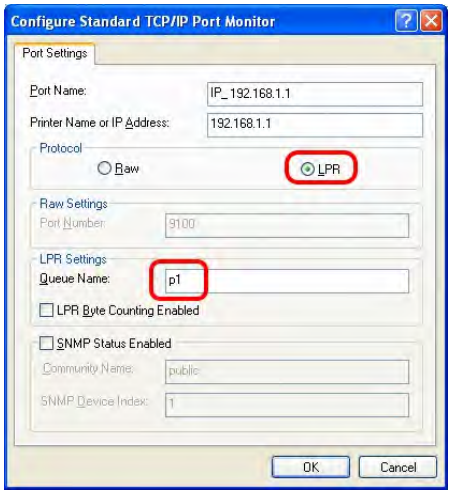
9. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



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

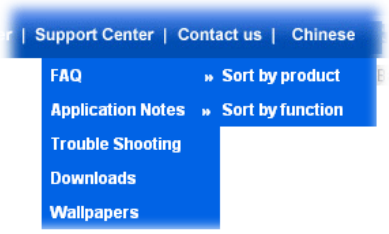


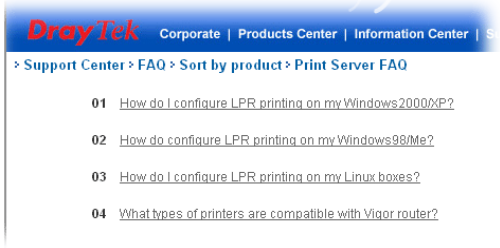
11. Select "**LPR**" on Protocol, type **p1** (number 1) as Queue Name. Then click **OK**. Next please refer to the red rectangle for choosing the correct protocol and UPR name.



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

Note 1: Some printers with the fax/scanning or other additional functions are not supported. If you do not know whether your printer is supported or not, please visit www.draytek.com to find out the printer list. Open **Support Center->FAQ->Sort by product**; select the model of the router and click on it; find out the link of **Printer Server FAQ**; 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.

This page is left blank.

2 Configuring Basic Settings

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

This chapter explains how to setup a password for an administrator and how to adjust basic settings for accessing Internet successfully. Be aware that only the administrator can change the router configuration.

2.1 Changing Password

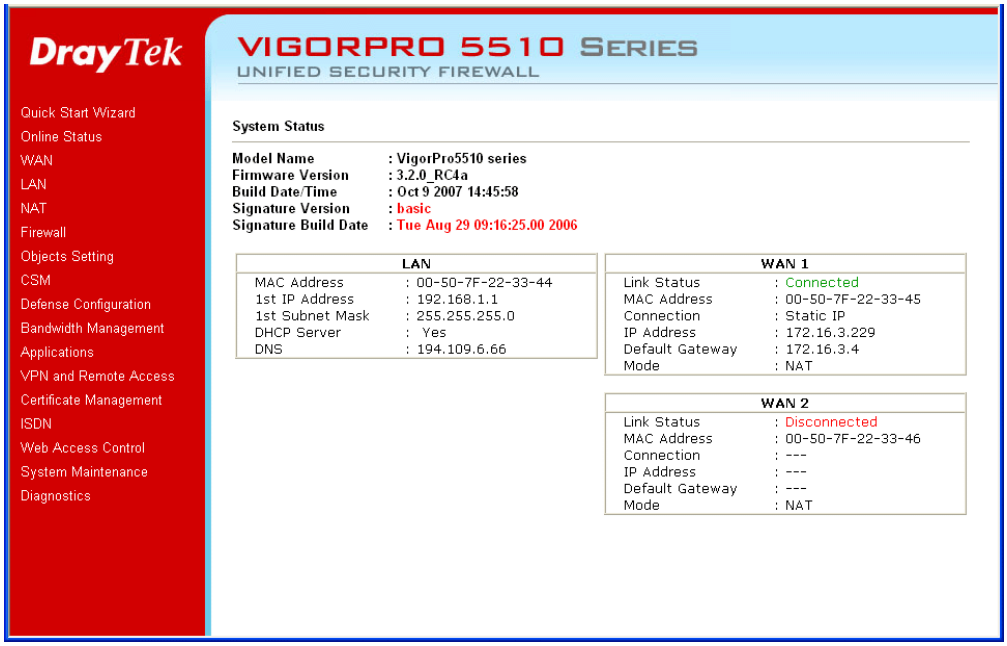
To change the password for this device, you have to access into the web browse with default password first.

1. Make sure your computer 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 this guide.

2. 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. Please type default values (both username and password are Null) on the window for the first time accessing and click **OK** for next screen.

3. Now, the **Main Screen** will pop up.

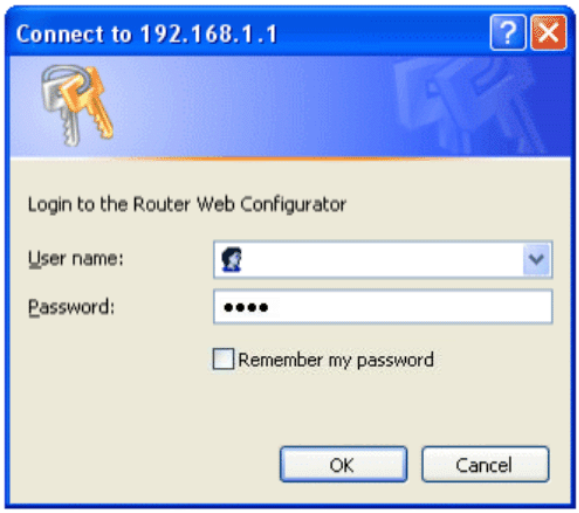


Note: The home page will change slightly in accordance with the router you have.

4. Go to **System Maintenance** page and choose **Administrator Password**.

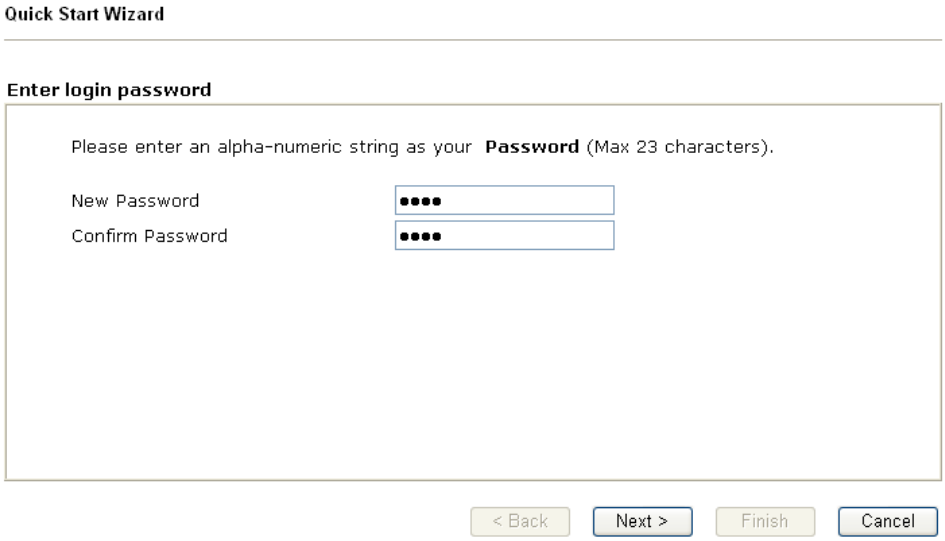
5. Enter the login password (the default is blank) on the field of **Old Password**. Type a new one in the field of **New Password** and retype it on the field of **Retype New Password**. Then click **OK** to continue.

6. Now, the password has been changed. Next time, use the new password to access the Web Configurator for this router.

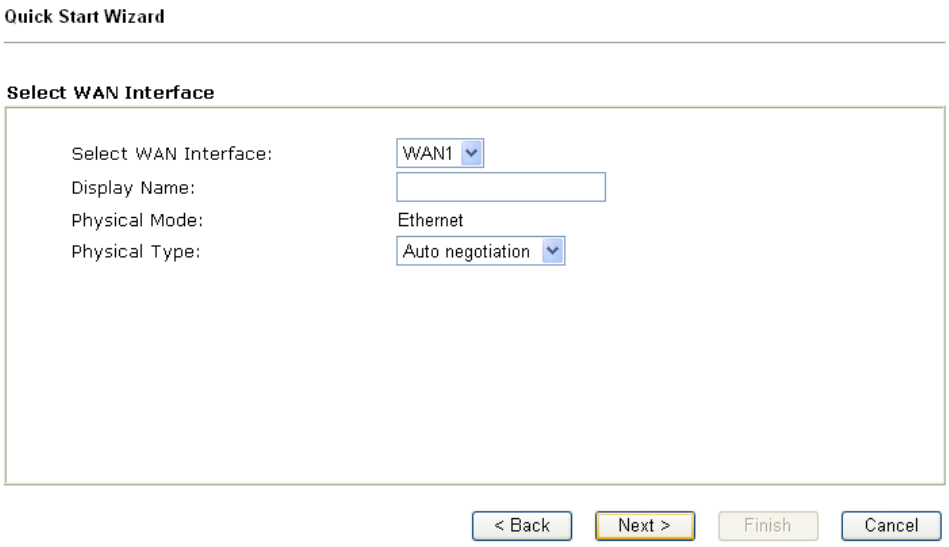


2.2 Quick Start Wizard

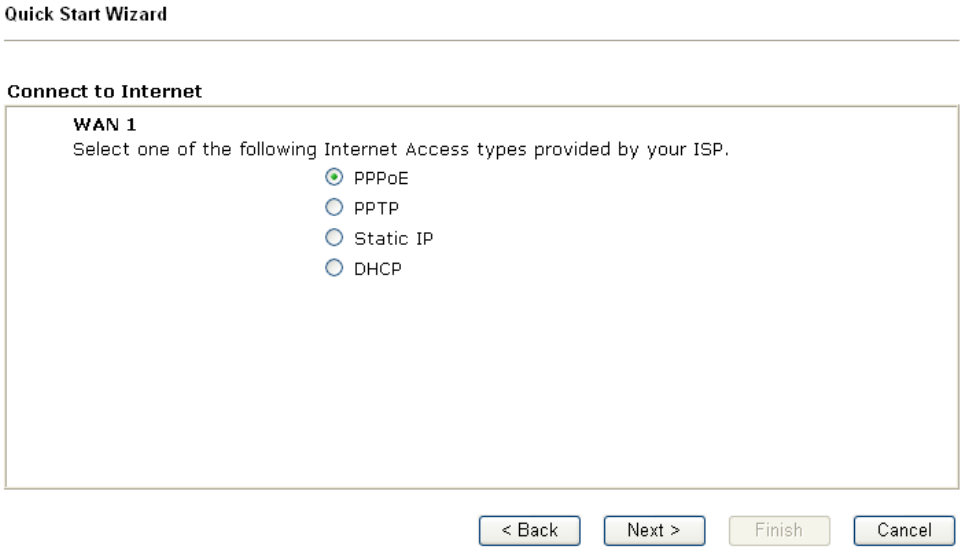
If your router can be under an environment with high speed NAT, the configuration provide here can help you to deploy and use the router quickly. The first screen of **Quick Start Wizard** is entering login password. After typing the password, please click **Next**.



On the next page as shown below, please select the WAN interface that you use. Choose **Auto negotiation** as the physical type for your router. Then click **Next** for next step.



On the next page as shown below, please select the appropriate Internet access type according to the information from your ISP. For example, you should select PPPoE mode if the ISP provides you PPPoE interface. Then click **Next** for next step.



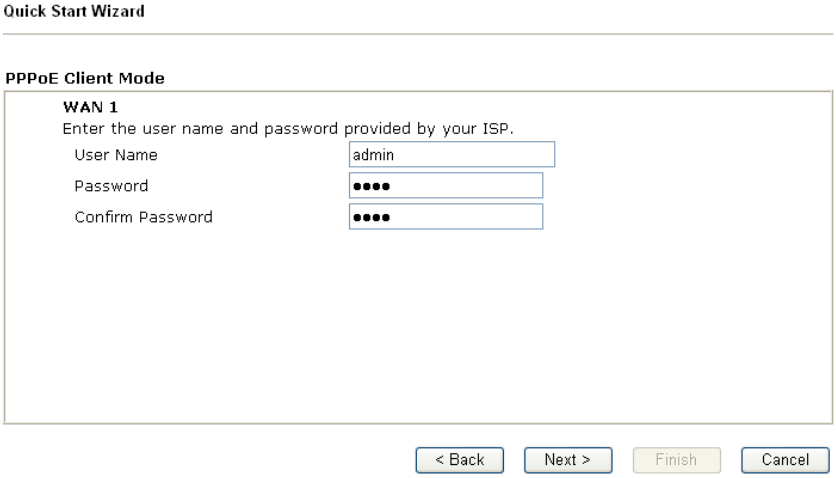
In the **Quick Start Wizard**, you can configure the router to access the Internet with different protocol/modes such as **PPPoE**, **PPTP**, **Static IP** or **DHCP**. The router supports the DSL WAN interface for Internet access.

2.2.1 PPPoE

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

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

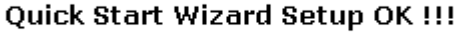
If your ISP provides you the **PPPoE** connection, please select **PPPoE** for this router. The following page will be shown.



User Name	Assign a specific valid user name provided by the ISP.
Password	Assign a valid password provided by the ISP.
Confirm Password	Retype the password for confirmation.

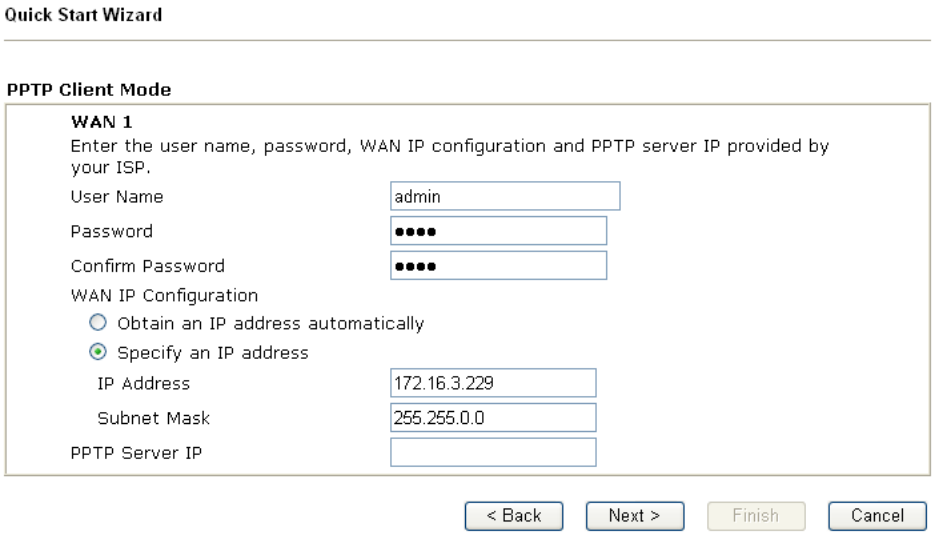
Click **Next** for viewing summary of such connection.

Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



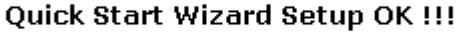
2.2.2 PPTP

Click **PPTP** as the protocol. Type in all the information that your ISP provides for this protocol.



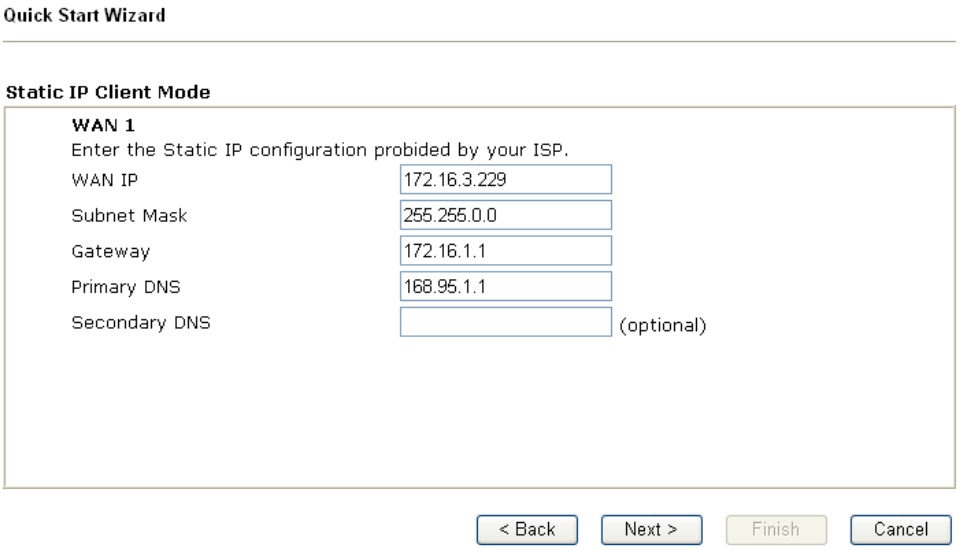
Click **Next** for viewing summary of such connection.

Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

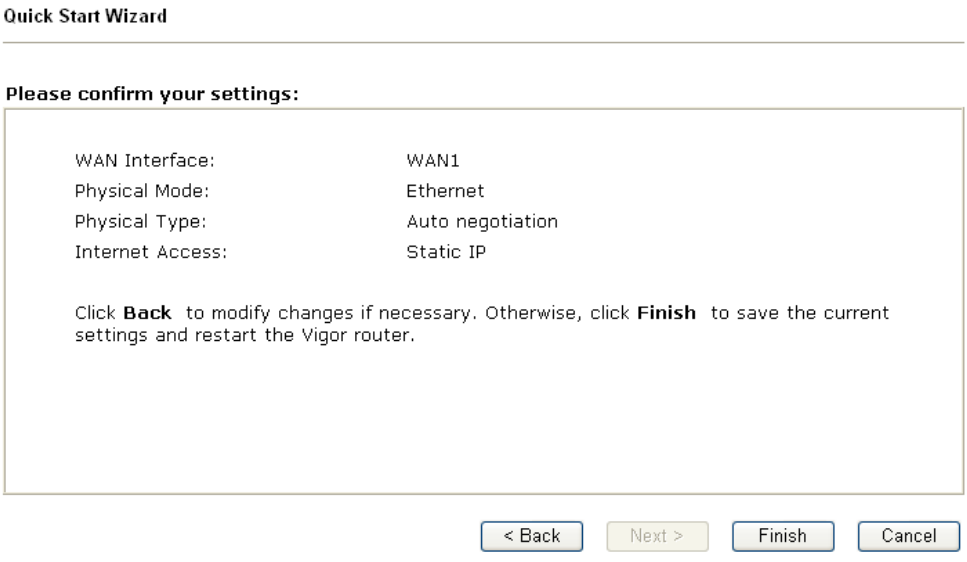


2.2.3 Static IP

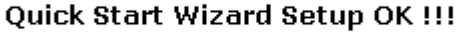
Click **Static IP** as the protocol. Type in all the information that your ISP provides for this protocol.



After finishing the settings in this page, click **Next** to see the following page.

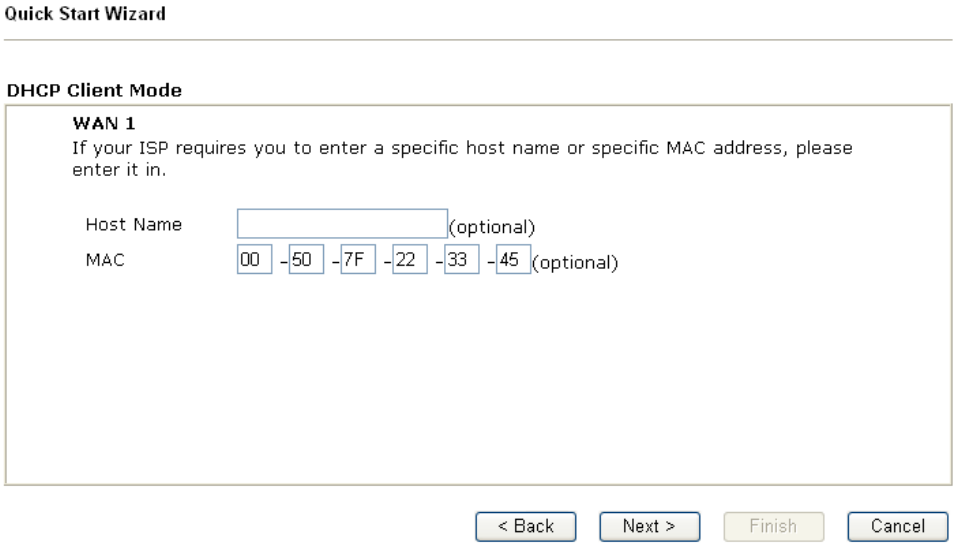


Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



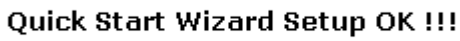
2.2.4 DHCP

Click **DHCP** as the protocol. Type in all the information that your ISP provides for this protocol.



After finishing the settings in this page, click **Next** to see the following page.

Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



2.3 Online Status

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

Online status for PPPoE (WAN2)

System Status **System Uptime: 0:0:18**

LAN Status **Primary DNS:** 168.95.192.1 **Secondary DNS:** 168.95.1.1

IP Address	TX Packets	RX Packets
192.168.1.1	77	56

WAN 1 Status

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		Static IP	0:00:11	
IP	**GW IP**	**TX Packets**	**TX Rate**	**RX Packets**	**RX Rate**
192.168.5.100	192.168.5.1	3	17	3	42

WAN 2 Status >> Drop PPPoE

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:00:11	
IP	**GW IP**	**TX Packets**	**TX Rate**	**RX Packets**	**RX Rate**
61.230.209.207	61.230.192.254	10	16	10	12

Online status for PPTP (for WAN2)

System Status **System Uptime: 0:0:18**

LAN Status **Primary DNS:** 168.95.192.1 **Secondary DNS:** 168.95.1.1

IP Address	TX Packets	RX Packets
192.168.1.1	77	56

WAN 1 Status

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		Static IP	0:00:11	
IP	**GW IP**	**TX Packets**	**TX Rate**	**RX Packets**	**RX Rate**
192.168.5.100	192.168.5.1	3	17	3	42

WAN 2 Status >> Drop PPPoE

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet	WAN2	PPTP	0:00:15	
IP	**GW IP**	**TX Packets**	**TX Rate**	**RX Packets**	**RX Rate**
192.168.29.202	192.168.29.1	103	119	14	6

Online status for Static IP (for WAN1)

System Status **System Uptime: 0:0:18**

LAN Status **Primary DNS:** 168.95.192.1 **Secondary DNS:** 168.95.1.1

IP Address	TX Packets	RX Packets
192.168.1.1	77	56

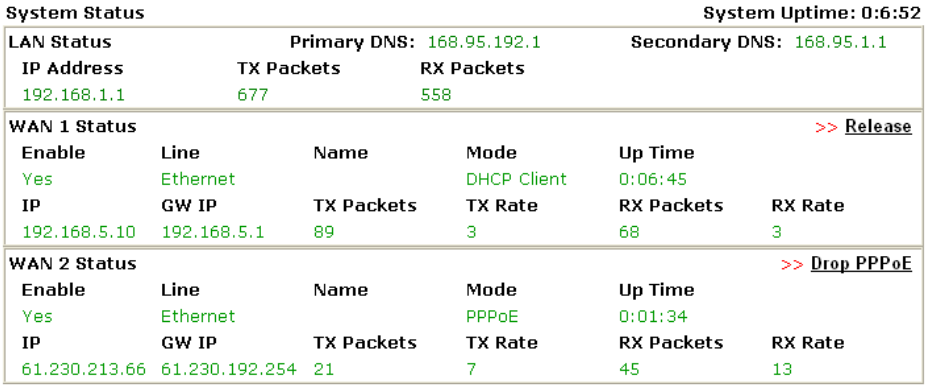
WAN 1 Status

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		Static IP	0:00:11	
IP	**GW IP**	**TX Packets**	**TX Rate**	**RX Packets**	**RX Rate**
192.168.5.100	192.168.5.1	3	17	3	42

WAN 2 Status >> Drop PPPoE

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:00:11	
IP	**GW IP**	**TX Packets**	**TX Rate**	**RX Packets**	**RX Rate**
61.230.209.207	61.230.192.254	10	16	10	12

Online status for DHCP



Detailed explanation is shown below:

Primary DNS	Displays the IP address of the primary DNS.
Secondary DNS	Displays the IP address of the secondary DNS.
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.
WAN1/2 Status	
Line	Displays the physical connection (Ethernet) of this interface.
Name	Displays the name set in WAN1/WAN web page.
Mode	Displays the type of WAN connection (e.g., PPPoE).
Up Time	Displays the total uptime of the interface.
IP	Displays the IP address of the WAN interface.
GW IP	Displays the IP address of the default gateway.
TX Packets	Displays the total transmitted packets at the WAN interface.
TX Rate	Displays the speed of transmitted octets at the WAN interface.
RX Packets	Displays the total number of received packets at the WAN interface.
RX Rate	Displays the speed of received octets at the WAN interface.

Note: The words in green mean that the WAN connection of that interface (WAN1/WAN2) is ready for accessing Internet; the words in red mean that the WAN connection of that interface (WAN1/WAN2) is not ready for accessing Internet.

2.4 Saving Configuration

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

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

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

This page is left blank.

3 Advanced Web Configuration

After finished basic configuration of the router, you can access Internet with ease. For the people who want to adjust more setting for suiting his/her request, please refer to this chapter for getting detailed information about the advanced configuration of this router. As for other examples of application, please refer to chapter 4.

3.1 WAN

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

3.1.1 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

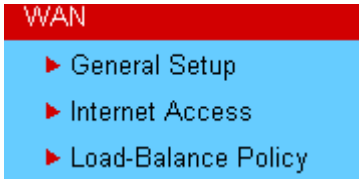
As the router plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor router. The router itself will also use the default **private IP** address: 192.168.1.1 to communicate with the 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.

Below shows the menu items for WAN.



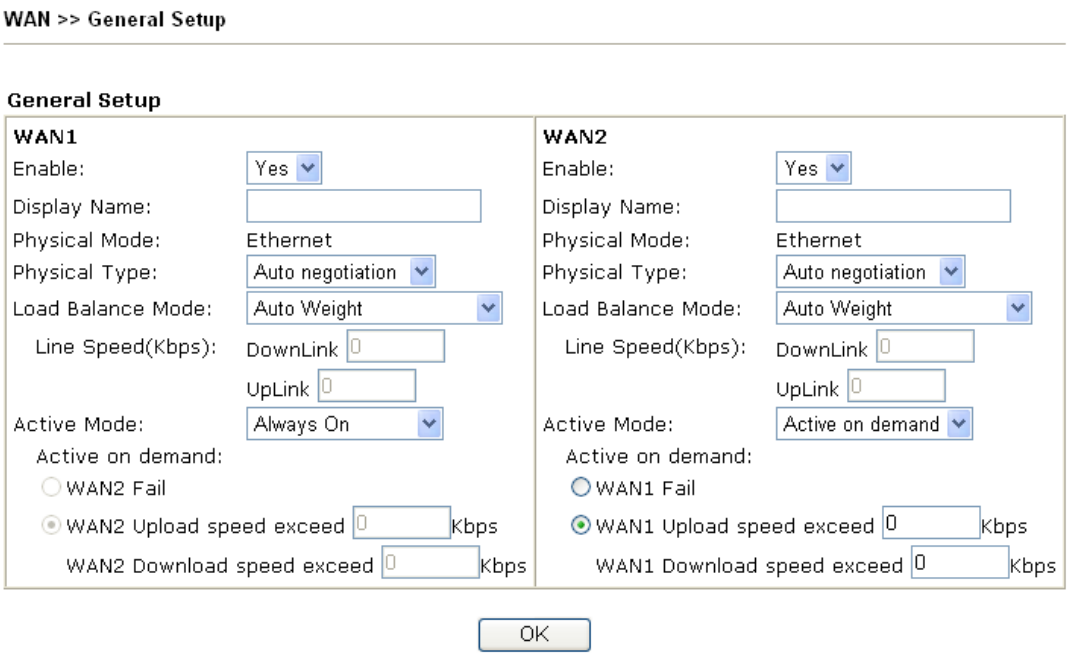
3.1.2 General Setup

This section will introduce some general settings of Internet and explain the connection modes for WAN1 and WAN2 in details.

This router supports dual WAN function. It allows users to access Internet and combine the bandwidth of the dual WAN to speed up the transmission through the network. Each WAN port can connect to different ISPs, Even if the ISPs use different technology to provide telecommunication service (such as DSL, Cable modem, etc.). If any connection problem occurred on one of the ISP connections, all the traffic will be guided and switched to the normal communication port for proper operation. Please configure WAN1 and WAN2 settings.

This webpage allows you to set general setup for WAN1 and WAN respectively.

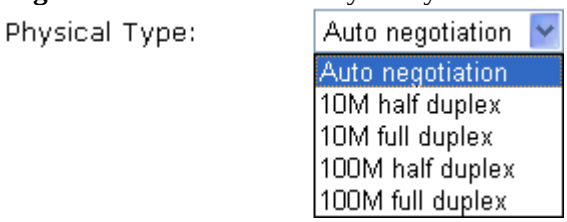
Note: In default, WAN1 and WAN2 are enabled.



Enable	Choose **Yes** to invoke the settings for this WAN interface. Choose **No** to disable the settings for this WAN interface.
Display Name	Type the description for the WAN1/WAN2 interface.
Physical Mode	For WAN1, the physical connection is done through ADSL port; yet the physical connection for WAN2 is done through an Ethernet port (P1). You cannot change it.

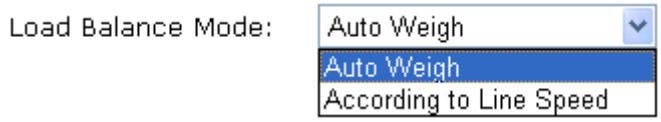
Physical Type

You can change the physical type for WAN2 or choose **Auto negotiation** for determined by the system.



Load Balance Mode

If you know the practical bandwidth for your WAN interface, please choose the setting of **According to Line Speed**. Otherwise, please choose **Auto Weigh** to let the router reach the best load balance.

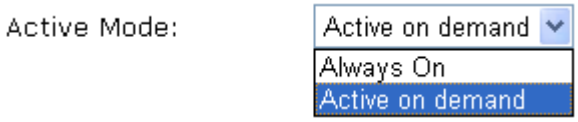


Line Speed

If your choose **According to Line Speed** as the **Load Balance Mode**, please type the line speed for downloading and uploading through WAN1/WAN2. The unit is kbps.

Active Mode

Choose **Always On** to make the WAN connection (WAN1/WAN2) being activated always; or choose **Active on demand** to make the WAN connection (WAN1/WAN2) activated if it is necessary.



If you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the Details Page of WAN>>Internet Access. In addition, there are three selections for you to choose for different purposes.

WAN2 Fail – It means the connection for WAN1 will be activated when WAN2 is failed.

WAN2 Upload speed exceed XX kbps – It means the connection for WAN1 will be activated when WAN2 Upload speed exceed certain value that you set in this box for 15 seconds.

WAN2 Download speed exceed XX kbps– It means the connection for WAN1 will be activated when WAN2 Download speed exceed certain value that you set in this box for 15 seconds.

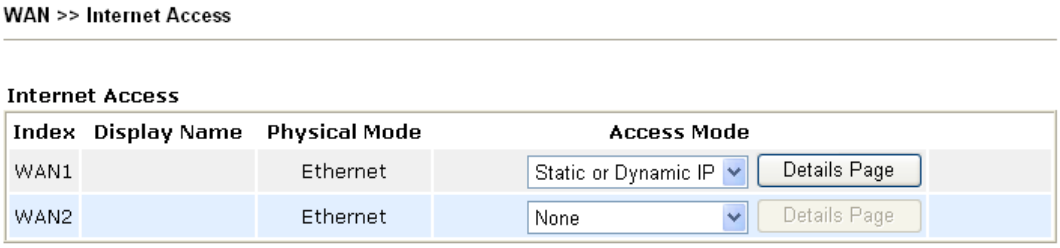
WAN1 Fail – It means the connection for WAN2 will be activated when WAN1 is failed.

WAN1 Upload speed exceed XX kbps – It means the connection for WAN2 will be activated when WAN1 Upload speed exceed certain value that you set in this box for 15 seconds.

WAN1 Download speed exceed XX kbps– It means the connection for WAN2 will be activated when WAN1 Download speed exceed certain value that you set in this box for 15 seconds.

3.1.3 Internet Access

For the router supports dual WAN function, the users can set different WAN settings (for WAN1/WAN2) for Internet Access. Due to different physical mode for WAN1 and WAN2, the Access Mode for these two connections also varies slightly.

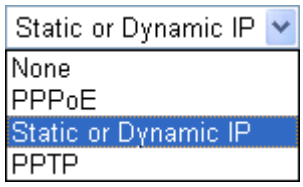


Index — It shows the WAN modes that this router supports. WAN1 is the default WAN interface for accessing into the Internet. WAN2 is the optional WAN interface for accessing into the Internet when WAN 1 is inactive for some reason.

Display Name — It shows the name of the WAN1/WAN2 that entered in general setup.

Physical Mode — It shows the physical port for WAN1/WAN2.

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.

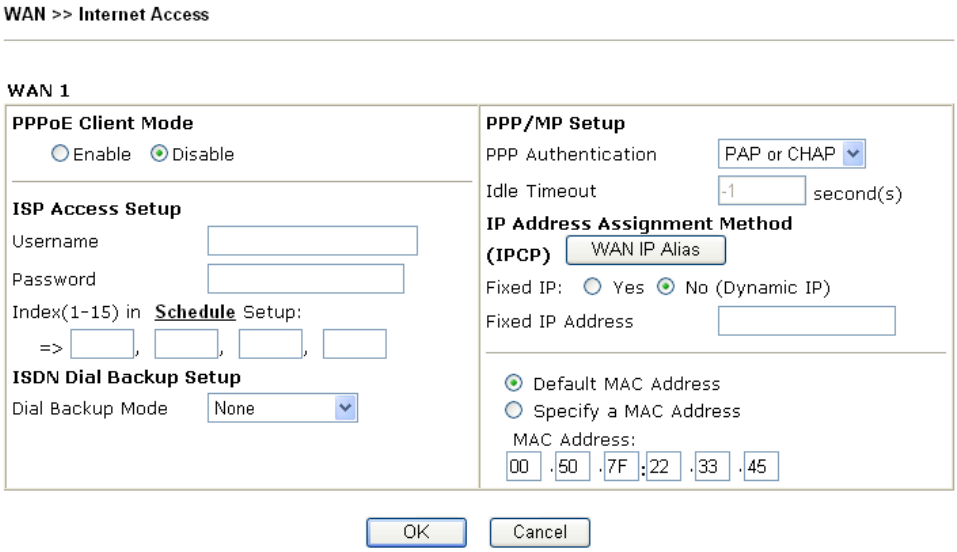


There are three access modes provided for PPPoE, Static or Dynamic IP and PPTP.

Details Page — This button will open different web page according to the access mode that you choose in WAN1 or WAN2.

Details Page for PPPoE

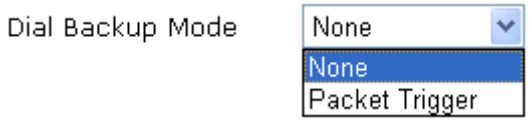
To use **PPPoE** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **PPPoE** mode for WAN2. The following web page will be shown.



PPPoE Client Mode — Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.

ISP Access Setup — Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check **Always On**.
Username – Type in the username provided by ISP in this field.
Password – Type in the password provided by ISP in this field.
Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application – Schedule** web page and you can use the number that you have set in that web page.

ISDN Dial Backup Setup — This setting is available for the routers supporting ISDN function only. Before utilizing the ISDN dial backup feature, you must create a dial backup profile first. Please click **Internet Access Setup** > **Dialing to a Single ISP** to enter the backup profile.



This setting is available for *i* model only.

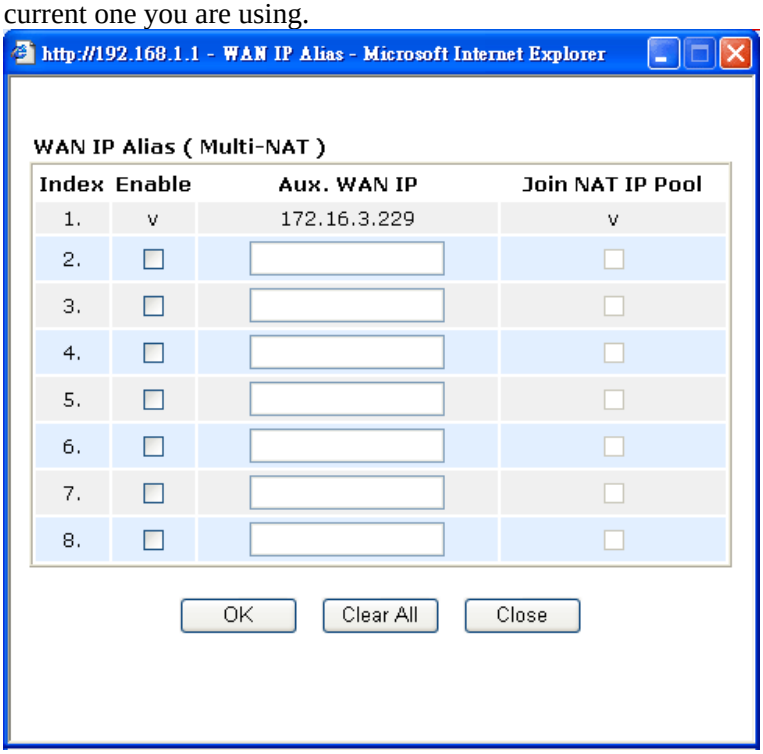
PPP/MP Setup — **PPP Authentication** – Select **PAP only** or **PAP or CHAP** for PPP.
Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action. This setting is active only when the **Active on demand** option for Active Mode is selected in **WAN>> General Setup** page.

IP Address Assignment Method — Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request.

(IPCP)

In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.

WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.



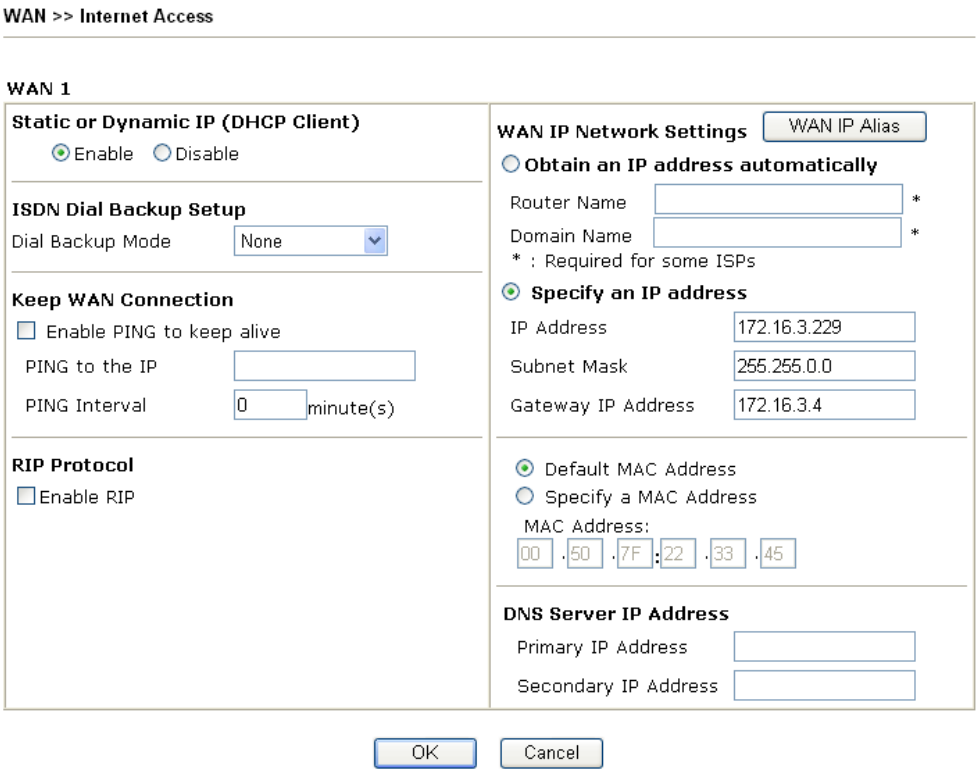
Fixed IP – Click **Yes** to use this function and type in a fixed IP address in the box of **Fixed IP Address**.
Default MAC Address – You can use **Default MAC Address** or specify another MAC address by typing on the boxes of MAC Address for the router.
Specify a MAC Address – Type the MAC address for the router manually.

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

Details Page for Static or Dynamic IP

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

To use **Static or Dynamic IP** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **Static or Dynamic IP** mode for WAN2. The following web page will be shown.

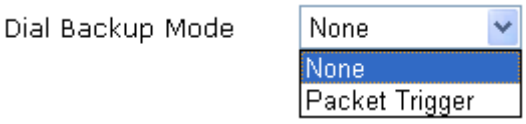


Static or Dynamic IP (DHCP Client)

Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.

ISDN Dial Backup Setup

This setting is available for the routers supporting ISDN function only. Before utilizing the ISDN dial backup feature, you must create a dial backup profile first. Please click **Internet Access Setup** > **Dialing to a Single ISP** to enter the backup profile.



This setting is available for *i* model only.

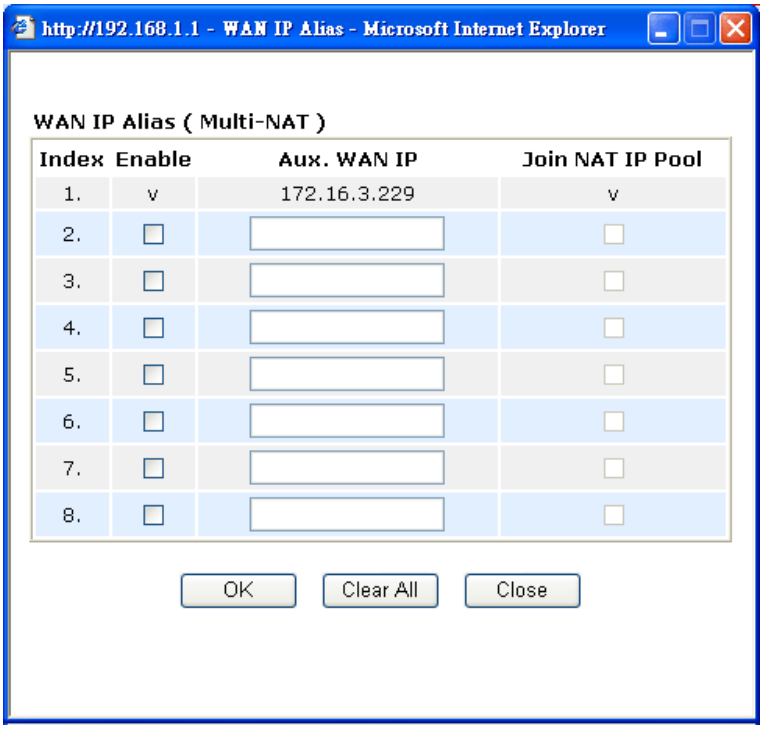
RIP Protocol

Routing Information Protocol is abbreviated as RIP(RFC1058）specifying how routers exchange routing tables information. Click **Enable RIP** for activating this function.

WAN IP Network Settings

This group allows you to obtain an IP address automatically and allows you type in IP address manually.

WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only.



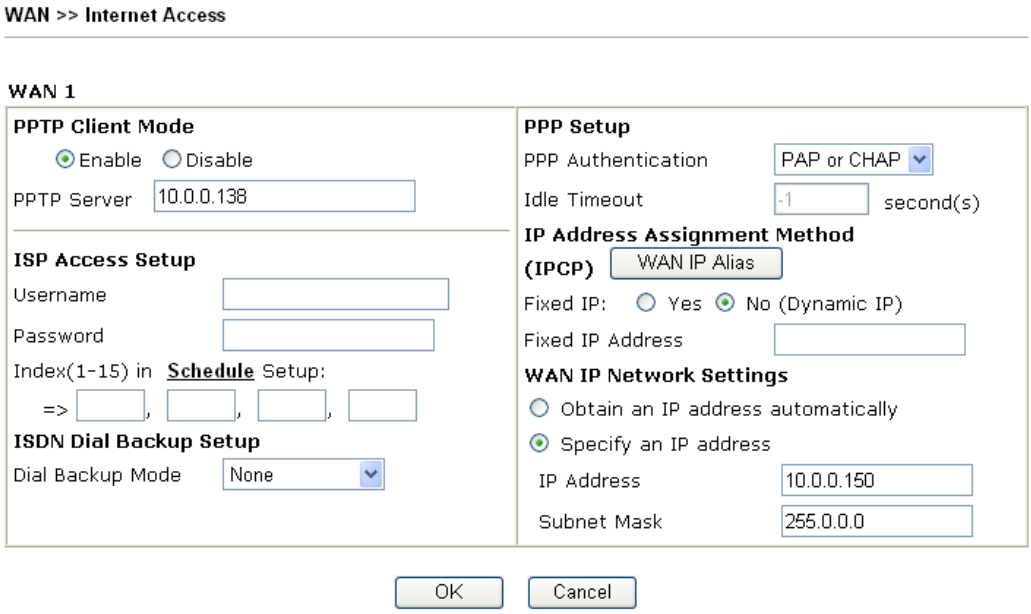
Obtain an IP address automatically – Click this button to obtain the IP address automatically if you want to use **Dynamic IP** mode.
Router Name: Type in the router name provided by ISP.
Domain Name: Type in the domain name that you have assigned.
Specify an IP address – Click this radio button to specify 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.
Default MAC Address: Click this radio button to use default MAC address for the router.
Specify a MAC Address: Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the **Specify a MAC Address** and enter the MAC address in the MAC Address field.

DNS Server IP Address

Type in the primary IP address for the router if you want to use **Static IP** mode. If necessary, type in secondary IP address for necessity in the future.

Details Page for PPTP

To use **PPTP** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **PPTP** mode for WAN2. The following web page will be shown.



PPTP Setup

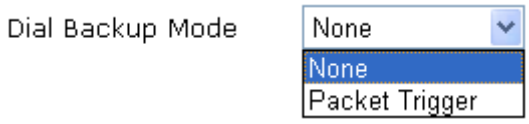
PPTP Link - Click **Enable** to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface.
PPTP Server - Specify the IP address of the PPTP server.

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.
Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application – Schedule** web page and you can use the number that you have set in that web page.

ISDN Dial Backup Setup

This setting is available for the routers supporting ISDN function only. Before utilizing the ISDN dial backup feature, you must create a dial backup profile first. Please click **Internet Access Setup** > **Dialing to a Single ISP** to enter the backup profile.



This setting is available for *i* model only.

PPP Setup

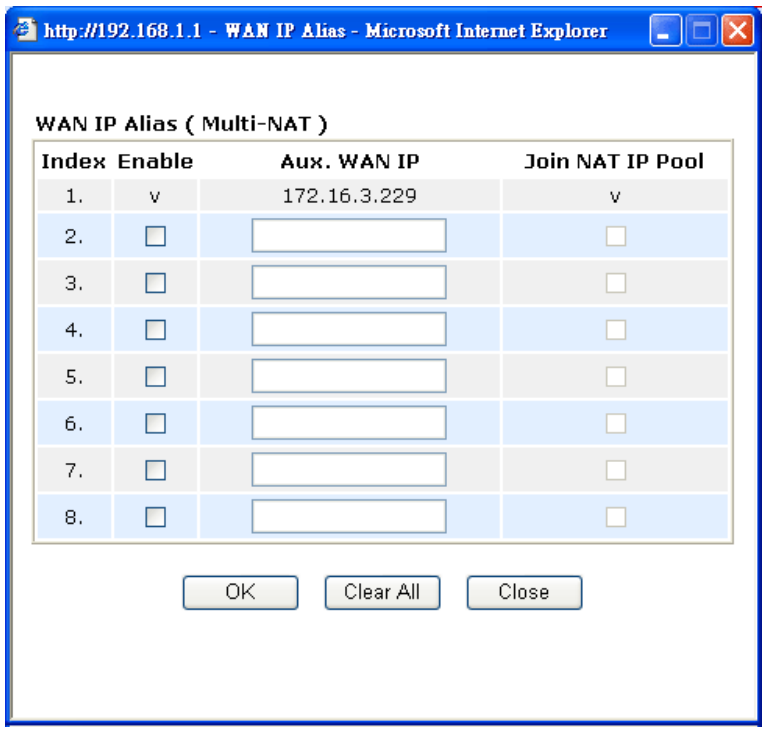
PPP Authentication - Select **PAP only** or **PAP or CHAP** for PPP.
Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action. This setting is active only when the **Active on demand** option for Active Mode is selected in **WAN>> General Setup** page.

IP Address Assignment Method(IPCP)

Fixed IP - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click **Yes** to use this function and type in a fixed IP address in the

box.

Fixed IP Address -Type a fixed IP address.
WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only.



Default MAC Address – Click this radio button to use default MAC address for the router.
Specify a MAC Address - Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the **Specify a MAC Address** and enter the MAC address in the MAC Address field.

WAN IP Network Settings

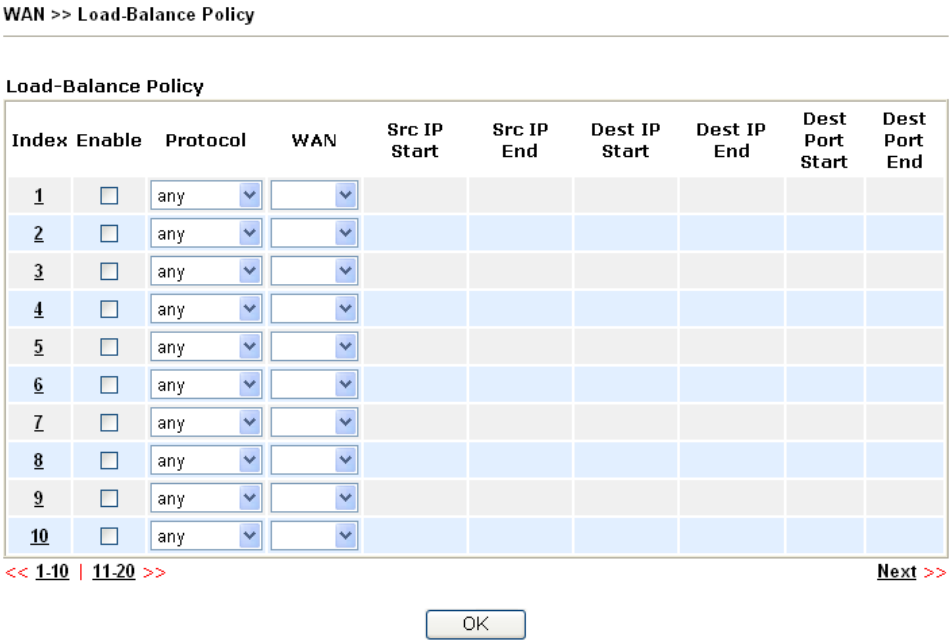
Obtain an IP address automatically – Click this button to obtain the IP address automatically.

Specify an IP address – Click this radio button to specify some data.
IP Address – Type the IP address.
Subnet Mask – Type the subnet mask.

3.1.4 Load-Balance Policy

This router supports the function of load balancing. It can assign traffic with protocol type, IP address for specific host, a subnet of hosts, and port range to be allocated in WAN1 or WAN2 interface. The user can assign traffic category and force it to go to dedicate network interface based on the following web page setup. Twenty policies of load-balance are supported by this router.

Note: Load-Balance Policy is running only when both WAN1 and WAN2 are activated.

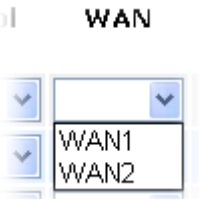


Index Click the number of index to access into the load-balance policy configuration web page.

Enable Check this box to enable this policy.

Protocol Use the drop-down menu to change the protocol for the WAN interface.

WAN Use the drop-down menu to change the WAN interface.



Src IP Start Displays the IP address for the start of the source IP.

Src IP End Displays the IP address for the end of the source IP.

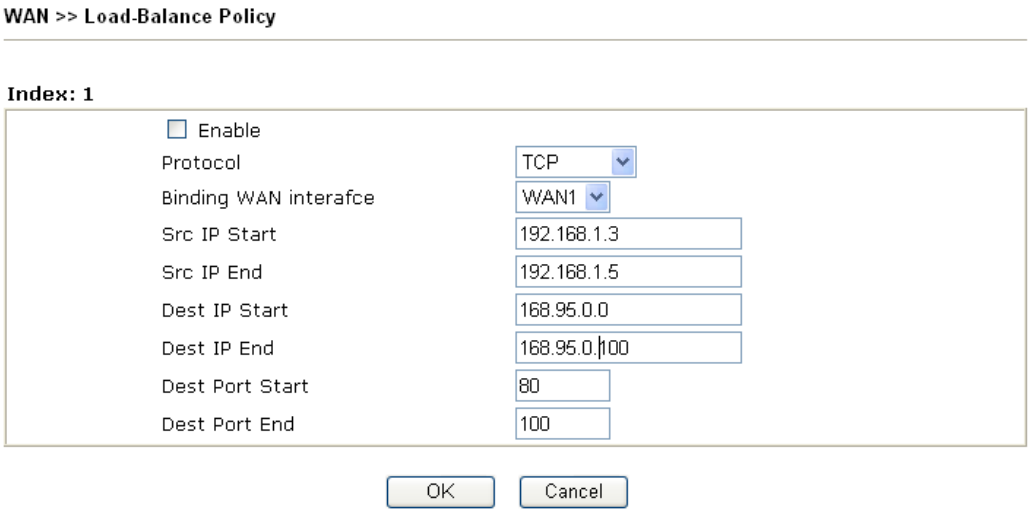
Dest IP Start Displays the IP address for the start of the destination IP.

Dest IP End Displays the IP address for the end of the destination IP.

Dest Port Start Displays the IP address for the start of the destination port.

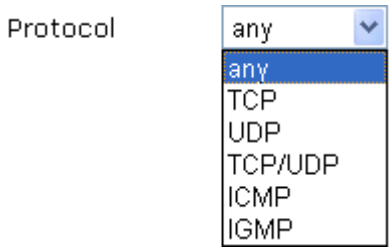
Dest Port End Displays the IP address for the end of the destination port.

Click **Index 1** to access into the following page for configuring load-balance policy.



Enable Check this box to enable this policy.

Protocol Use the drop-down menu to choose a proper protocol for the WAN interface.



Binding WAN interface Choose the WAN interface (WAN1 or WAN2) for binding.

Src IP Start Type the source IP start for the specified WAN interface.

Src IP End Type the source IP end for the specified WAN interface. If this field is blank, it means that all the source IPs inside the LAN will be passed through the WAN interface.

Dest IP Start Type the destination IP start for the specified WAN interface.

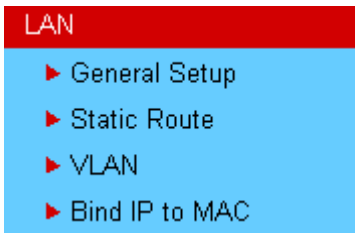
Dest IP End Type the destination IP end for the specified WAN interface. If this field is blank, it means that all the destination IPs will be passed through the WAN interface.

Dest Port Start Type the destination port start for the destination IP.

Dest Port End Type the destination port end for the destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.

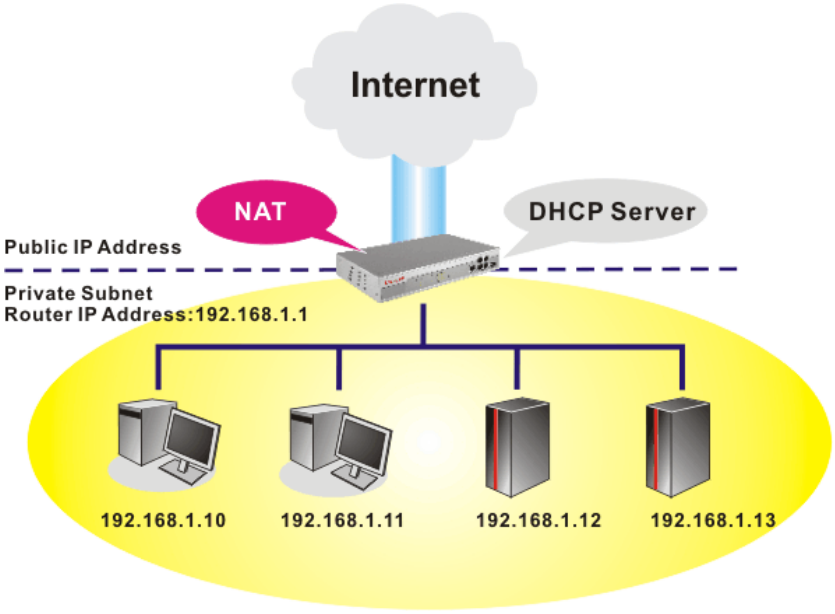
3.2 LAN

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.

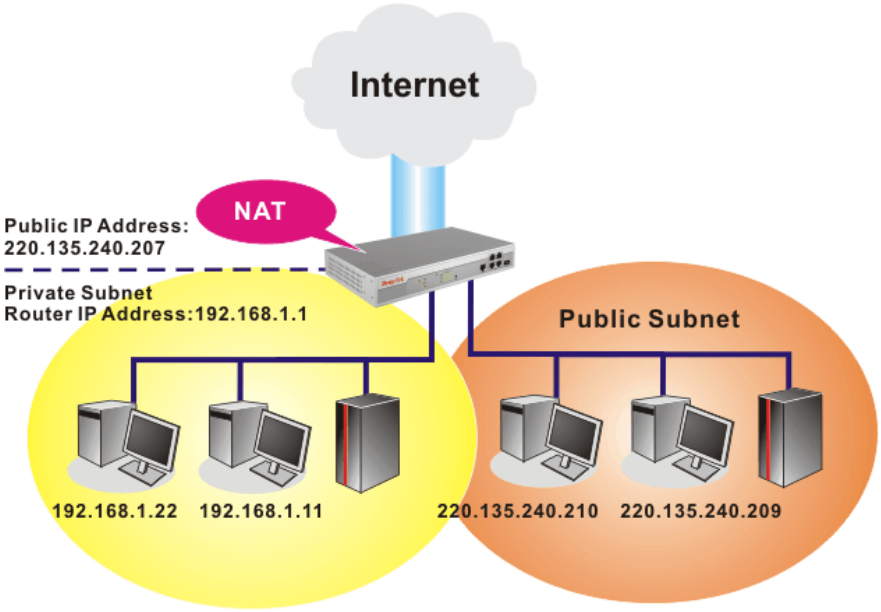


3.2.1 Basics of LAN

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)

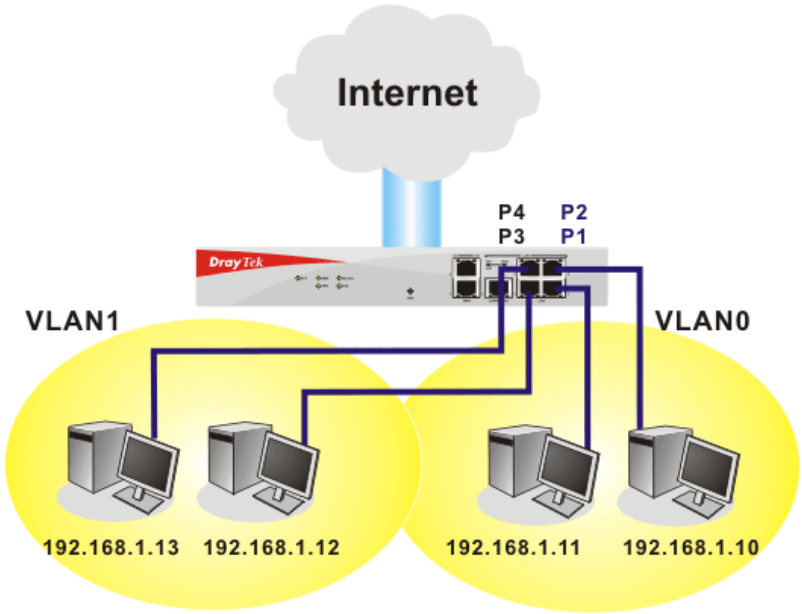
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

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.

What are Virtual LANs and Rate Control

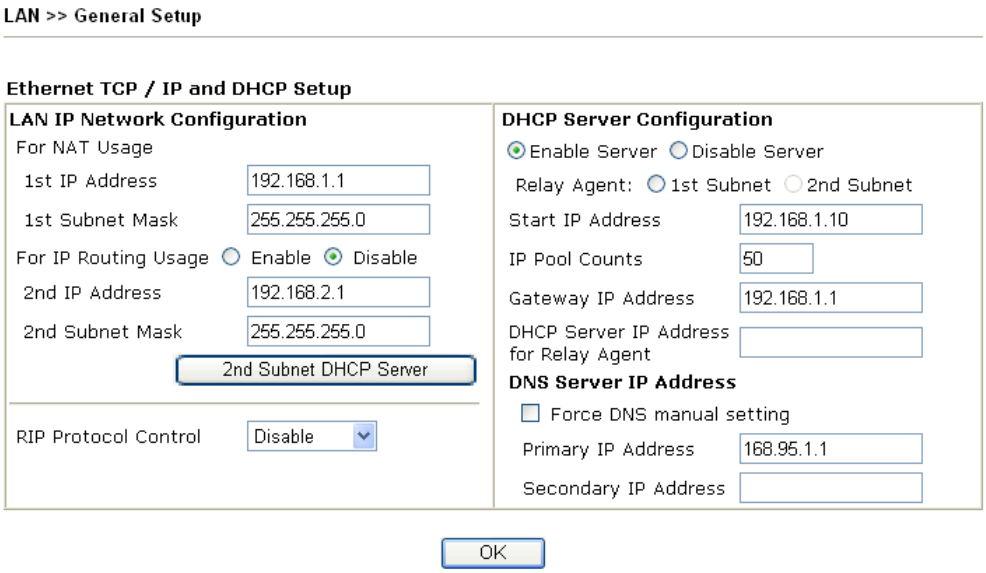
You can group local hosts by physical ports and create up to 4 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.



3.2.2 General Setup

This page provides you the general settings for LAN.

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



1st IP Address — Type in private IP address for connecting to a local private network (Default: 192.168.1.1).

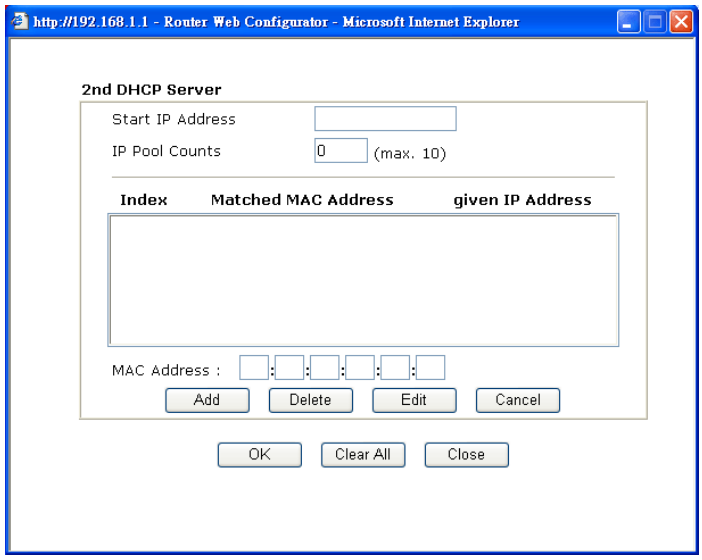
1st Subnet Mask — Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)

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/ 24)

2nd Subnet Mask — An address code that determines the size of the network. (Default: 255.255.255.0/ 24)

2nd DHCP Server — You can configure the router to serve as a DHCP server for the 2nd subnet.



Start IP Address: Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 2nd IP address of your router is 220.135.240.1, the starting IP address must be 220.135.240.2 or greater, but smaller than 220.135.240.254.

IP Pool Counts: Enter the number of IP addresses in the pool. The maximum is 10. For example, if you type 3 and the 2nd IP address of your router is 220.135.240.1, the range of IP address by the DHCP server will be from 220.135.240.2 to 220.135.240.11.

MAC Address: Enter the MAC Address of the host one by one and click **Add** to create a list of hosts to be assigned, deleted or edited IP address from above pool. Set a list of MAC Address for 2nd DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet.

RIP Protocol Control

Disable deactivates the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)

1st Subnet - Select the router to change the RIP information of the 1st subnet with neighboring routers.
2nd Subnet - Select the router to change the RIP information of the 2nd subnet with neighboring routers.

DHCP Server Configuration

DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.

If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
Enable Server - Let the router assign IP address to every host in the LAN.
Disable Server – Let you manually assign IP address to every host in the LAN.
Relay Agent – (1st subnet/2nd subnet) Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.
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.
IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.
Gateway IP Address - 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.

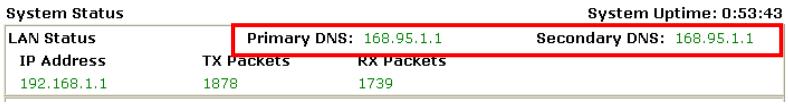
DHCP Server IP Address for Relay Agent - Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.

DNS Server Configuration

DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.

Force DNS manual setting - Force router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).
Primary IP 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 IP 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.

The default DNS Server IP address can be found via Online Status:



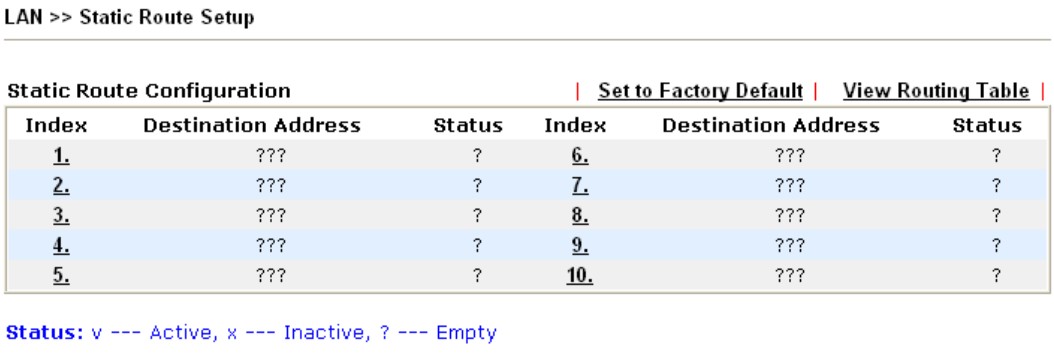
If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.

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.

There are two common scenarios of LAN settings that stated in Chapter 4. For the configuration examples, please refer to that chapter to get more information for your necessity.

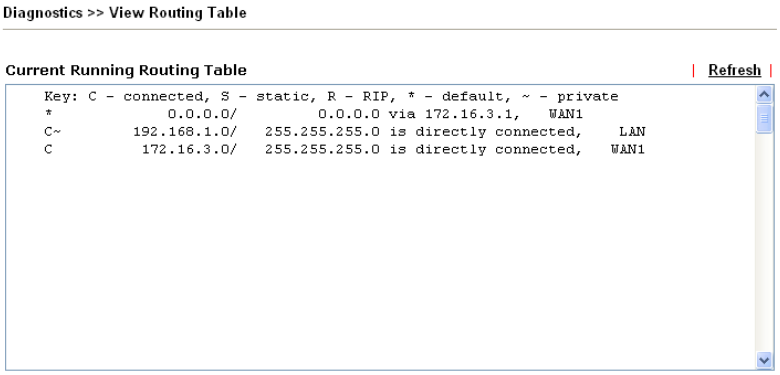
3.2.3 Static Route

Go to **LAN** to open setting page and choose **Static Route**.



Index The number (1 to 10) under Index allows you to open next page to set up static route.

Destination Address	Displays the destination address of the static route.
Status	Displays the status of the static route.
Viewing Routing Table	Displays the routing table for your reference.

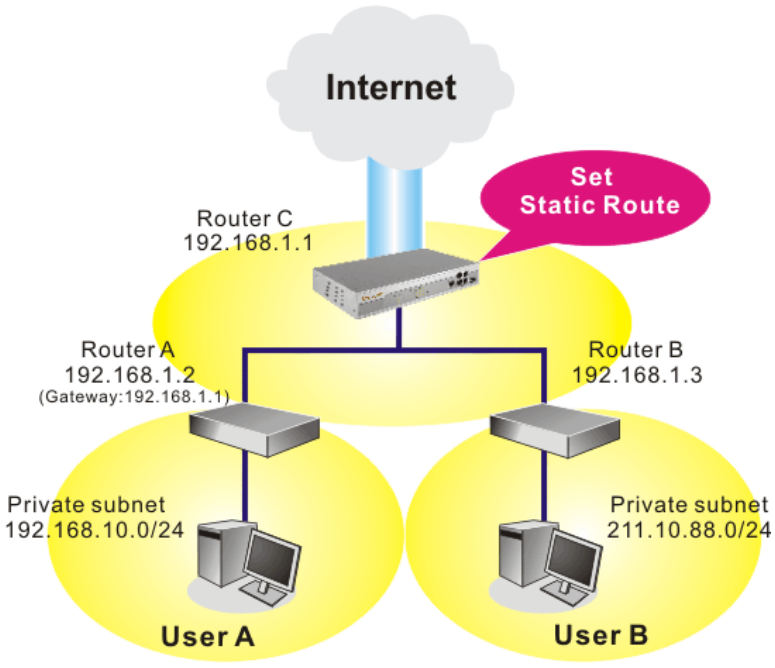


Add Static Routes to Private and Public Networks

Here is an example of setting Static Route in Main Router so that user A and B locating in different subnet can talk to each other via the router. Assuming the Internet access has been configured and the router works properly:

- use the Main Router to surf the Internet.
- create a private subnet 192.168.10.0 using an internal Router A (192.168.1.2)
- create a public subnet 211.100.88.0 via an internal Router B (192.168.1.3).
- have set Main Router 192.168.1.1 as the default gateway for the Router A 192.168.1.2.

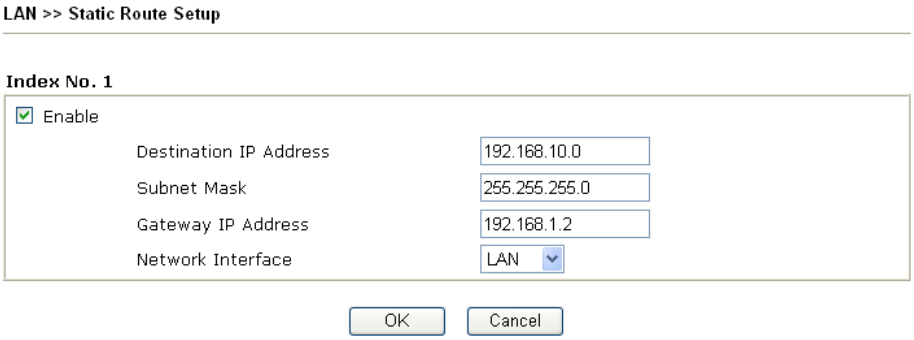
Before setting Static Route, user A cannot talk to user B for Router A can only forward recognized packets to its default gateway Main Router.



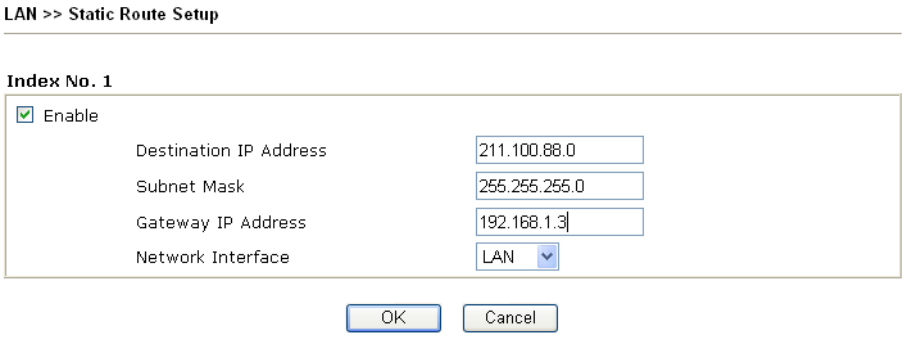
Go to **LAN** page and click **General Setup**, select 1st Subnet as the **RIP Protocol Control.** Then click the **OK** button.

Note: There are two reasons that we have to apply RIP Protocol Control on 1st Subnet. The first is that the LAN interface can exchange RIP packets with the neighboring routers via the 1st subnet (192.168.1.0/24). The second is that those hosts on the internal private subnets (ex. 192.168.10.0/24) can access the Internet via the router, and continuously exchange of IP routing information with different subnets.

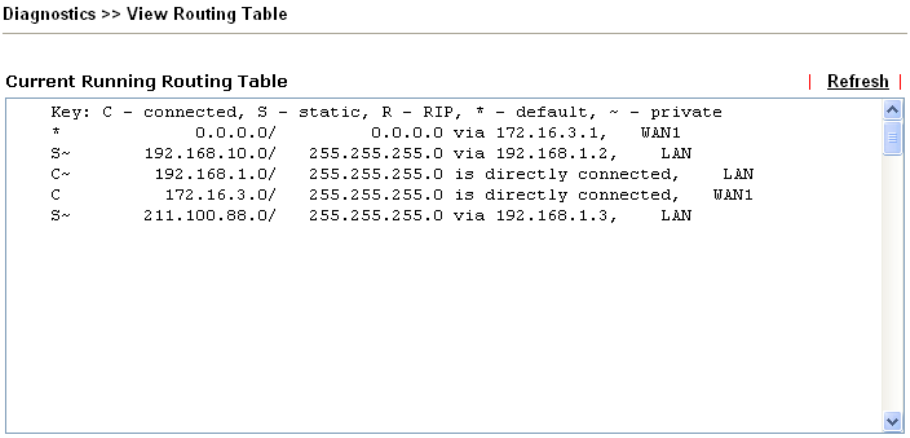
1. Click the **LAN - Static Route** and click on the **Index Number 1.** Check the **Enable** box. Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click **OK**.



2. Return to **Static Route Setup** page. Click on another **Index Number** to add another static route as show below, which regulates all packets destined to 211.100.88.0 will be forwarded to 192.168.1.3.

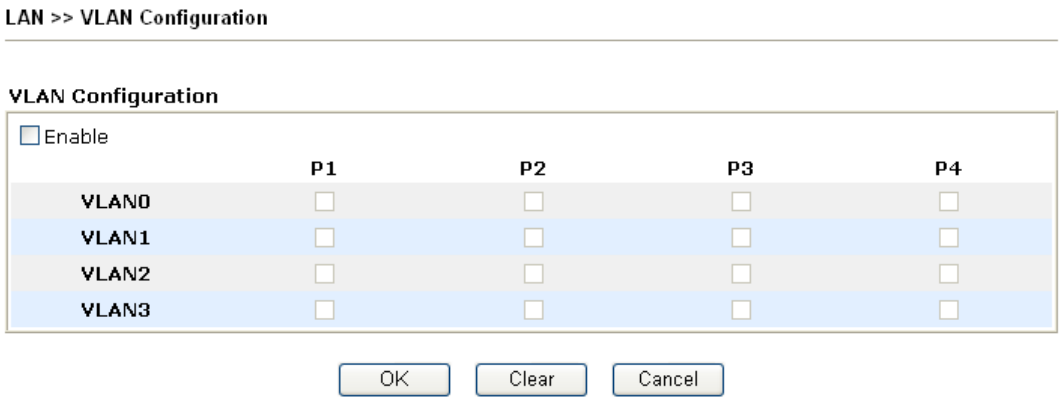


3. Go to **Diagnostics** and choose **Routing Table** to verify current routing table.



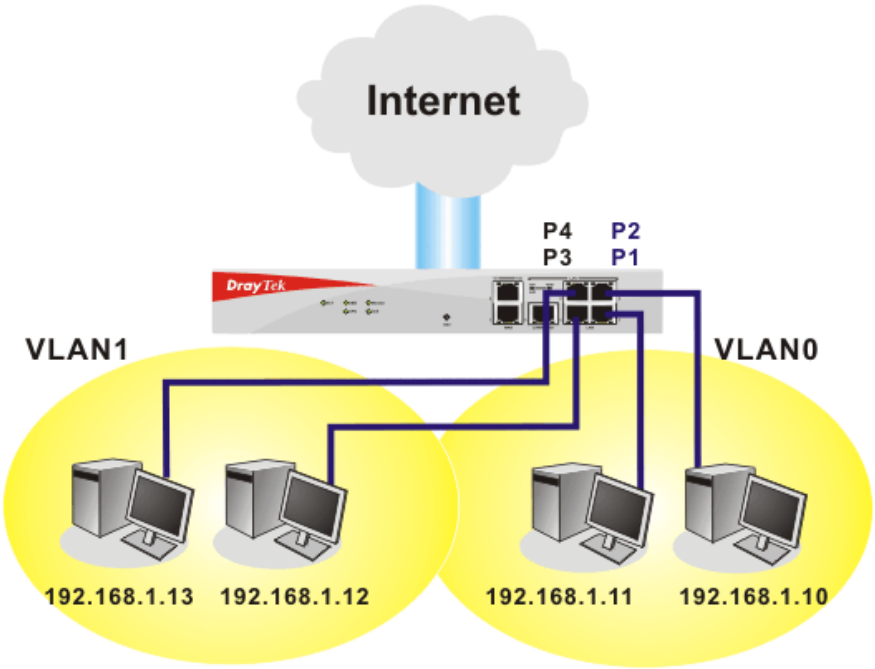
3.2.4 VLAN

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. You can also manage the in/out rate of each port. Go to **LAN** page and select **VLAN**. The following page will appear. Click **Enable** to invoke VLAN function.

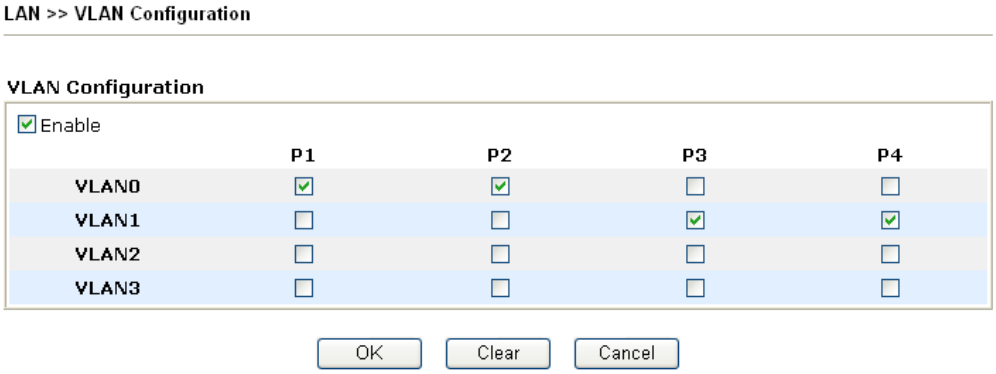


To add or remove a VLAN, please refer to the following example.

1. If, VLAN 0 is consisted of hosts linked to P1 and P2 and VLAN 1 is consisted of hosts linked to P3 and P4.



2. After checking the box to enable VLAN function, you will check the table according to the needs as shown below.

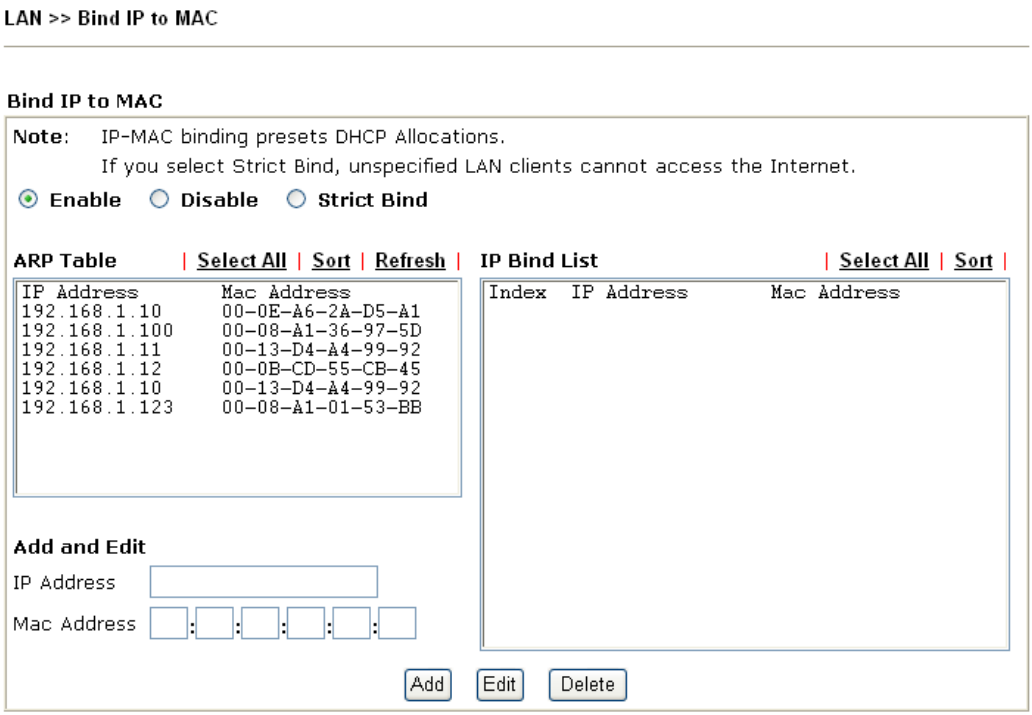


To remove VLAN, uncheck the needed box and click **OK** to save the results.

3.2.5 Bind IP to MAC

This function is used to bind the IP and MAC address in LAN to have a strengthen 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.



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.
Add and Edit	**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.
Refresh	It is used to refresh the ARP table. When there is one new PC added to the LAN, you can click this link to obtain the newly ARP table information.
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**.
Edit	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**.

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 configurator 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:

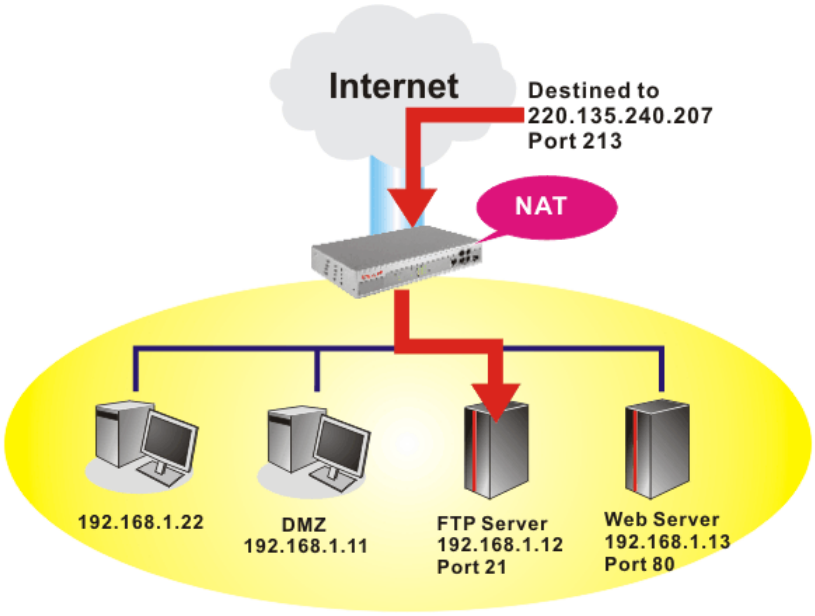
- **Save cost on applying public IP address and apply efficient usage of IP address.** NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- **Enhance security of the internal network 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.

Note: 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.

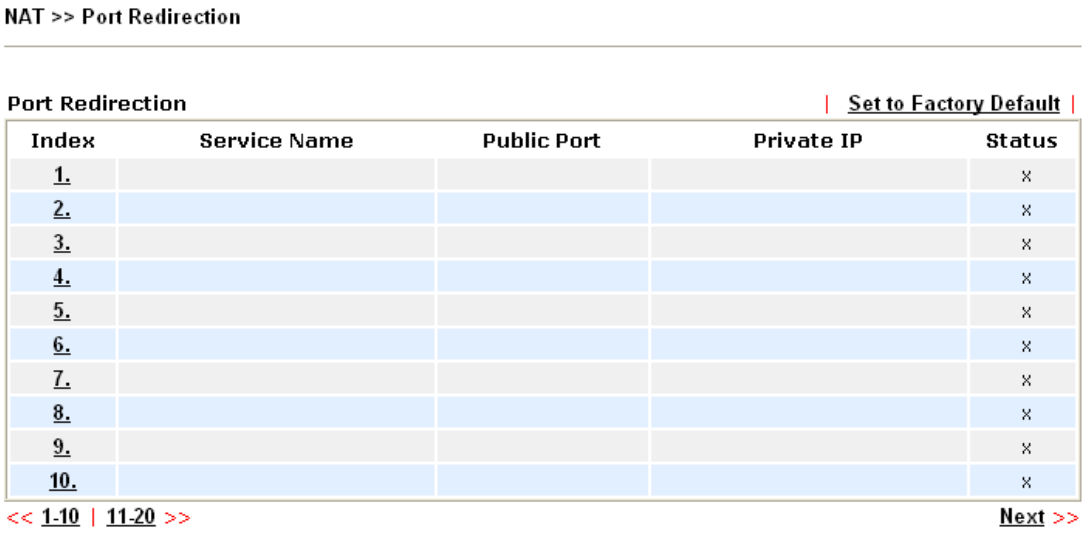
3.3.1 Port Redirection

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.

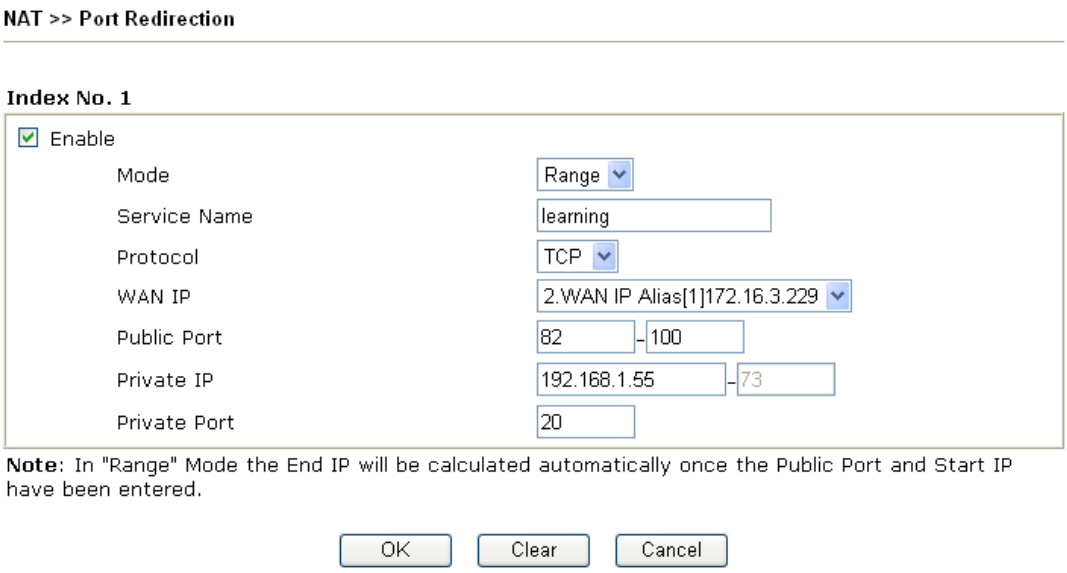


The port redirection can only apply to incoming traffic.

To use this function, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 20 port-mapping entries for the internal hosts.



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



Enable Check this box to enable such port redirection setting.

Mode Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select **Range**. In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.

Service Name Enter the description of the specific network service.

Protocol Select the transport layer protocol (TCP or UDP).

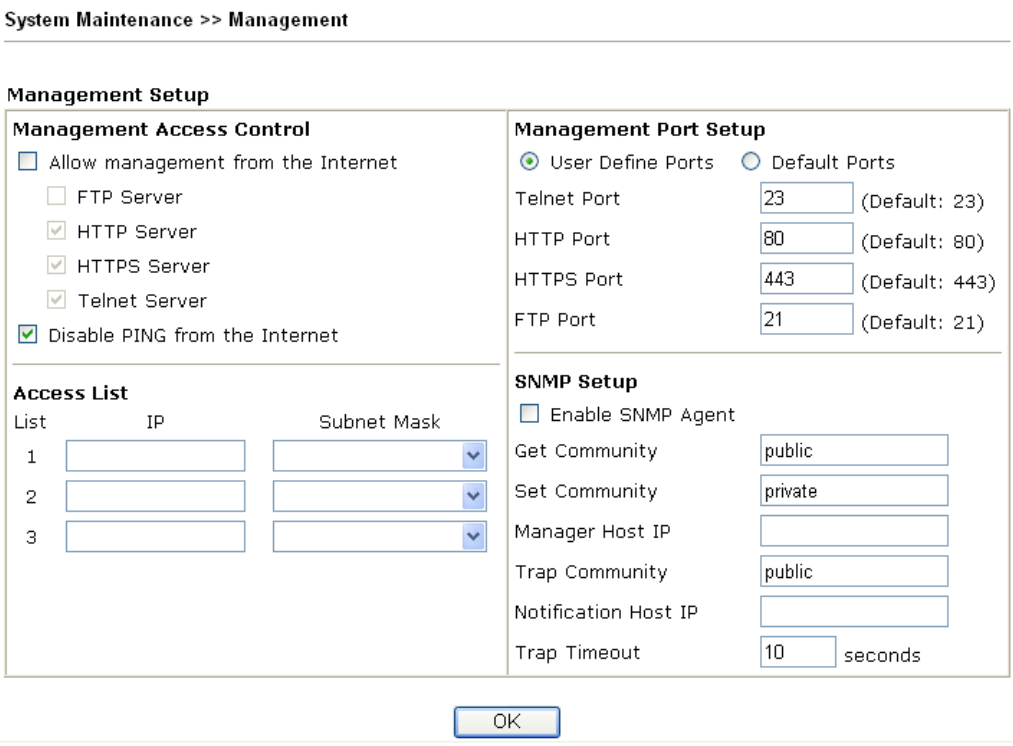
WAN IP Chose one set of WAN IP Alias address for applying port redirection. If you do not set any WAN IP Alias address, you can just choose **All** as WAN IP.

Public Port Specify which port can be redirected to the specified **Private IP and Port** of the internal host. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Simply type the required numbers on these two boxes.

Private IP	Specify the private IP address of the internal host providing the service. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Simply type the IP address in the first box (as the starting point). The second one is assigned automatically after you type the private port number below.
Private Port	Specify the private port number of the service offered by the internal host. After you enter the proper number in this box, the second box of Private IP address will be assigned accordingly.
Active	Check this box to activate the port-mapping entry you have defined.

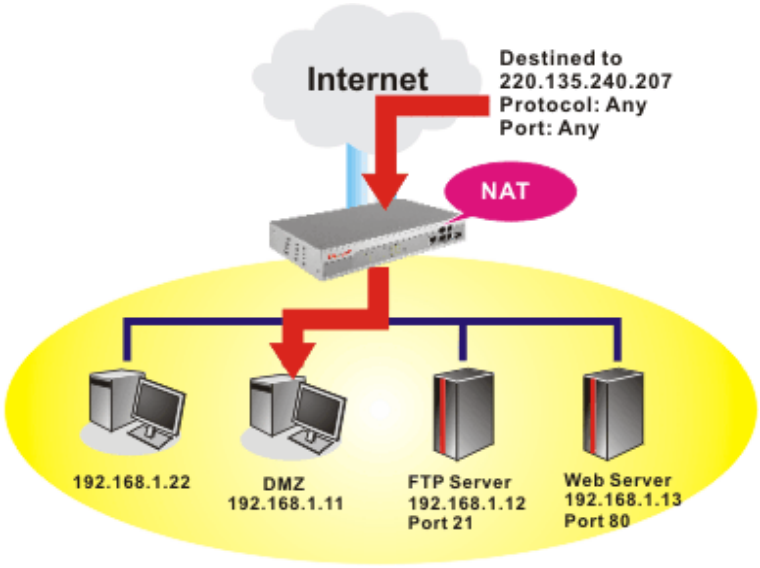
Note that the router has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the router in order to avoid confliction.

For example, the built-in web configurator in the router is with default port 80, which may conflict with the web server in the local network, http://192.168.1.13:80. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080. This can be set in the **System Maintenance >>Management Setup**. You then will access the admin screen of by suffixing the IP address with 8080, e.g., http://192.168.1.1:8080 instead of port 80.



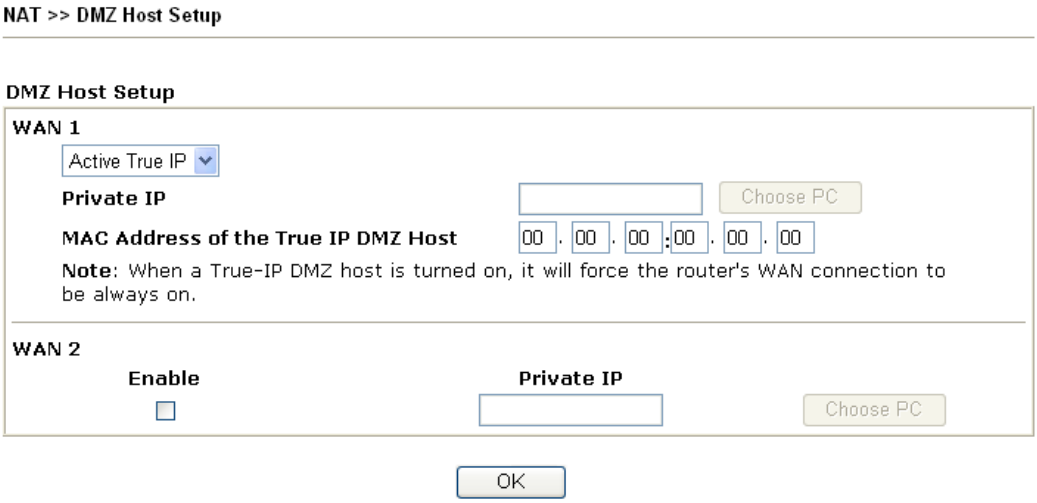
3.3.2 DMZ Host

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 inherent 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:

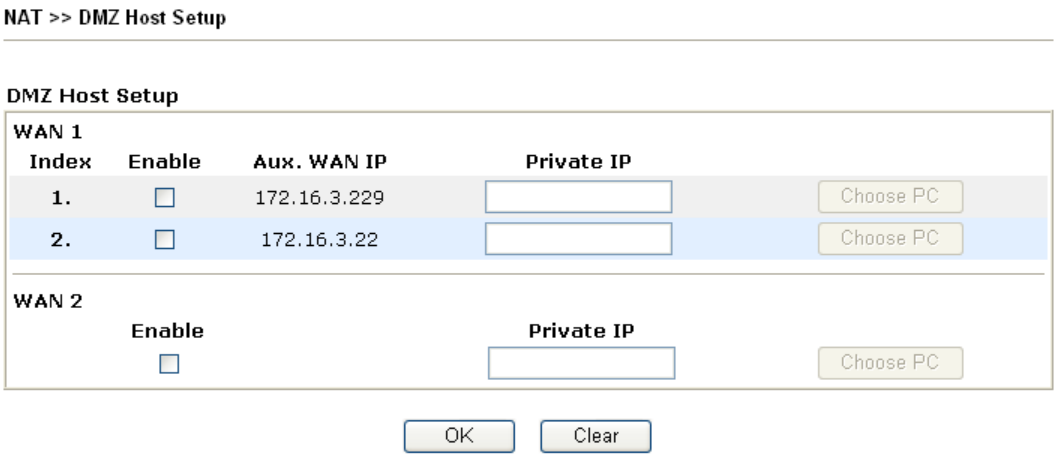


WAN1 — This page allows you to configure **Private IP** or **Active True IP** as DMZ host.

Private IP — If you choose **Private IP** as DMZ host, you can type a private IP in this box or use Choose PC button to choose the one you want.

MAC Address of the True…. — If you choose **Active True IP** as DMZ host, please type the MAC address of the one you want.

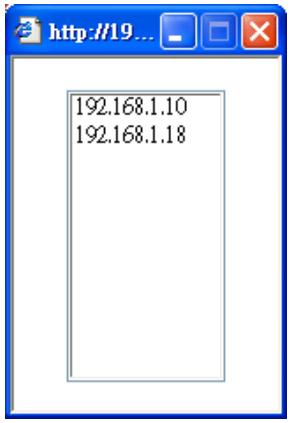
If you previously have set up **WAN Alias** in **Internet Access>>PPPoE,** you will find them in **Aux. WAN IP list** for your selection.



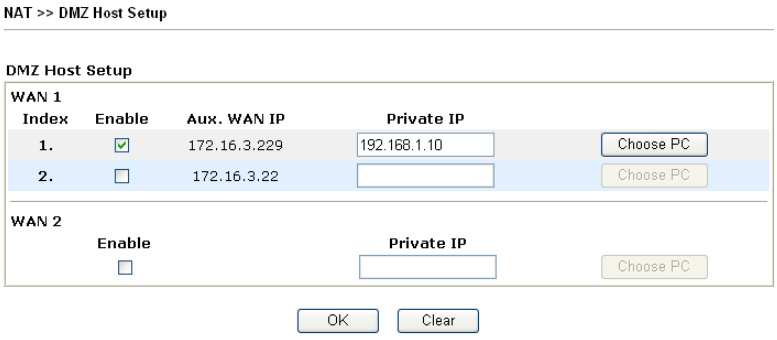
Enable Check to enable the DMZ Host function.

Private IP Enter the private IP address of the DMZ host, or click Choose PC to select one.

Choose PC Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.



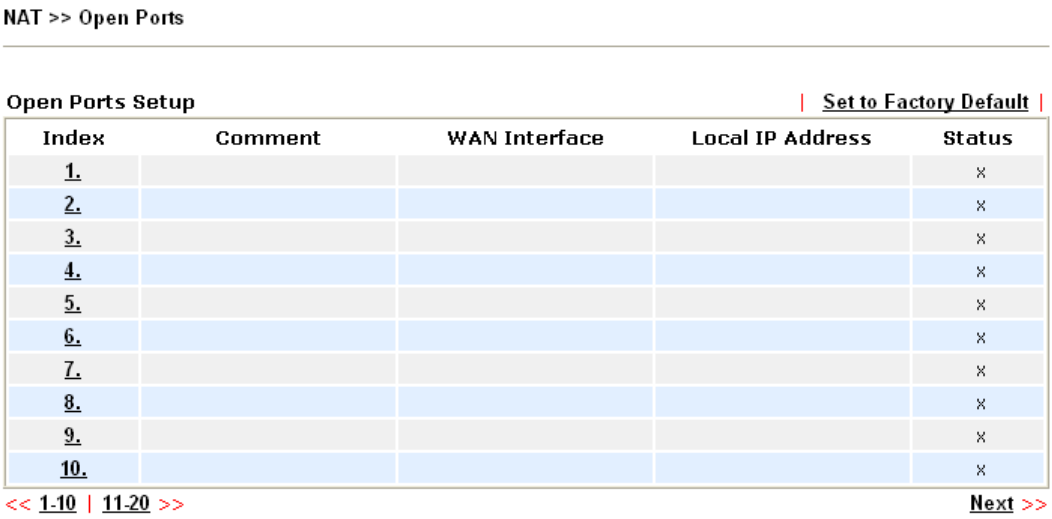
When you have selected one private IP from the above dialog, the IP address will be shown on the following screen. Click **OK** to save the setting.



3.3.3 Open Ports

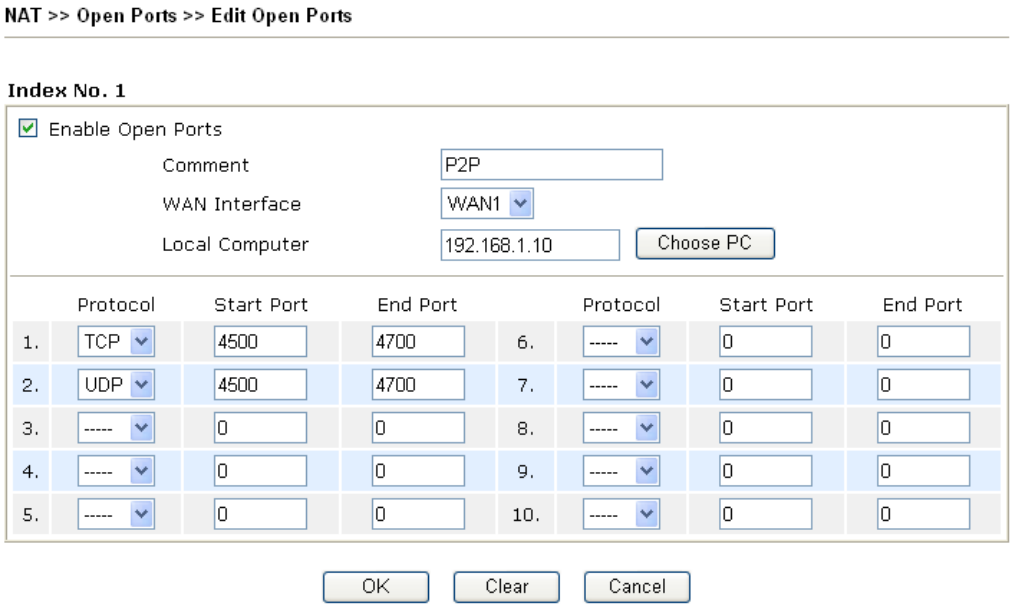
Open Ports allows you to open a range of ports for the traffic of special applications. Common application of Open Ports includes P2P application (e.g., BT, KaZaA, Gnutella, WinMX, eMule and others), Internet Camera etc. Ensure that you keep the application involved up-to-date to avoid falling victim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

Click **Open Ports** to open the following page:



Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
Comment	Specify the name for the defined network service.
WAN Interface	Display the WAN interface for the entry.
Local IP Address	Display the private IP address of the local host offering the service.
Status	Display the state for the corresponding entry. X or V is to represent the **Inactive** or **Active** state.

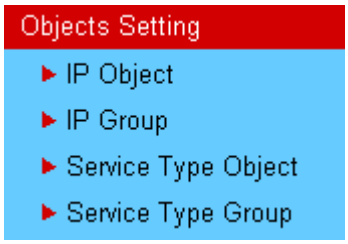
To add or edit port settings, click one index number on the page. The index entry setup page will pop up. In each index entry, you can specify **10** port ranges for diverse services.



Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
WAN Interface	Specify the WAN interface that will be used for this entry.
Local Computer	Enter the private IP address of the local host or click **Choose PC** to select one.
Choose PC	Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.
Protocol	Specify the transport layer protocol. It could be **TCP**, **UDP**, or **-----** (none) for selection.
Start Port	Specify the starting port number of the service offered by the local host.
End Port	Specify the ending port number of the service offered by the local host.

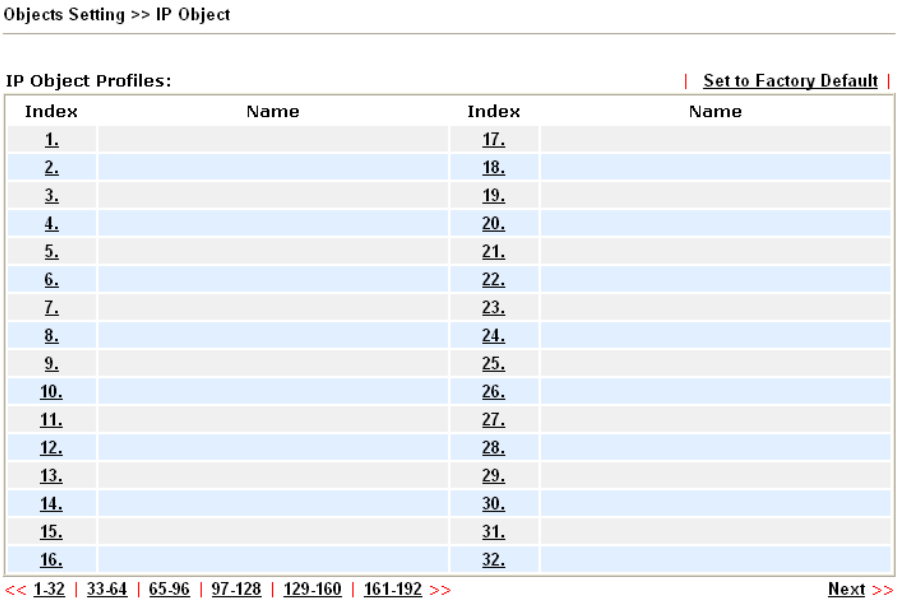
3.4 Objects Settings

For IPs in a range, service ports in a limited range and keywords usually will be applied for configuring router's settings, we can define them with ***objects*** and bind them with ***groups*** for using conveniently. Later, we can select that object/service for applying. For example, all the IPs in the same department can be defined with an IP object (a range of IP address).



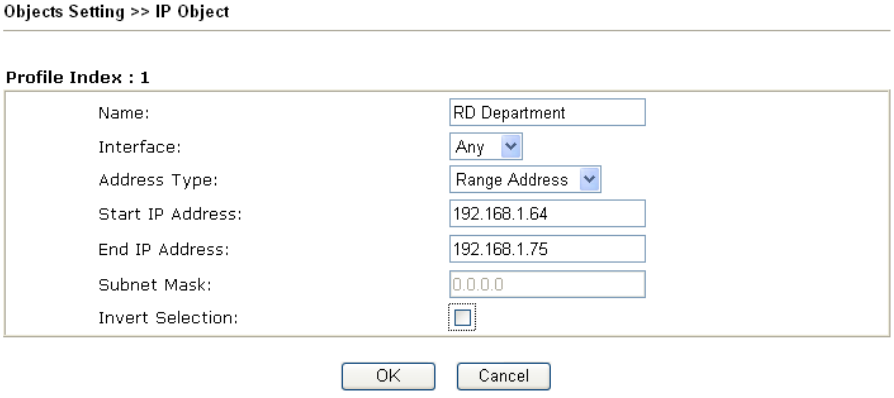
3.4.1 IP Object

You can set up to 192 sets of IP Objects with different conditions.

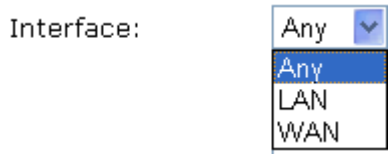


Set to Factory Default Clear all profiles.

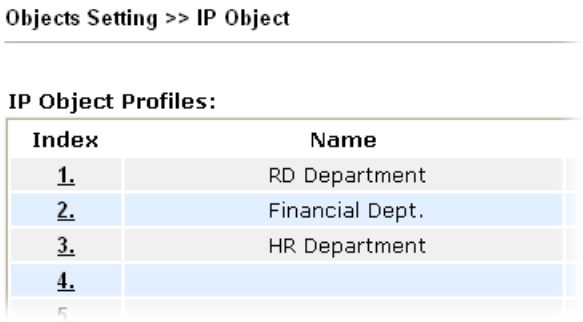
Click the number under Index column for settings in detail.



Name Type a name for this profile. Maximum 15 characters are allowed.

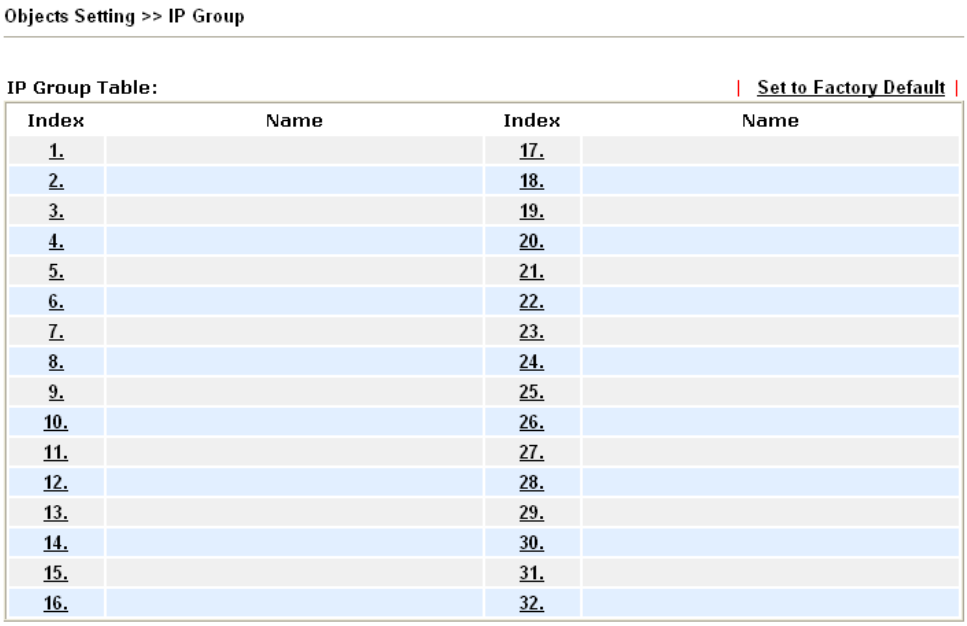
Interface	Choose a proper interface (WAN, LAN or Any).  For example, the **Direction** setting in **Edit Filter Rule** will ask you specify IP or IP range for WAN or LAN or any IP address. If you choose LAN as the **Interface** here, and choose LAN as the direction setting in **Edit Filter Rule**, then all the IP addresses specified with LAN interface will be opened for you to choose in **Edit Filter Rule** page.
Address Type	Determine the address type for the IP address. Select **Single Address** if this object contains one IP address only. Select **Range Address** if this object contains several IPs within a range. Select **Subnet Address** if this object contains one subnet for IP address. Select **Any Address** if this object contains any IP address.
Start IP Address	Type the start IP address for Single Address type.
End IP Address	Type the end IP address if the Range Address type is selected.
Subnet Mask	Type the subnet mask if the Subnet Address type is selected.
Invert Select	If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.

Below is an example of IP objects settings.



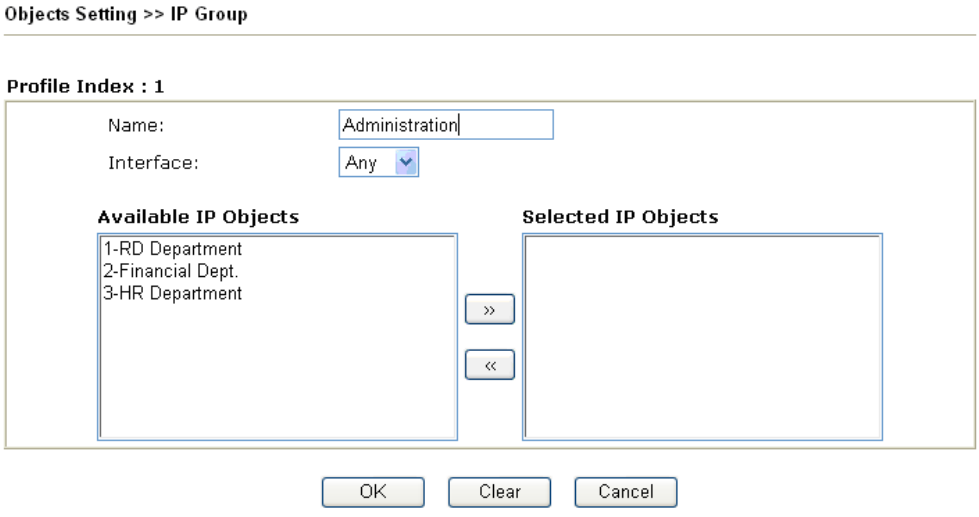
3.4.2 IP Group

This page allows you to bind several IP objects into one IP group.



Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.



Name Type a name for this profile. Maximum 15 characters are allowed.

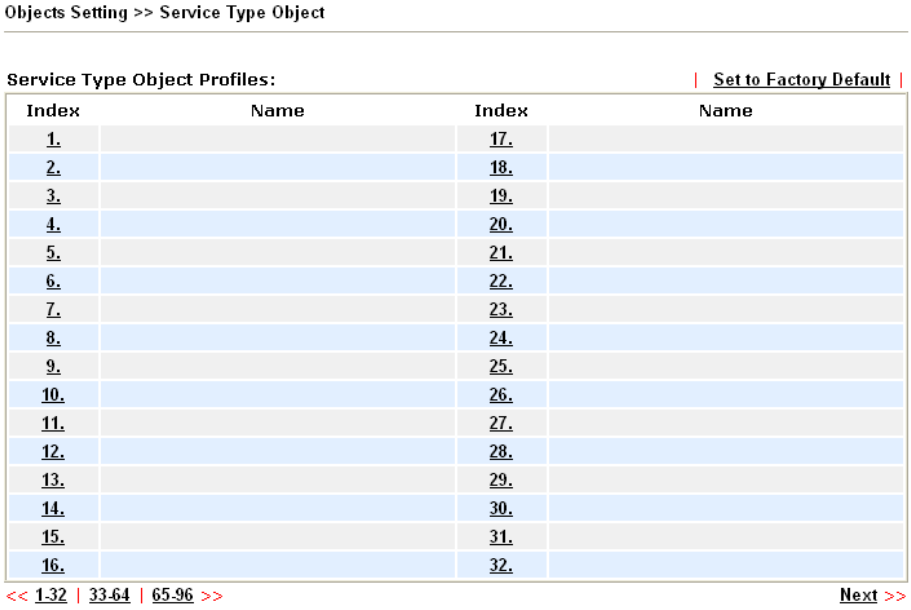
Interface Choose WAN, LAN or Any to display all the available IP objects with the specified interface.

Available IP Objects All the available IP objects (created in IP Object web page) with the specified interface chosen above will be shown in this box.

Selected IP Objects Click  button to add the selected IP objects in this box.

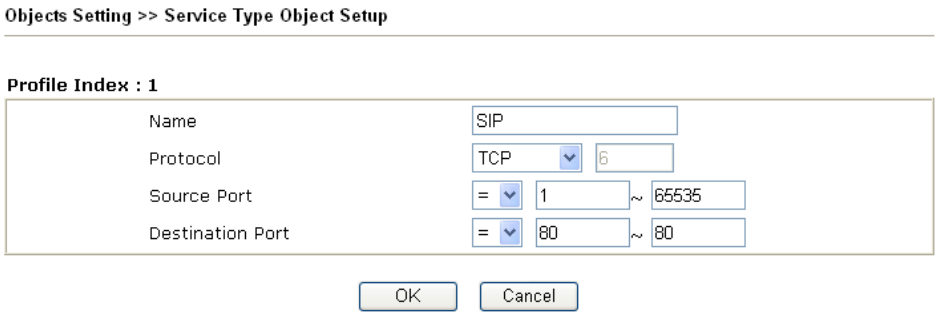
3.4.3 Service Type Object

You can set up to 96 sets of Service Type Objects with different conditions.



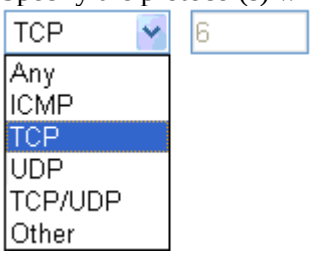
Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.



Name Type a name for this profile.

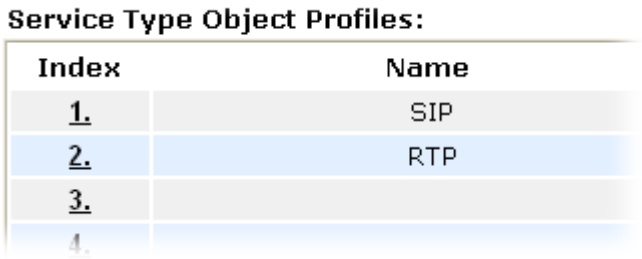
Protocol Specify the protocol(s) which this profile will apply to.



Source/Destination Port **Source Port** and the **Destination Port** column are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number.
(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile.
(!=) – when the first and last value are the same, it indicates

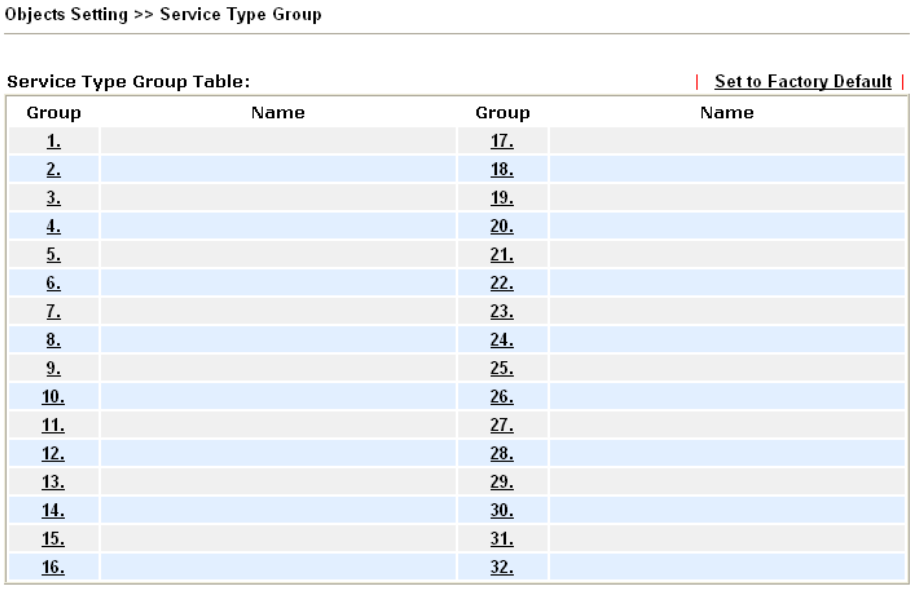
all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.
(>) – the port number greater than this value is available.
(<) – the port number less than this value is available for this profile.

Below is an example of service type objects settings.



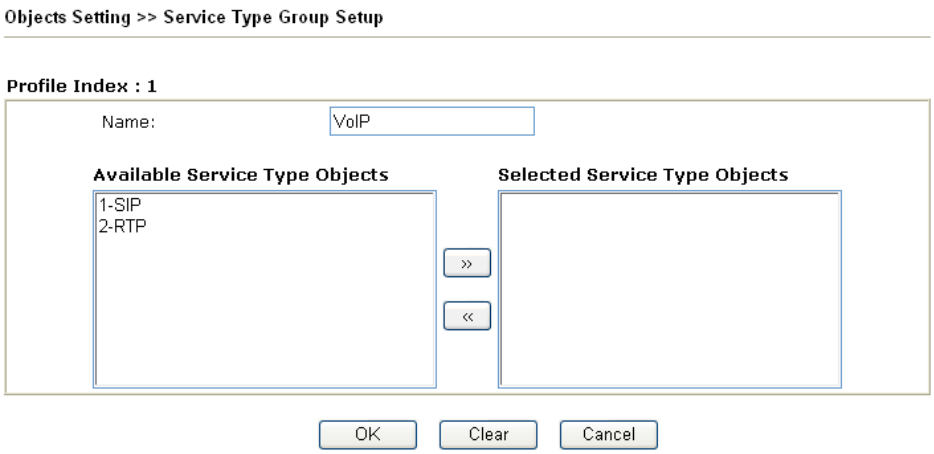
3.4.4 Service Type Group

This page allows you to bind several service types into one group.



Set to Factory Default Clear all profiles.

Click the number under Index column for setting in detail.



Name	Type a name for this profile.
Available Service Type Objects	You can add IP objects from IP Object page. All the available IP objects will be shown in this box.
Selected Service Type Objects	Click » button to add the selected IP objects in this box.

3.5 CSM

CSM is an abbreviation of **Content Security Management** which is used to control IM/P2P usage, filter the web content and URL content to reach a goal of security management.

IM/P2P

As the popularity of all kinds of instant messenger application arises, communication cannot become much easier. Nevertheless, while some industry may leverage this as a great tool to connect with their customers, some industry may take reserve attitude in order to reduce employee misusage during office hour or prevent unknown security leak. It is similar situation for corporation towards peer-to-peer applications since file-sharing can be convenient but insecure at the same time.

Content Filtering

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.

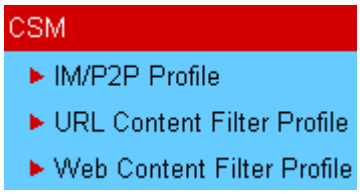
For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

Web Filtering

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, powered by SurfControl. The database covering over 70 languages and 200 countries, over 1 billion Web pages divided into 40 easy-to-understand categories. 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: The priority of URL Content Filter is higher than Web Content Filter.



3.5.1 IM/P2P Profile

You can define policy profiles for different policy of IM (Instant Messenger)/P2P (Peer to Peer) application. IM/P2P profile can be used in Filter Setup page.

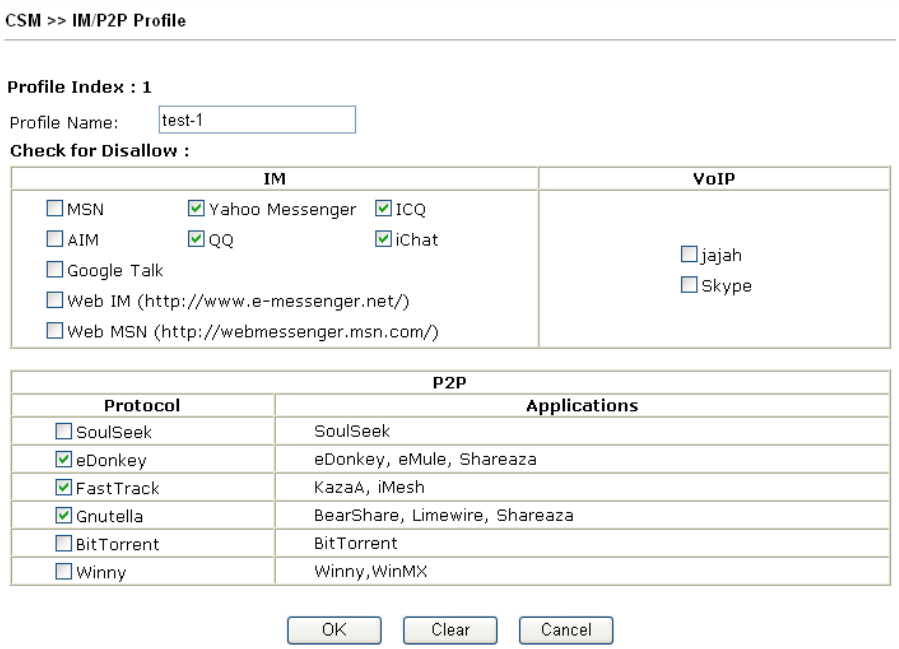
CSM >> IM/P2P Profile

IM/P2P Profile Table: | Set to Factory Default |

Profile	Name	Profile	Name
1.	test-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.	

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.



Profile Name Type a name for the IM/P2P profile.

There are several items for IM, VoIP, P2P provided here for you to choose to disallow people using. Simple check the box (es) and then click **OK**. Later, in the **Firewall>>Edit Filter Set>>Edit Filter Rule** page, you can use **Content Management** drop down list to choose the proper IM/P2P profile as the standard for the host(s) to follow.

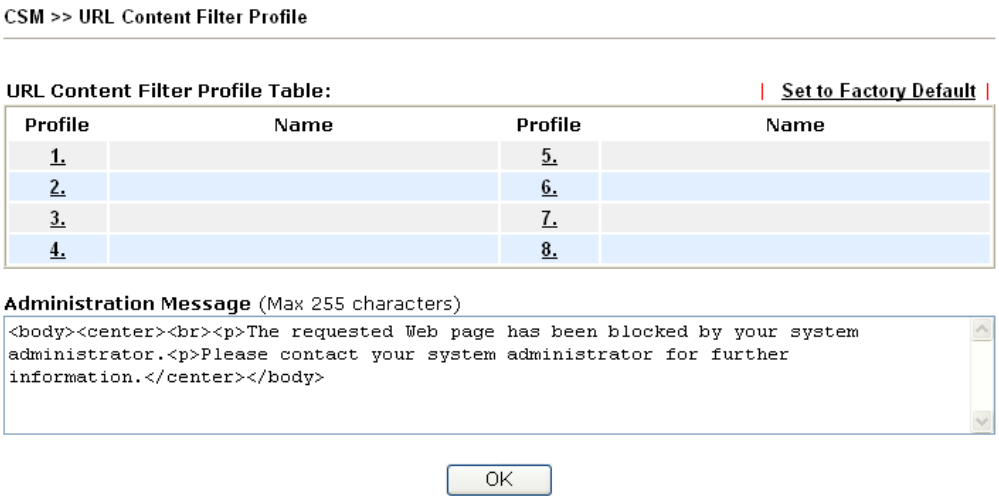
3.5.2 URL Content Filter Profile

Based on the list of user defined keywords, the **URL Content Filter** facility in Vigor router inspects the URL string in every outgoing HTTP request. No matter the URL string is found full or partial matched with a keyword, the Vigor router will block the associated HTTP connection.

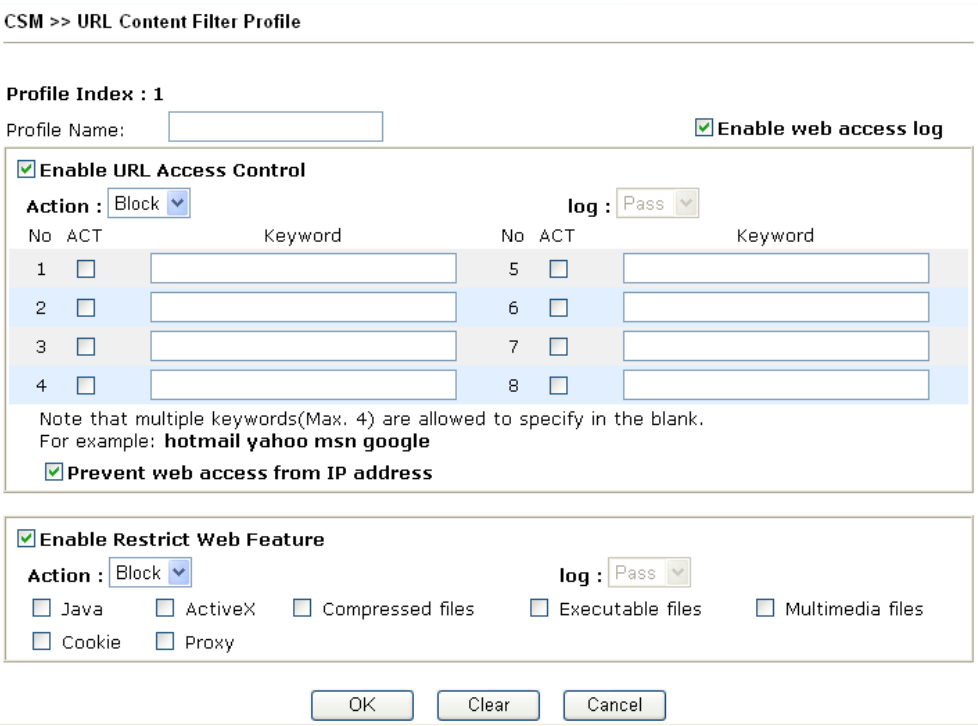
For example, if you add key words such as “sex”, Vigor router will limit web access to web sites or web pages such as “www.sex.com”, ”www.backdoor.net/images/sex/p_386.html”. Or you may simply specify the full or partial URL such as “www.sex.com” or “sex.com”.

Also the Vigor router will discard any request that tries to retrieve the malicious code.

Click **CSM** and click **URL Content Filter** to open the profile setting page.



You can set eight profiles as URL content filter. Simply click the index number under Profile to open the following web page.

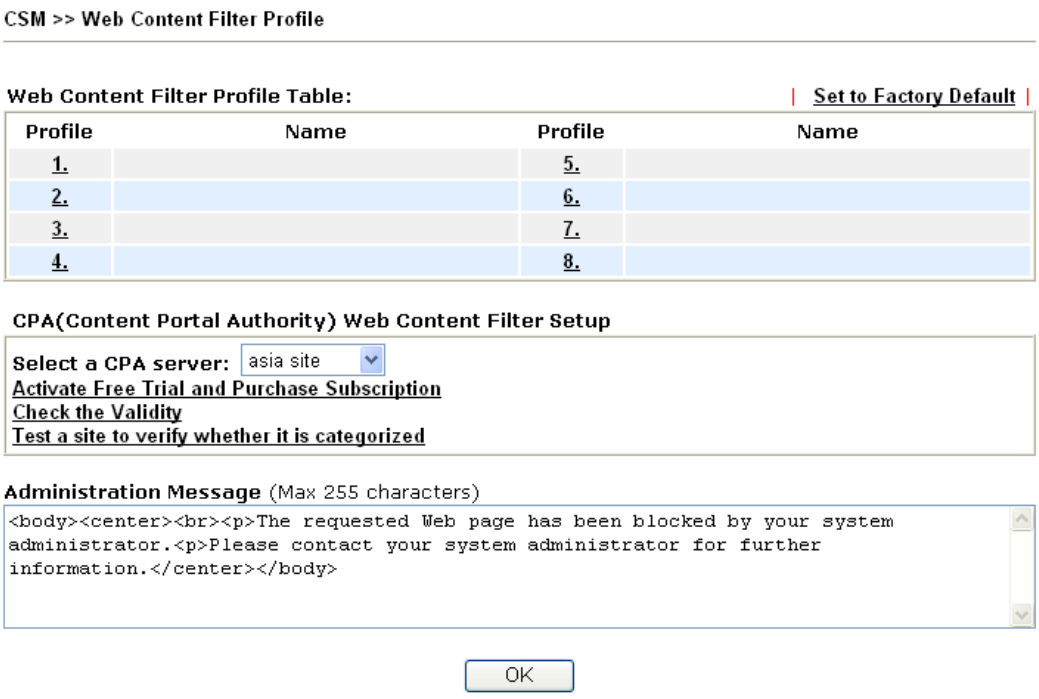


Profile Name	Type the name for such profile.
Enable web access log	Check the box to record URL Access Control and Restrict Web Features actions on Syslog. If you want to record them on Syslog for your request, please uncheck this box.
Enable URL Access Control	Check the box to activate URL Access Control. Note that the priority for **URL Access Control** is higher than **Restrict Web Feature**. If the web content match the setting set in URL Access Control, the router will execute the action specified in this field and ignore the action specified under Restrict Web Feature.
Action	**Pass** - allow accessing into the corresponding webpage with the keywords listed on the box below. **Block** - restrict accessing into the corresponding webpage with the keywords listed on the box below.

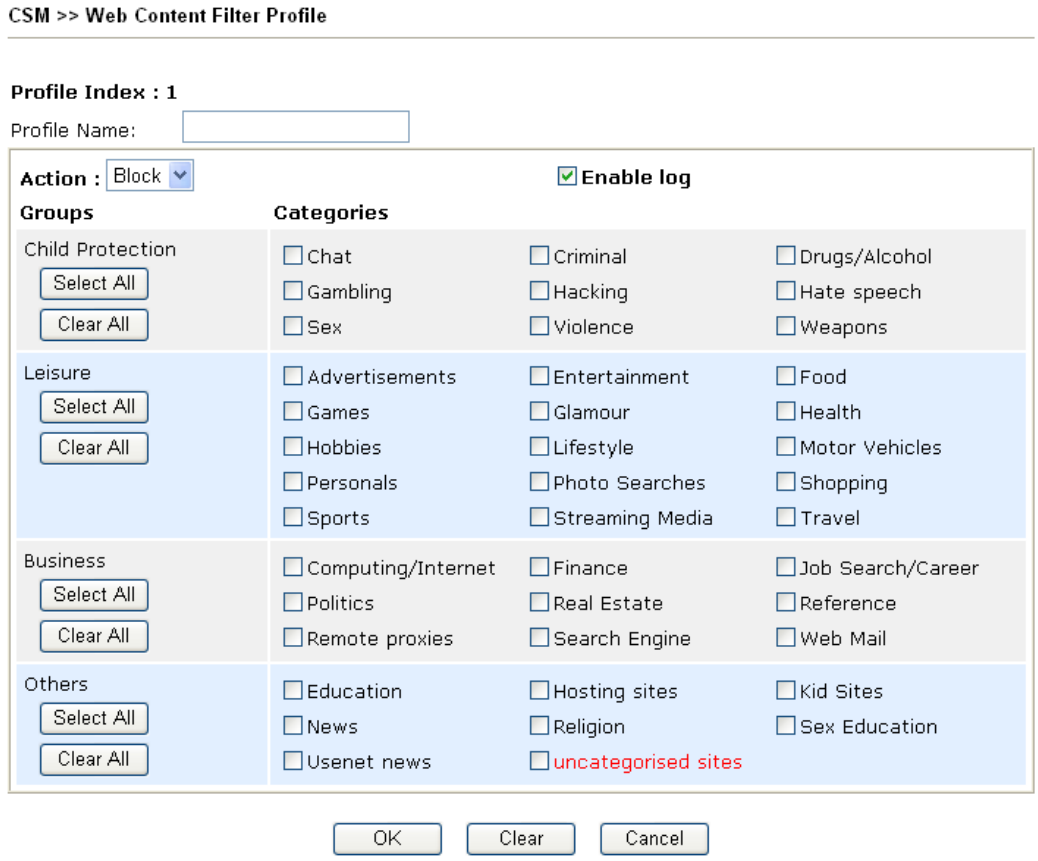
	If the web pages do not match with the keyword set here, it will be processed with reverse action.
ACT	Check this box to make the keyword being blocked or passed.
Keyword	The Vigor router provides 8 frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor router will decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the more simplified the blocking keyword list, the more efficiently the Vigor router perform.
Prevent web access from IP address	Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.
Enable Restrict Web Feature	Check the box to activate the function.
Action	**Pass** - allow accessing into the corresponding webpage with the keywords listed on the box below. **Block** - restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the specified feature set here, it will be processed with reverse action. ***Java*** - Check the checkbox to activate the Block Java object function. The Vigor router will discard the Java objects from the Internet. ***ActiveX*** - Check the box to activate the Block ActiveX object function. Any ActiveX object from the Internet will be refused. ***Compressed file*** - Check the box to activate the Block Compressed file function to prevent someone from downloading any compressed file. The following list shows the types of compressed files that can be blocked by the Vigor router. **.** **zip, rar, .arj, .ace, .cab, .sit** ***Executable file*** - Check the box to reject any downloading behavior of the executable file from the Internet. **.exe, .com, .scr, .pif, .bas, .bat, .inf, .reg** ***Cookie*** - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy. ***Proxy*** - Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages. Accordingly, files with the following extensions will be blocked by the Vigor router. **.mov .mp3 .rm .ra .au .wmv** **.wav .asf .mpg .mpeg .avi .ram**

3.5.3 Web Content Filter Profile

Click **CSM** and click **Web Content Filter** to open the profile setting page.



You can set eight profiles as Web content filter. Simply click the index number under Profile to open the following web page.



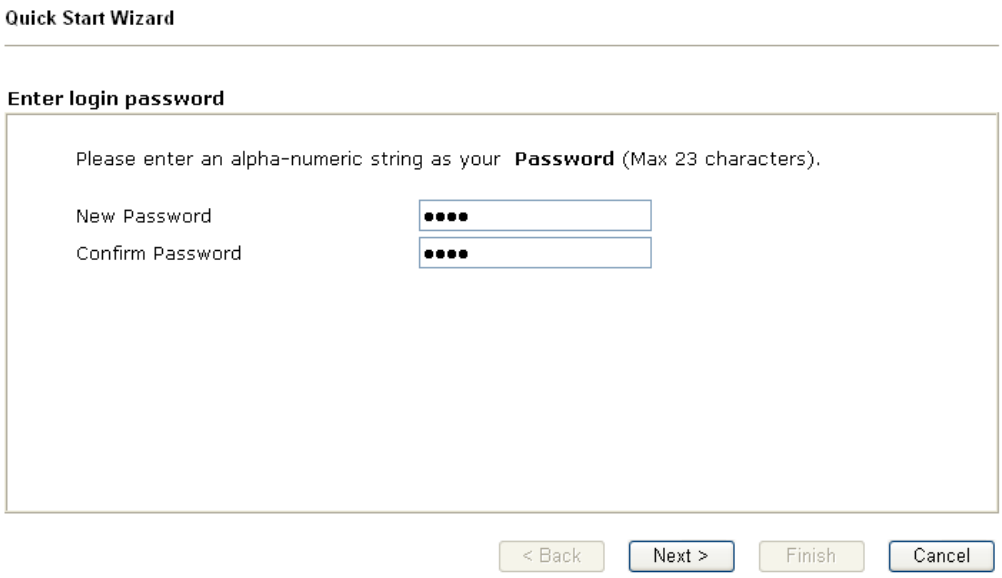
For this section, please refer to **Web Content Filter** user's guide.

3.6 Firewall

3.6.1 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.

The most basic security concept is to set user name and password while you install your router. The administrator login will prevent unauthorized access to the router configuration from your router.



If you did not set password during installation; you can go to **System Maintenance** to set up your password.

Firewall Facilities

The users on the LAN are provided with secured protection by the following firewall facilities:

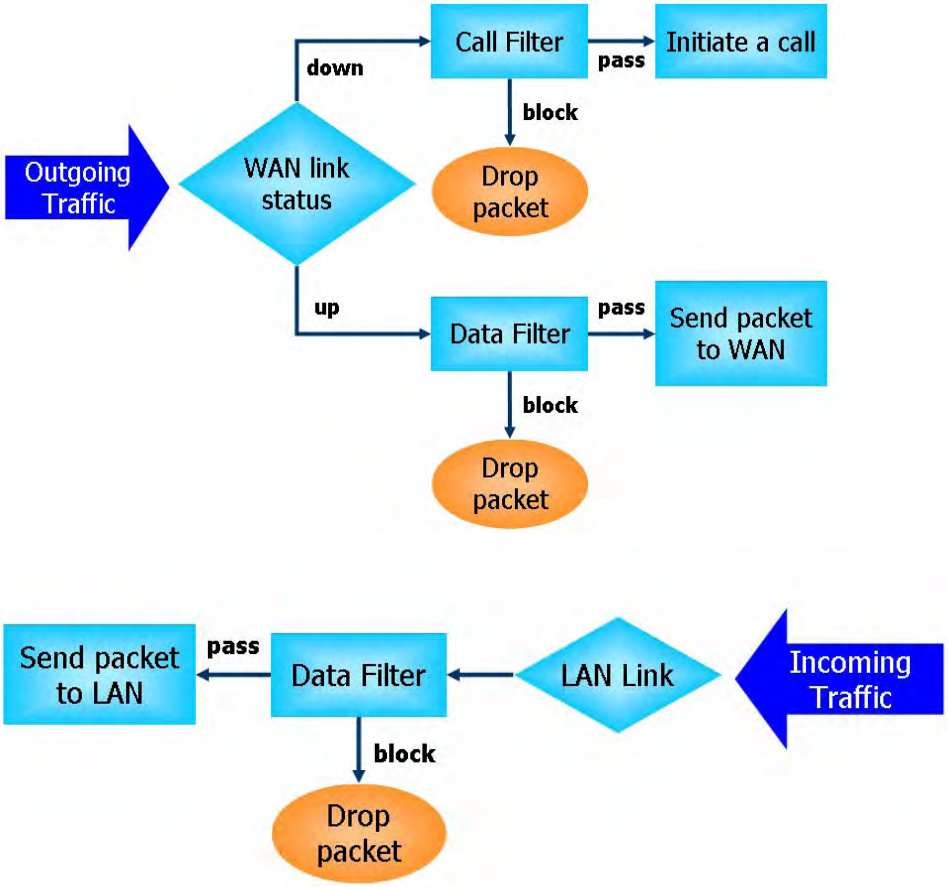
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection
- URL Content Filter

IP Filters

Depending on whether there is an existing Internet connection, or in other words “the WAN link status is up or down”, the IP filter architecture categorizes traffic into two: **Call Filter** and **Data Filter**.

- **Call Filter -** When there is no existing Internet connection, **Call Filter** is applied to all traffic, all of which should be outgoing. It will check packets according to the filter rules. If legal, the packet will pass. Then the router shall **“initiate a call”** to build the Internet connection and send the packet to Internet.
- **Data Filter** - When there is an existing Internet connection, **Data Filter** is applied to incoming and outgoing traffic. It will check packets according to the filter rules. If legal, the packet will pass the router.

The following illustrations are flow charts explaining how router will treat incoming traffic and outgoing traffic respectively.



Stateful Packet Inspection (SPI)

Stateful inspection 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.

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.

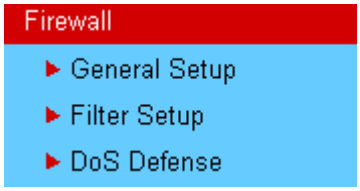
The below shows the attack types that DoS/DDoS defense function can detect:

1. SYN flood attack
2. UDP flood attack
3. ICMP flood attack
4. TCP Flag scan
5. Trace route
6. IP options
7. Unknown protocol
8. Land attack
9. Smurf attack
10. SYN fragment
11. ICMP fragment
12. Tear drop attack
13. Fraggle attack
14. Ping of Death attack
15. TCP/UDP port scan

Anti-Virus and Anti-Intrusion

Users might have much more confidence about the security in the network for data transmission if the functions of anti-virus and anti-intrusion are activated. The VigorPro router offers the mechanism of anti-virus and anti-intrusion. What you have to do is to set the proper profiles and invoke them. The anti-virus profile and anti-intrusion configuration can be set in Anti-Virus menu (refer to section 3.7) and Anti-Intrusion menu (refer to section 3.6). However, the mechanism must be enabled either in **Firewall>>General Setup** or **Firewall>>Filter Setup** web page. After you choose proper Anti-Virus profile and check Anti-Intrusion box, the Anti-Virus and Anti-Intrusion LEDs on the front panel will light up.

Below shows the menu items for Firewall.

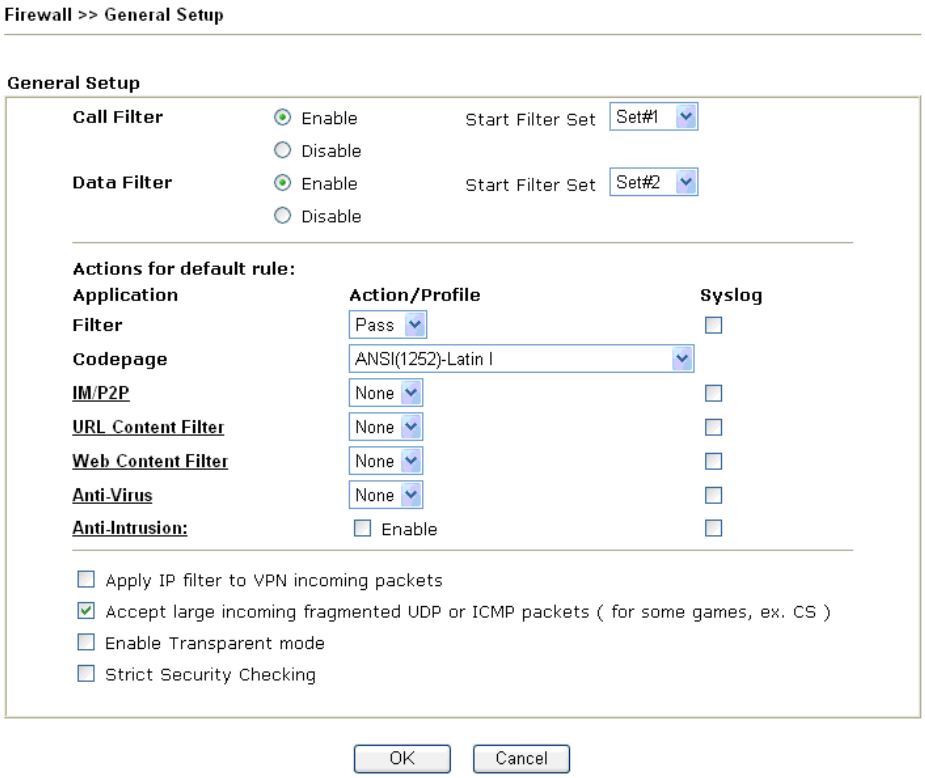


3.6.2 General Setup

General Setup allows you to adjust settings of IP Filter and common options. Here you can enable or disable the **Call Filter** or **Data Filter**. Under some circumstance, your filter set can be linked to work in a serial manner. So here you assign the **Start Filter Set** only. Also you can configure the **Log Flag** settings, **Apply IP filter to VPN incoming packets**, and **Accept incoming fragmented UDP packets**.

> **Important:** When some packet does not fit the rule configured in **Filter Setup** web page, the filtering action configured in general setup web page will apply to that packet.

Click **Firewall** and click **General Setup** to open the general setup page.

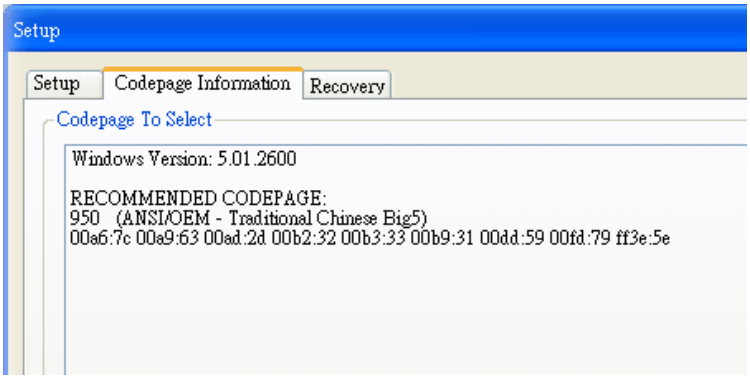


Call Filter Check **Enable** to activate the Call Filter function. Assign a start filter set for the Call Filter.

Data Filter Check **Enable** to activate the Data Filter function. Assign a start filter set for the Data Filter.

Filter Select **Pass** or **Block** for the packets that do not match with the filter rules.

CodePage This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.
If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.

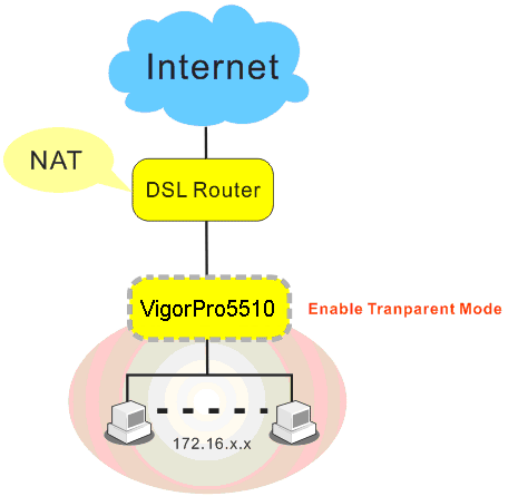


IM/P2P	Select an IM/P2P profile for global IM/P2P application blocking. All the hosts in LAN must follow the standard configured in the IM/P2P profile selected here. For detailed information, refer to the section of IM/P2P profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section 3.13.4 Syslog/Mail Alert for more detailed information.
URL Content Filter	Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter** web page first. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section 3.13.4 Syslog/Mail Alert for more detailed information.
Web Content Filter	Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter** web page first. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section 3.13.4 Syslog/Mail Alert for more detailed information.
Anti-Virus	Select one of the anti-virus profile settings (created in **Anti-Virus>>Profile Setting**) for applying with this router. Please set at least one profile for anti-virus in **Anti-Virus-> Profile Setting** web page first. For troubleshooting needs, you can specify to record information for **Anti-Virus** by checking the Log box. It will be sent to Syslog server. Please refer to section 3.13.4 Syslog/Mail Alert for more detailed information.
Anti-Intrusion	Check the **Enable** box to invoke anti-intrusion filter function. For troubleshooting needs, you can specify to record information for **Anti-Intrusion** by checking the Log box. It will be sent to Syslog server. Please refer to section 3.13.4 Syslog/Mail Alert for more detailed information.
Apply IP filter to VPN incoming packets	Check this box to enable the function.
Accept large incoming…	Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable "**Accept large incoming**

fragmented UDP or ICMP Packets". By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable "**Accept large incoming fragmented UDP or ICMP Packets**".

Enable Transparent Mode

Check this box to enable transparent function for such router. It is not necessary for users to re-organize the network or configure the subnet settings for each PC connected under such router. However, the configured Anti-Virus and Anti-Intrusion profiles can be applied to PCs connected behind vigor router to have the best security. The following picture explains the basic structure for using transparent mode for vigor router.



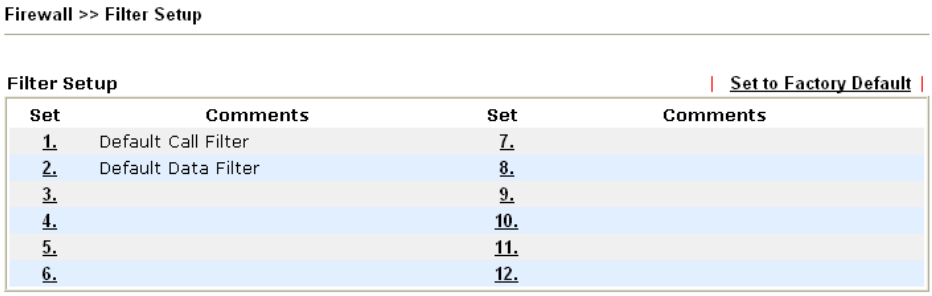
PCs with subnet "172.16.x.x" connected under VigorPro 5510 will be protected by security settings enabled and configured on the web pages of Vigor router. When the transparent mode has been checked, hackers from Internet do not sense the existence of vigor router, therefore they cannot attack the router.

Strict Security Checking

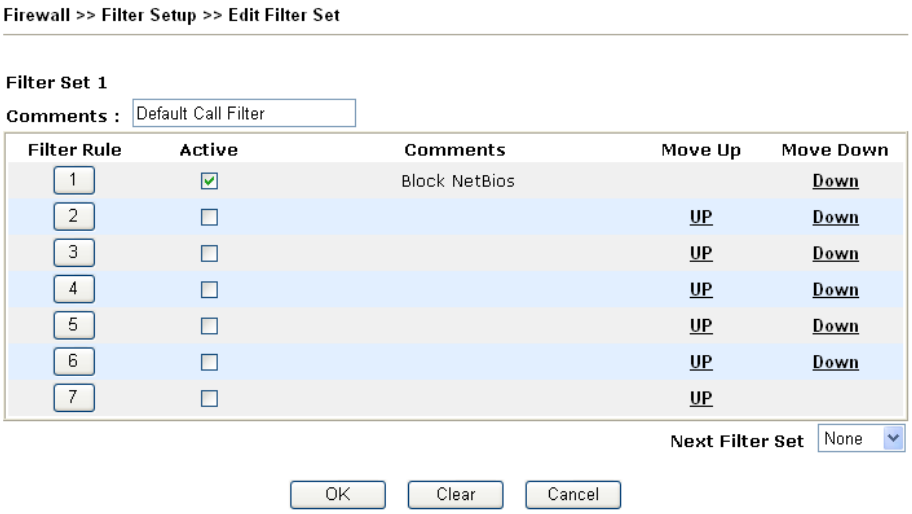
When the system resource is insufficient, the network connection will be examined for blocking or passing transmitted data. If it is not checked, the default action is "pass" for the data transmission.

3.6.3 Filter Setup

Click **Firewall** and click **Filter Setup** to open the setup page.



To edit or add a filter, click on the set number to edit the individual set. The following page will be shown. Each filter set contains up to 7 rules. Click on the rule number button to edit each rule. Check **Active** to enable the rule.



Filter Rule Click a button numbered (1 ~ 7) to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.

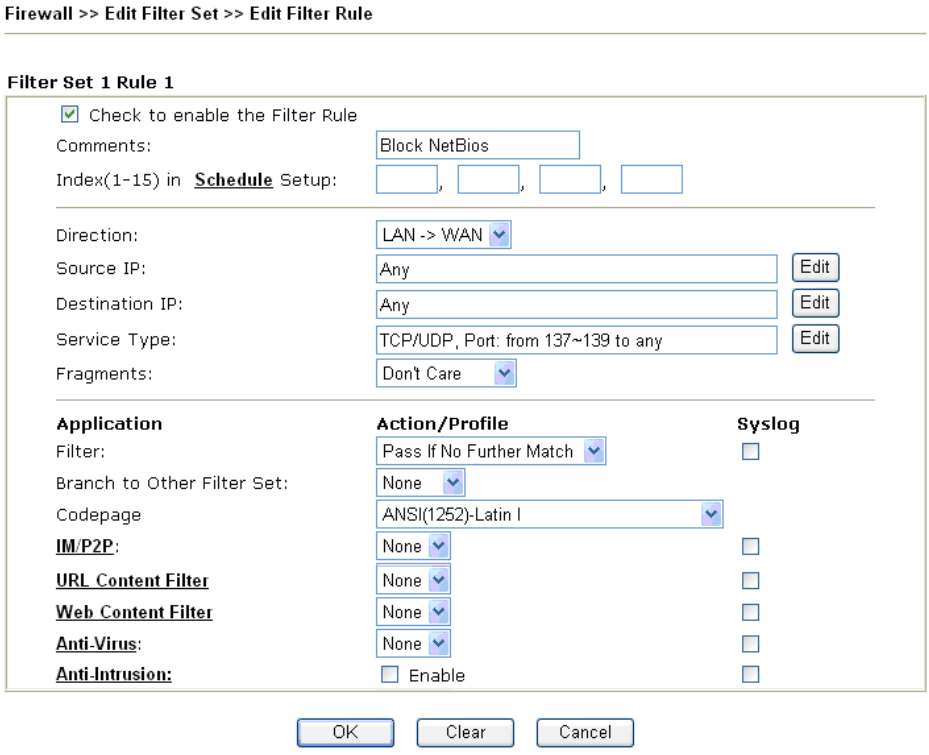
Active Enable or disable the filter rule.

Comment Enter filter set comments/description. Maximum length is 23–character long.

Move Up/Down Use **Up** or **Down** link to move the order of the filter rules.

Next Filter Set Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.

To edit **Filter Rule**, click the **Filter Rule** index button to enter the **Filter Rule** setup page.



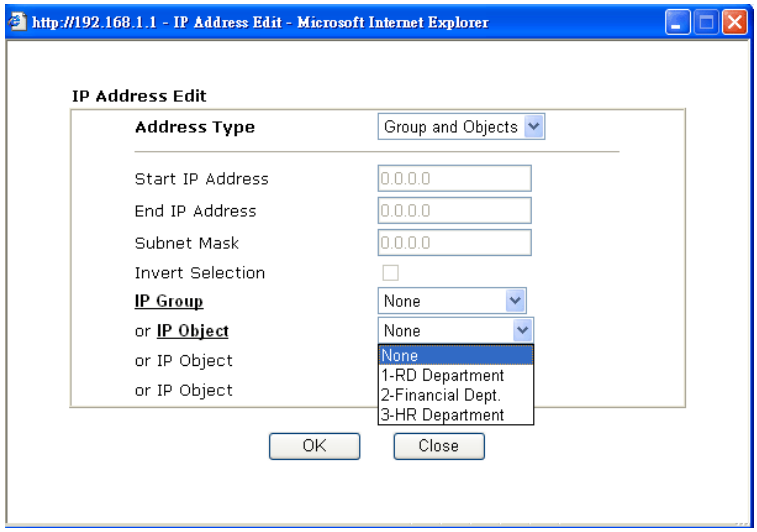
Check to enable the Filter Rule Check this box to enable the filter rule.

Comments Enter filter set comments/description. Maximum length is 14-character long.

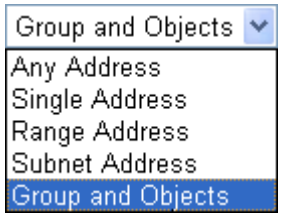
Index (1-15) Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications >> Schedule** setup. The default setting of this filed is blank and the function will always work.

Direction Set the direction of packet flow (LAN->WAN/WAN->LAN). It is for **Data Filter** only. For the **Call Filter**, this setting is not available since **Call Filter** is only applied to outgoing traffic.

Source/Destination IP Click **Edit** to access into the following dialog to choose the source/destination IP or IP ranges.

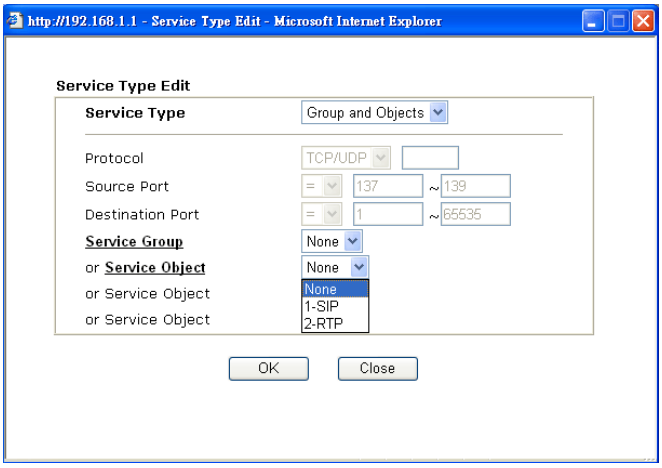


To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.

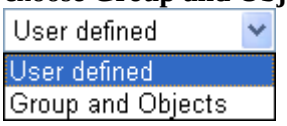


From the **IP Group** drop down list, choose the one that you want to apply. Or use the **IP Object** drop down list to choose the object that you want.

Service Type Click **Edit** to access into the following dialog to choose a suitable service type.



To set the service type manually, please choose **User defined** as the Service Type and type them in this dialog. In addition, if you want to use the service type from defined groups or objects, please choose **Group and Objects** as the Service Type.



Protocol - Specify the protocol(s) which this filter rule will apply to.
Source/Destination Port -
(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type.
(!=) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.
(>) – the port number greater than this value is available.
(<) – the port number less than this value is available for this profile.
Service Group/Object - Use the drop down list to choose the one that you want.

Fragments

Specify the action for fragmented packets. And it is used for **Data Filter** only.
Don't care -No action will be taken towards fragmented packets.
Unfragmented -Apply the rule to unfragmented packets.
Fragmented - Apply the rule to fragmented packets.
Too Short - Apply the rule only to packets that are too short to contain a complete header.

Filter

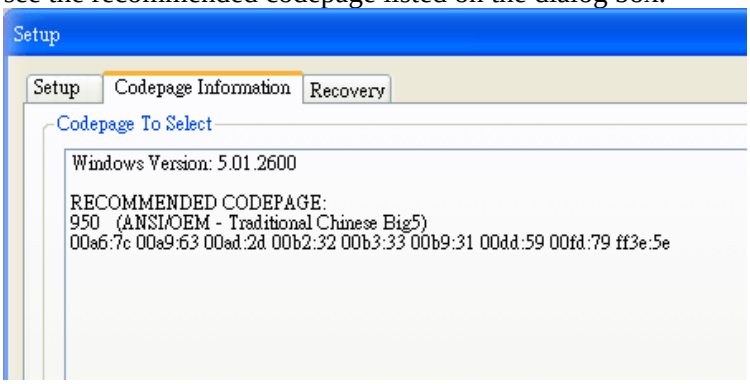
Specifies the action to be taken when packets match the rule.
Block Immediately - Packets matching the rule will be dropped immediately.
Pass Immediately - Packets matching the rule will be passed immediately.
Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.
Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.

Branch to other Filter

If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the

Set drop-down menu. Be aware that the router will apply the specified filter rule for ever and will not return to previous filter rule any more.

CodePage This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.
If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.



IM/P2P Select a IM/P2P profile for global IM/P2P application blocking. All the hosts in LAN must follow the standard configured in the IM/P2P profile selected here. For detailed information, refer to the section of IM/P2P profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section 3.13.4 Syslog/Mail Alert for more detailed information.

URL Content Filter Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter** web page first. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section 3.13.4 Syslog/Mail Alert for more detailed information.

Web Content Filter Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter** web page first. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section 3.13.4 Syslog/Mail Alert for more detailed information.

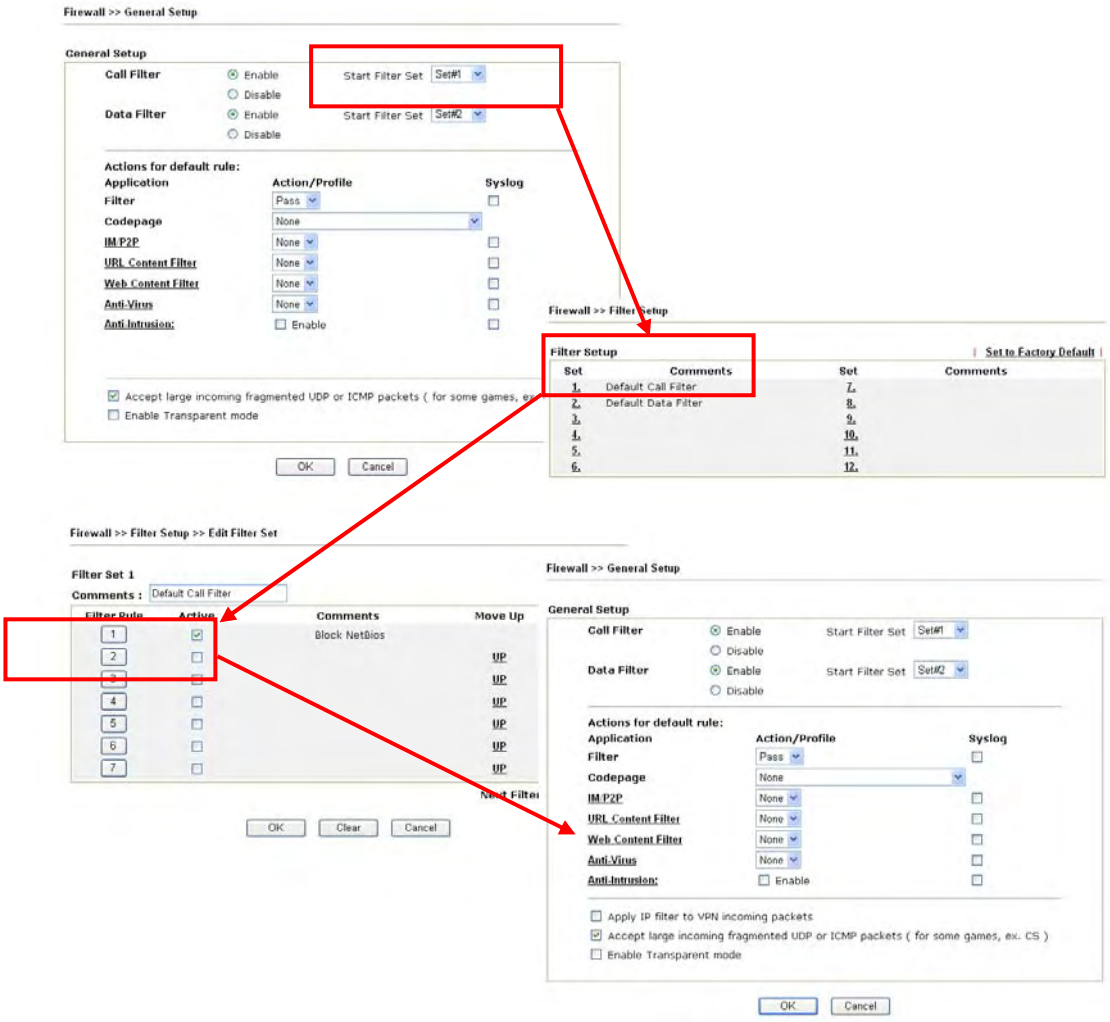
Anti-Virus Select one of the anti-virus profile settings (created in **Anti-Virus>>Profile Setting**) for applying with this router. Please set at least one profile for anti-virus in **Anti-Virus-> Profile Setting** web page first. For troubleshooting needs, you can specify to record information for **Anti-Virus** by checking the Log box. It

will be sent to Syslog server. Please refer to section 3.13.4 Syslog/Mail Alert for more detailed information.

Anti-Intrusion Check the **Enable** box to invoke anti-intrusion filter function. For troubleshooting needs, you can specify to record information for **Anti-Intrusion** by checking the Log box. It will be sent to Syslog server. Please refer to section 3.13.4 Syslog/Mail Alert for more detailed information.

Example

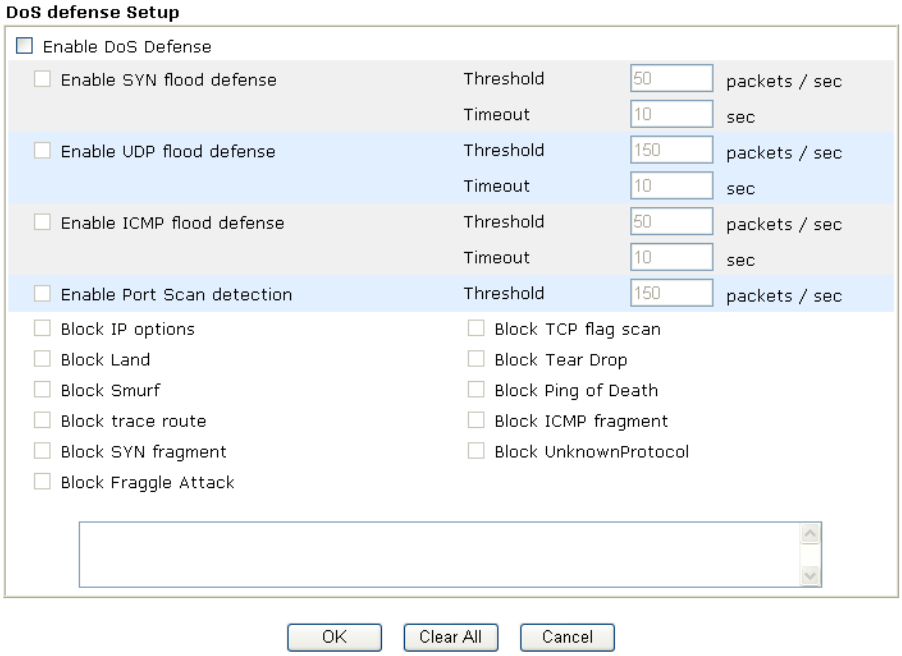
As stated before, all the traffic will be separated and arbitrated using on of two IP filters: call filter or data filter. You may preset 12 call filters and data filters in **Filter Setup** and even link them in a serial manner. Each filter set is composed by 7 filter rules, which can be further defined. After that, in **General Setup** you may specify one set for call filter and one set for data filter to execute first.



3.6.4 DoS Defense

As a sub-functionality of IP Filter/Firewall, there are 15 types of detect/defense function in the **DoS Defense** setup. The DoS Defense functionality is disabled for default.

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



Enable Dos Defense	Check the box to activate the DoS Defense Functionality.
Enable SYN flood defense	Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router. By default, the threshold and timeout values are set to 50 packets per second and 10 seconds, respectively.
Enable UDP flood defense	Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout. The default setting for threshold and timeout are 150 packets per second and 10 seconds, respectively.
Enable ICMP flood defense	Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet. The default setting for threshold and timeout are 50 packets per second and 10 seconds, respectively.
Enable PortScan 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 by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning. By default, the Vigor router sets the threshold as 150

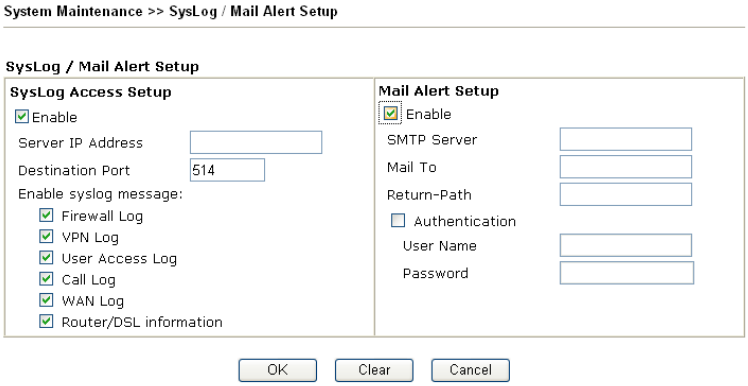
	packets per second.
Block IP options	Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages...etc. An eavesdropper outside might learn the details of your private networks.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.
Block trace router	Check the box to enforce the Vigor router not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.
Block Fraggle Attack	Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked. Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.
Block TCP flag scan	Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include *no flag scan*, *FIN without ACK scan*, *SYN FINscan*, *Xmas scan* and *full Xmas scan*.
Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
Block Ping of Death	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.
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.
Block Unknown Protocol	Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and

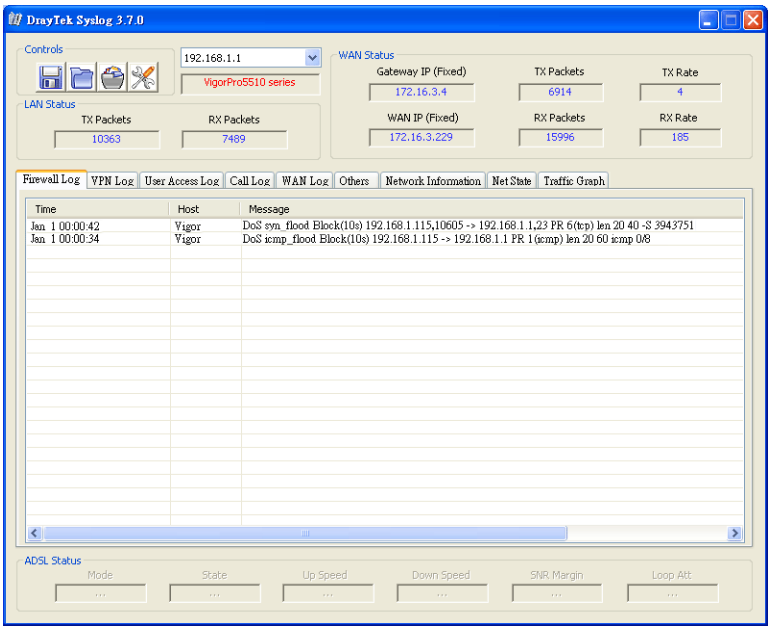
reject this kind of packets.

Warning Messages

We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client.

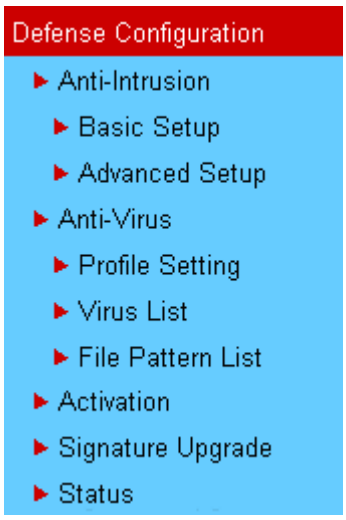
All the warning messages related to **DoS defense** will be sent to user and user can review it through Syslog daemon. Look for the keyword **DoS** in the message, followed by a name to indicate what kind of attacks is detected.





3.7 Defense Configuration

This menu allows you to set profiles for, activate and upgrade the service of Anti-Intrusion/Anti-Virus in your system.



3.7.1 Anti-Intrusion

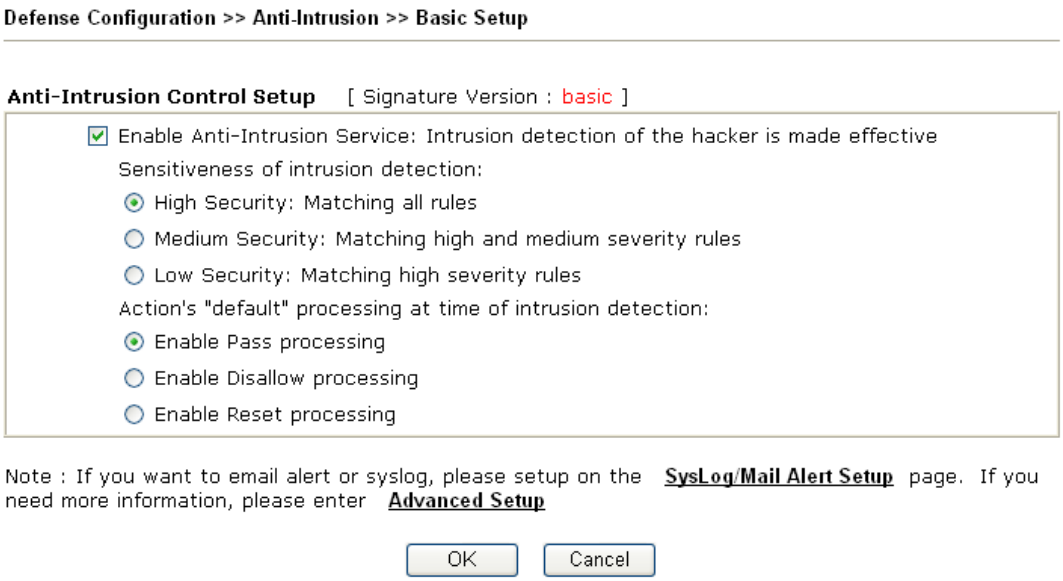
Anti-Intrusion allows you to prevent the intrusion from hackers while accessing into Internet. It can detect the intrusion and execute basic defense.

There are more than 200 basic rules for anti-intrusion and anti-virus for this router. To acquire more rules for anti-intrusion, it is suggested for you to register your router by entering www.vigorpro.com. When you finished the registration, you can get and activate a wide range of anti-intrusion rules from the website. In addition, you will be allowed to download/update new rules (if they are released) from the websites lately (during the valid time of the license key you purchased) after completing the registration.

You are allowed to use trial version with anti-intrusion and anti-virus features for 30 days after you register for the router. And you will be noticed with an e-mail while it is going to expire.

3.7.1.1 Basic Setup

Basic Setup page lets you to enable the anti-intrusion service and choose the suitable level for the detection.

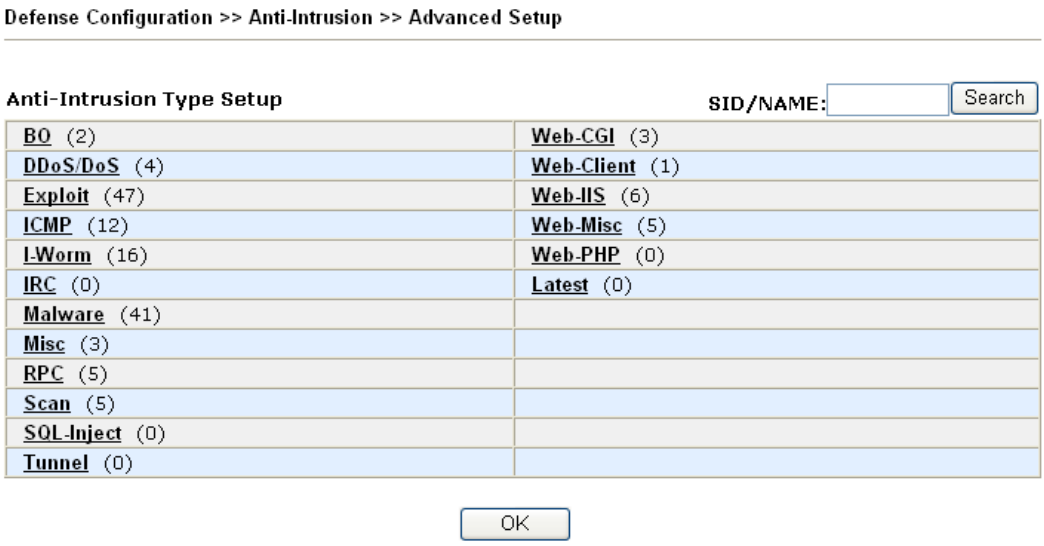


Anti-Intrusion Control Setup	This field will display the signature version of this router. The default signature version is "**basic**". In this version, you can modify the settings for Anti-Intrusion rules in **Defense Configuration>>Anti-Intrusion >>Advanced Setup** page. However, if you restart/reset the router, all the modified configurations for the rules will not be available and return to the default settings. Except "**basic**", the modified configurations for other signature versions are available all the time after you saved them in **Defense Configuration>>Anti-Intrusion >>Advanced Setup** page.
Enable Anti-Intrusion Service	Check this box to enable the anti-intrusion function.
High Security	Click this radio button to activate the anti-intrusion service with overall detecting conditions. That is, the router will detect and block the incoming/outgoing packets which match all the severity rules, including high, medium and low. The degree of severity for each rule is defined in Advance Setup.
Medium Security	Click this radio button to activate the anti-intrusion service with medium detecting conditions. That is, the router will detect and block the incoming/outgoing packets which match the highest and medium severity rules. The degree of severity for each rule is defined in Advance Setup.
Low Security	Click this radio button to activate the anti-intrusion service with minimum detecting conditions. That is, the router will detect and block the incoming/outgoing packets which match the highest severity rules. The degree of severity for each rule is defined in **Advanced Setup**.
Enable Pass processing	Click this radio button to detect if there is any intrusion occurrence for your reference. The system will not do any advanced action for such condition.
Enable Disallow processing	Click this radio button to block the incoming/outgoing packets with possible intrusion actions transmitting through the router.

Enable Reset procession Click this radio button to break down the communication between your computer and specific link which might have intrusion actions.

3.7.1.2 Advanced Setup

This page lists all the available types and allows you to adjust the rule setting for each type. The rules will be applied by the options chosen in the page of **Defense Configuration>>Anti-Intrusion>>Basic Setup** for Anti-Intrusion.



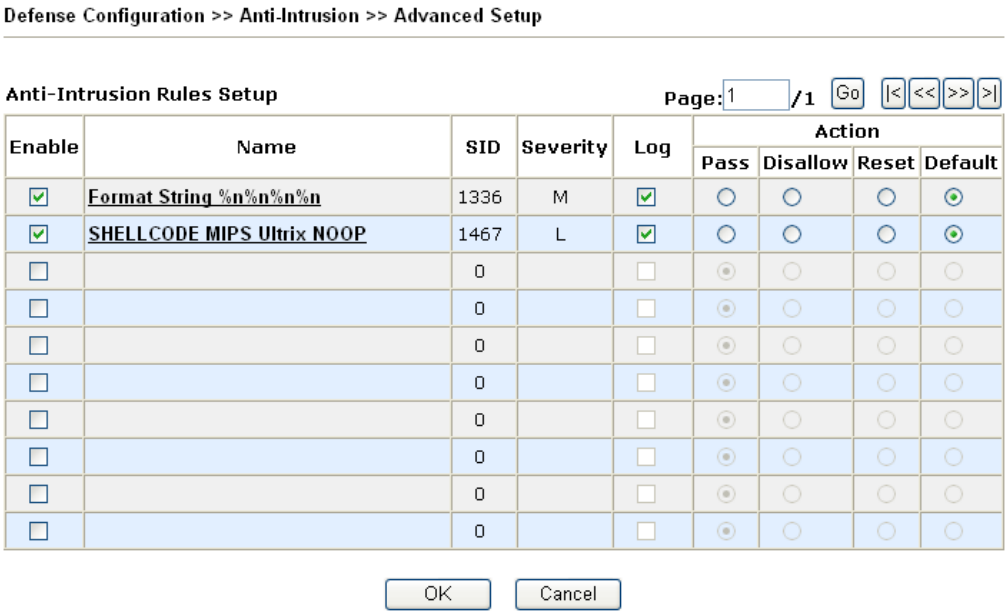
SID/Name To find the specific type of anti-intrusion, you can type its SID number or name in this field if you know, and then click **Search**. The system will locate that type for you.

Search It can help the user to find out specific anti-intrusion rule quickly.

Type links Click any anti-intrusion type link to access into next page for configuring the rules settings. Here we provide several rules for each type. The factory types and rules for anti-intrusion are shown in this page. If you want to acquire more types and rules, please go to www.vigorpro.com and finish the registration work. Later, the wide range of anti-intrusion types will be added into this page.

After you click any one of type links, you can access into the rules setup page for activating rules. We take the type of BO as an example. Below is the rules setup page for BO type.

For the detailed information about the full name, meaning of each rule and/or type, you can click the name link list on the Anti-Intrusion Rules Setup page to connect VigorPro webpage for viewing.



Enable Check to enable this rule. If you uncheck this box, the corresponding settings for the rule will not be executed.

SID The number for each anti-intrusion rule is displayed in this field.

Name A brief description name for the anti-intrusion rule is shown in this field. Click the name link to access into VigorPro website for checking the detailed information for the specified anti-intrusion.

Severity It means the degree of the influence for this type to the computer, machine, network and environment.
H: representing that this type will cause severest affection which must crash/destroy your computer.
M: representing that this type will cause severer affection which might crash your computer.
L: representing that this type will cause small affection which might not crash your computer.

Log In order to show the detection log with such rule on the window of Draytek Syslog, you have to check the log box here and enable the **SysLog Access Setup** from **System Maintenance >> Syslog/Mail Alert**.

Action **Pass -** Click this radio button to detect if there is any intrusion occurrence for your reference. The system will not do any advanced action for such condition.
Disallow - Click this radio button to block the incoming/outgoing packets with possible intrusion actions transmitting through the router.
Reset - Click this radio button to break down the communication between your computer and specific link which might have intrusion actions.
Default - Click this radio button to execute the anti-intrusion detection according to the setting that you set in Basic Setup.

Page Type the page number in this field (if there is more than one page of anti-virus detail view displayed on this page). Then

click **Go** to the specified page. Or you can click /**>**, **>>**, << or > / button on the right side of the **Go** button to access to the home/previous/next/end page.

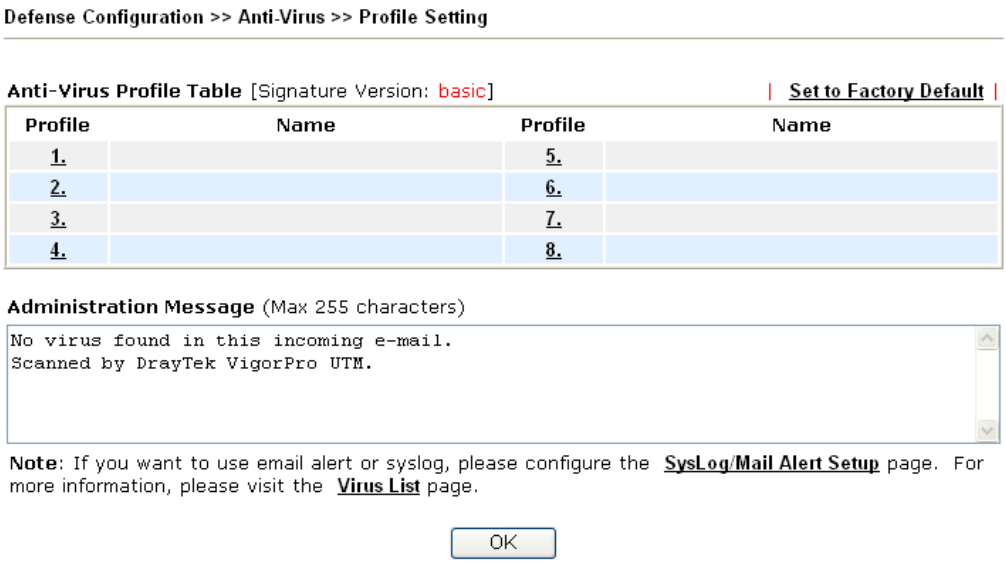
3.7.2 Anti-Virus

Vigor router can offer basic virus scanning, destroying and cut off the connection between questionable link and your computer for the files transmitted through specified protocol. In addition, several types of compressed file formats such as .zip, .gzip, .bzip2 are supported and can be scanned with this router. There is no limitation in the file size for the transmitted (incoming or outgoing) file. With this feature, all the files processed with the protocol specified in Anti-Virus web page will be scanned for finding out virus while passing through the router.

Note: Files with three-layer compression (the files are compressed with three times) also can be scanned by this router.

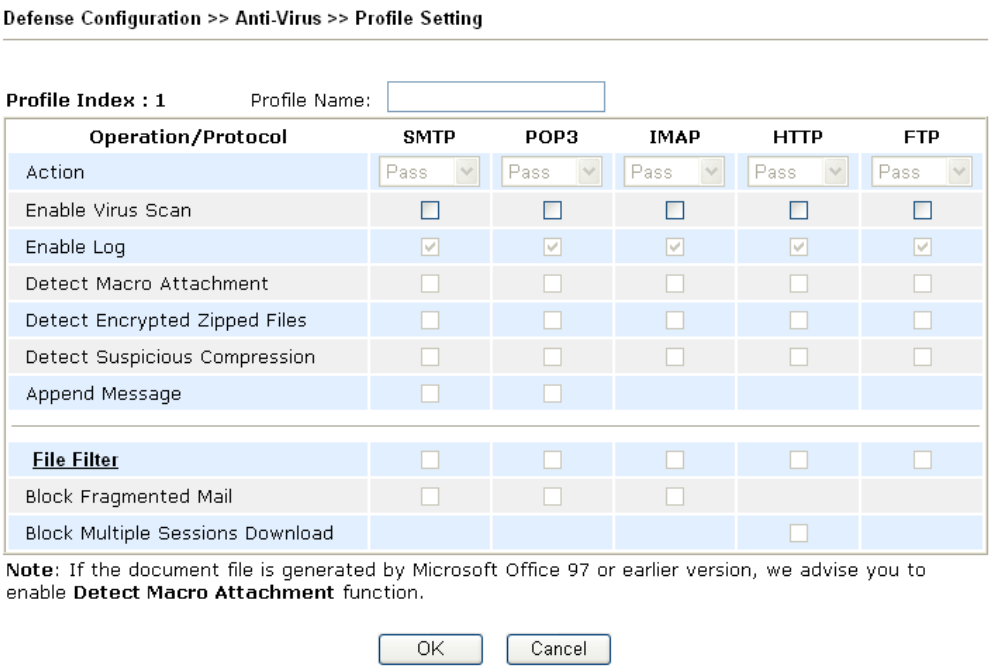
3.7.2.1 Profile Setting

This page allows you to set eight profiles for anti-virus scanning. These profiles can be invoked through firewall configuration. It is recommended to build one profile at least. Thus you will have selectable anti-virus profile setting in **Firewall->General Setup**.



The Administration Message box allows you to fill in important notification directly for SMTP and POP3 protocols. It will be saved as a file. While receiving an e-mail, the user will receive an attached file with the content listed in this box.

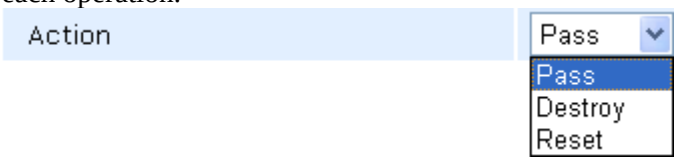
To edit a profile setting, please click the number link under Profile. You can see the following screen. You can check the boxes listed below for different operation respectively. If you uncheck this box, the corresponding settings for the protocol will not be performed.



Profile Name Type a name for the profile.

Protocol Currently, only the files transmitted through the protocols listed in this page including **SMTP**, **POP3**, **IMAP**, **HTTP** and **FTP** will be scanned by this router.

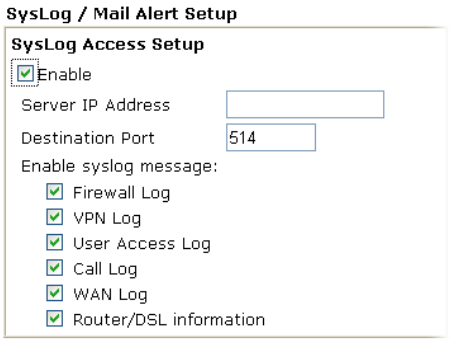
Action Choose the action that you want to apply to the protocols of each operation.



Pass - Detect if there is any virus for your reference. The system will not do any advanced action for such condition.
Destroy- Destroy the infected file found by the router system.
Reset - Break down the communication between your computer and specific link which might have virus included.

Enable Virus Scan Check this box to enable the general virus scan procedure for different protocols.

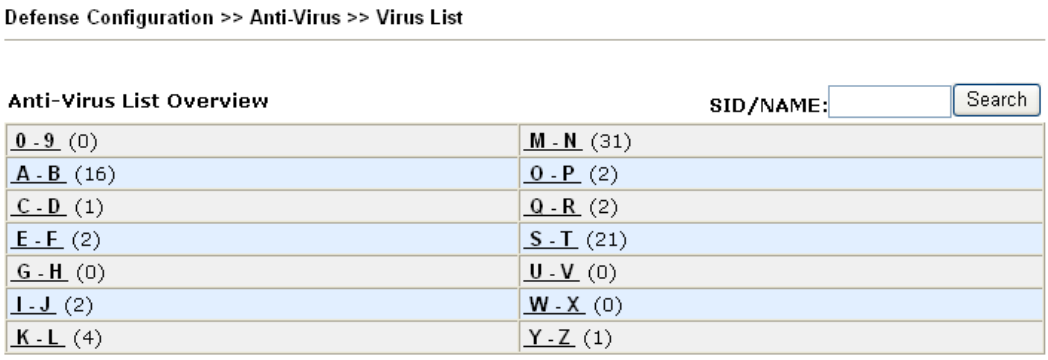
Enable Log In order to show the virus detection log on the window of Draytek Syslog, you have to check the log box here and enable the **SysLog Access Setup** from **System Maintenance >> Syslog/Mail Alert**.



Detect Macro Attachment	The file with macro attachment will be passed/destroyed/reset under different protocols. The system will detect it automatically if you set corresponding configuration here.
Detect Encrypted Zipped Files	The file zipped with encryption will be detected and then be passed/destroyed/reset according to the configuration set here.
Detect Suspicious Compression	The file with suspicious or non-support compression format will be detected and then be passed/destroyed/reset according to the configuration set here.
Append Message	This function is available for SMTP and POP3 protocols. If you check it, the message typed under the box of Administration Message will be sent out with e-mail.
File Filter	Click this link to open **Defense Configuration>>Anti-Virus >>File Pattern List** for viewing current settings.
Block Fragmented Mail	The file with fragmentations will be passed/destroyed/reset under different protocols. The router cannot execute the scanning job for some mail fragmentation if you check the boxes here.
Block Multiple Sessions Download	The file with multiple sessions which are created by **HTTP** will be detected and then be passed/destroyed/reset according to the configuration set here.

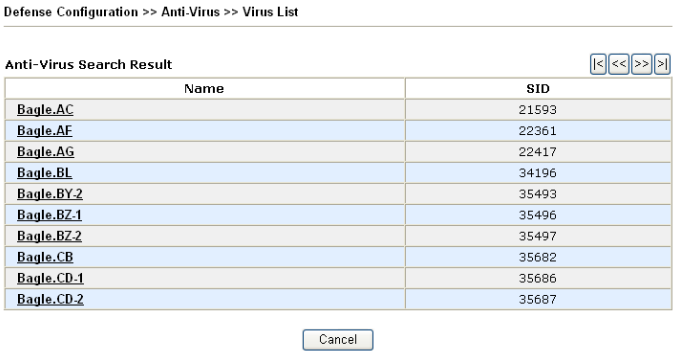
3.7.2.2 Virus List

This page displays the virus list ordered by digits (0-9) and letters (A-Z). Each number after the letter link indicates the total types of the virus collected.



SID/NAME To find the specific type of anti-virus, you can type its SID number or name in this field if you know, and then click **Search**. The system will locate that rule for you.

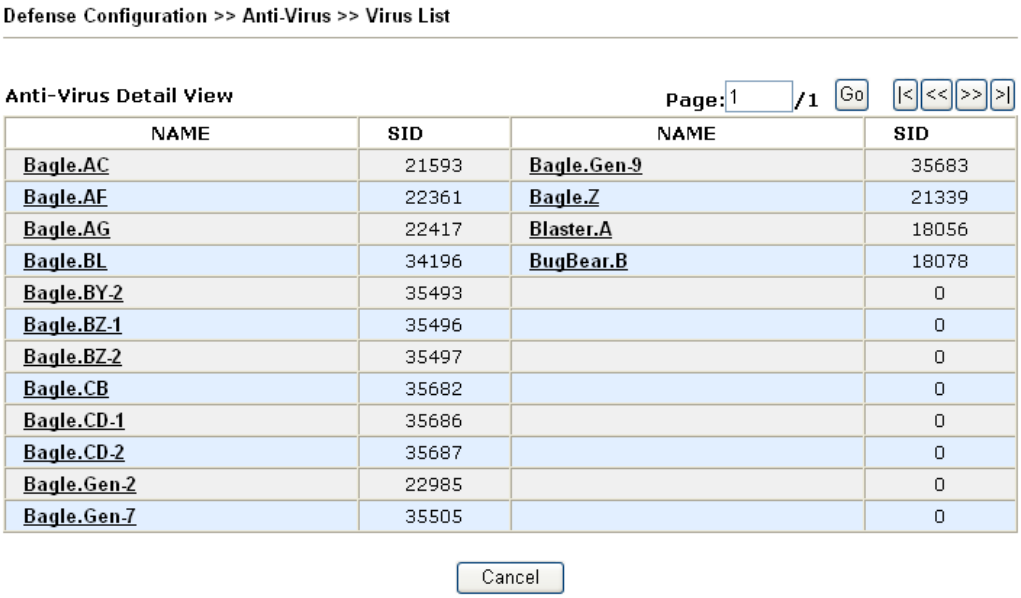
Search Click this button to find out all the virus rules related to the SID/NAME that you entered. The page of the searching result will be shown as the following picture.



Click each name link to check the detailed information of the anti-virus rule.

Detailed View for Anti-Virus

From the fourteen types of anti-virus list, click any one of them to access into next page. The detailed view list for anti-virus rule will be shown as below.



NAME A brief description name for the anti-virus rule is shown in this field. Click the name link to access into VigorPro website for checking the detailed information for the specified anti-virus.

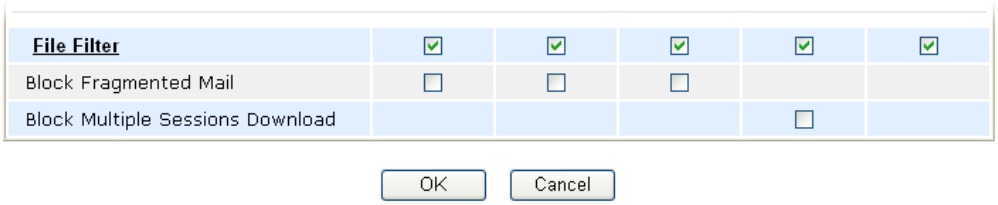
SID The number for each anti-virus rule is displayed in this field.

Page Type the page number in this field (if there is more than one page of anti-virus detail view displayed on this page). Then click **Go** to the specified page. Or you can click /**>, >>,** << or > / button on the right side of the Go button to access to the home/previous/next/end page.

3.7.2.3 File Pattern List

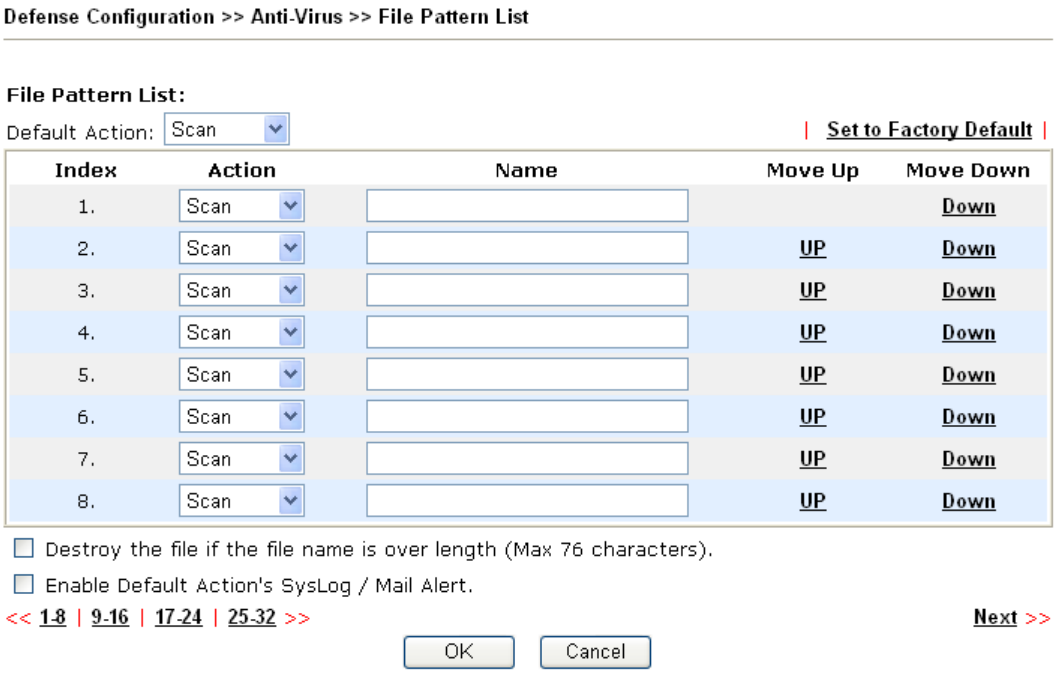
To avoid confidential file being leaked out by someone else through network and cause severe consequence, you can specify the file name in this page and determine to destroy or scan or pass it while the file passes through the router.

To activate the File Patter List, you have to set one Anti-Virus profile on **Defense Configuration>>Anti-Virus>>Profile Setting**. Also you can specify file names without virus appended to be ignored by anti-virus server to improve the performance.



This page allows you to set 32 entries (rules) of file names to be filtered by the router. In such case, the file format is ignored. The router will destroy, scan or non-scan the specified filename according to the configuration that you set here.

Below is the page of **File Pattern List**. The priority of each entry is determined by the index number. That is, the entry of Index 1 has the highest priority in file name filtering; the entry of Index 32 has the lowest priority in filtering.



Default Action — Choose one of the actions (Scan, Non-Scan, Destroy) as the default action if the filename for one file does not meet the conditions configured in these thirty-two entries.

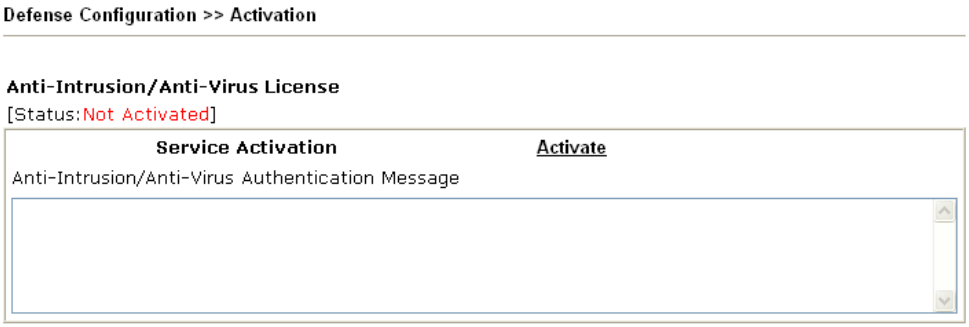
Action — Choose the action that you want to apply to the protocols of each operation.
Destroy- Destroy the file with name specified here which is found by the router system.
Non-Scan –The file will not be scanned and will not be processed by using general rules set in Anti-Virus profile.
Scan – Just scan the file with name specified here which is

	found by the router system, and be processed by using general rules set in Anti-Virus profile.
Name	Enter the keyword of the file that you want to filter. The maximum character is 30. And the name is case-sensitive.
Move Up/Down	Press **OK** to ensure the name you typed and then use **Up** or **Down** link to move the order of the file pattern entry.
Destroy the file if the file name is over length	Check this box to destroy the file with filename over 76 characters.
Enable Syslog/Mail Alert for Default Action	Check this box to have Syslog/Mail Alert list the information for default action.

Click **OK** to finish the page configuration.

3.7.3 Activation for Anti-Intrusion/Anti-Virus Service

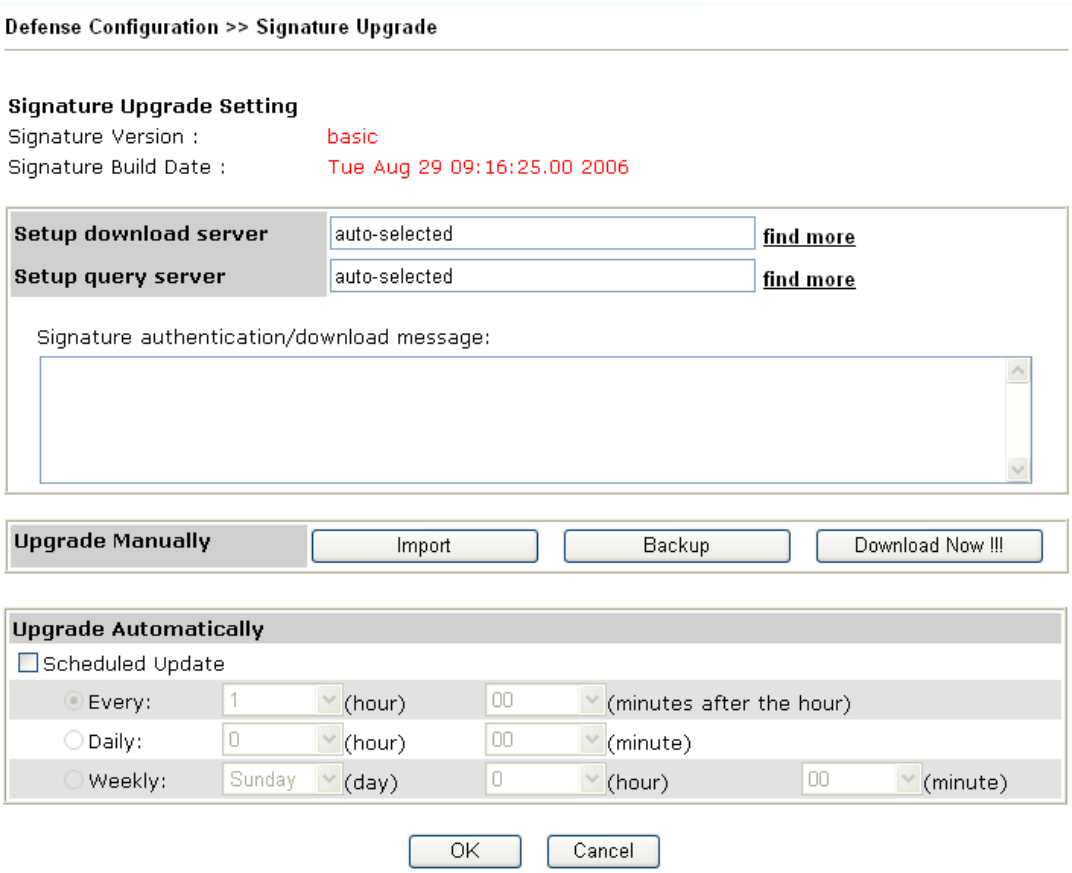
After you have finished the profile settings, it is the time to activate the mechanism for your computer. Click **Defense Configuration>>Activation** to open the following page for accessing www.vigorpro.com.



Service Activation	The **Activate** link brings you accessing into www.vigorpro.com to finish the activation of the account and the router.
Anti-Intrusion/Anti-Virus Authentication Message	As for authentication information of **Anti-Intrusion/Anti-Virus**, the process of authenticating will be displayed on this field for your reference.

3.7.4 Signature Upgrade

You can get the most updated signature from DrayTek's server if the license key of anti-virus/anti-intrusion for the VigorPro 5510 is not expired. Before you upgrade the signature, please check the validation information either from WEB user interface of VigorPro 5510 or account information from www.vigorpro.com.



Signature Upgrade Setting

It displays the signature version for your reference. There are three levels for the signature:
basic – If you did not register and activate your account, you can just own the default 200 (or more) anti-intrusion and anti-virus rules for your router.

DT-DT/DT-KL_XXXXXX – If you have registered and activated your AI/AV account, and downloaded the newest rules from www.vigorpro.com, you can see DT-DT/DT-KL in this field that means you have obtained the latest signature information.

Setup download server/Setup query server

The default setting is auto-selected. You can change the setting if it is required to be. Click the **find more** link to get more information.

Please choose a download server / query server of the continent that your router is located.

Zone Name	Download Server	Query Server
Africa	www.vigorpro.com	www.vigorpro.com
America	www.vigorpro.com	www.vigorpro.com
Asia	www.vigorpro.com	www.vigorpro.com
Europe	www.vigorpro.com	www.vigorpro.com
Oceania	www.vigorpro.com	www.vigorpro.com
The Antarctic	www.vigorpro.com	www.vigorpro.com

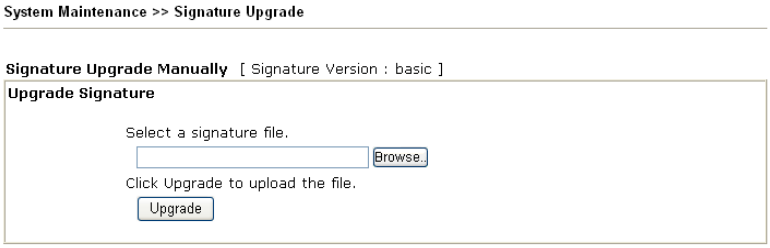
Signature authentication/download message

It displays the message of signature authentication or download procedure.

Upgrade Manually

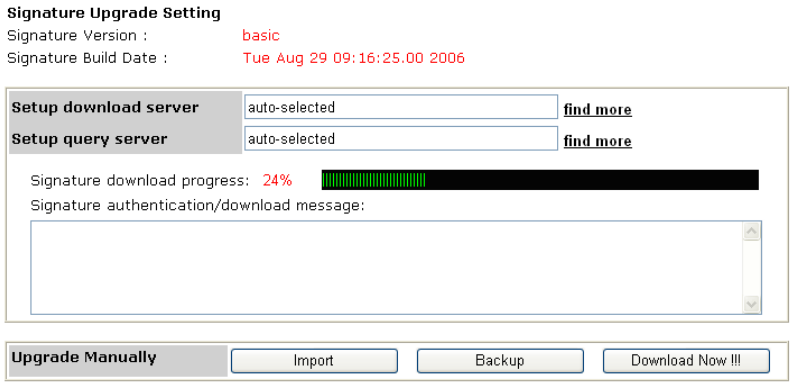
The buttons in this field are only available when you finished the registration and activation for new account and your router. If not, these buttons do not have any effect even if you click them.

Import – You can import a saved file to manually upgrade the signature. Click **Browse** to choose the right file with **.sig** file format. Next, click **Upgrade**.

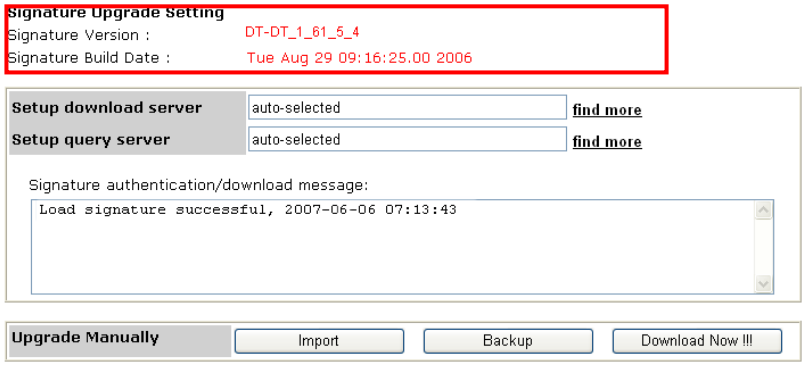


Backup - You can backup current signature information with the filename vigorpro.sig.

Download Now!!! – This button will download newly update anti-intrusion and anti-virus from VigorPro website. While downloading the file, a progress bar will be shown as follows.



After downloading is finished, the signature version will be upgraded and displayed on the web page.



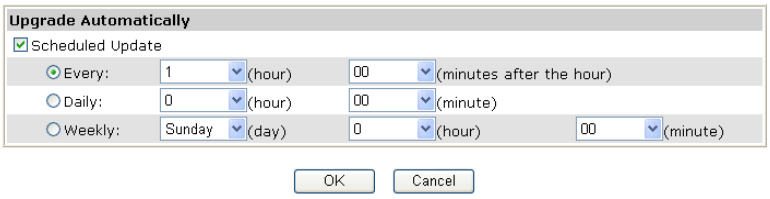
Upgrade Automatically

Specify certain time for executing the upgrade automatically. Remember to check the **Schedule Update** box to activate the time settings.

Every – It means the downloading procedure will be executed automatically whenever passing through the time (hours and minutes) that you set here.

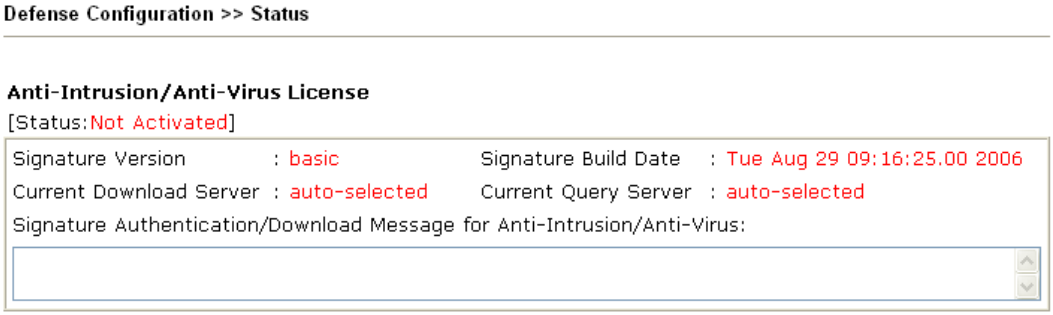
Daily - It means the downloading procedure will be automatically executed every day at the time (hours and minutes) that you set

here.
Weekly - It means the downloading procedure will be automatically executed at the time (hours and minutes) that you set here every week.



3.7.5 Status

This field will shows the status for the license, start date and expire date for Anti-Intrusion/Anti-Virus service. If your account or router is still not activated, the word **Not Activated** will be displayed here to inform you. Below is a sample page with valid license.



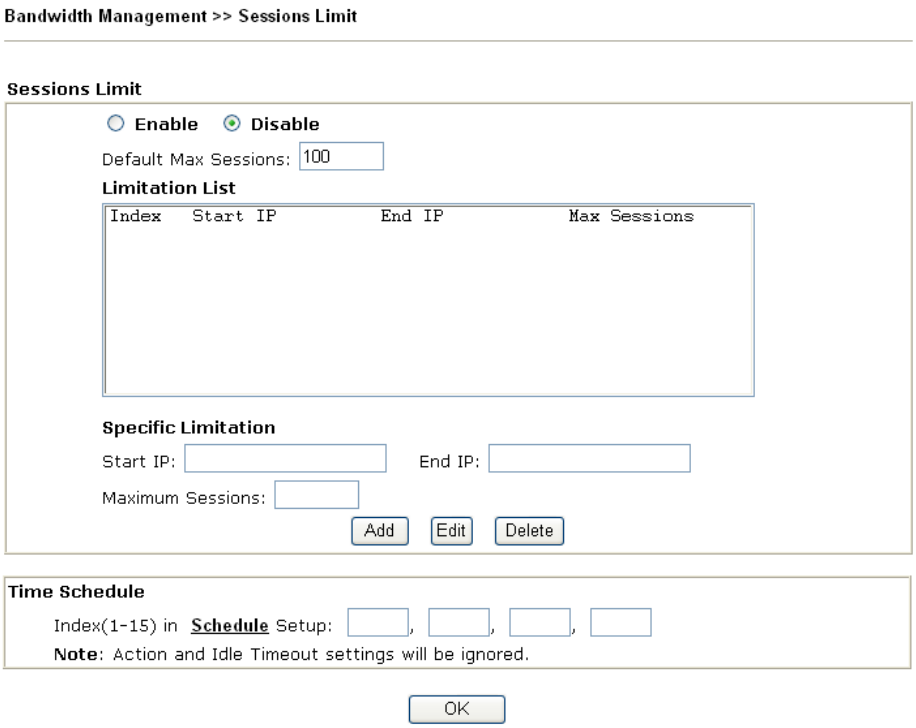
3.8 Bandwidth Management

Below shows the menu items for Bandwidth Management.

3.8.1 Sessions 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.

In the **Bandwidth Management** menu, click **Sessions Limit** to open the web page.



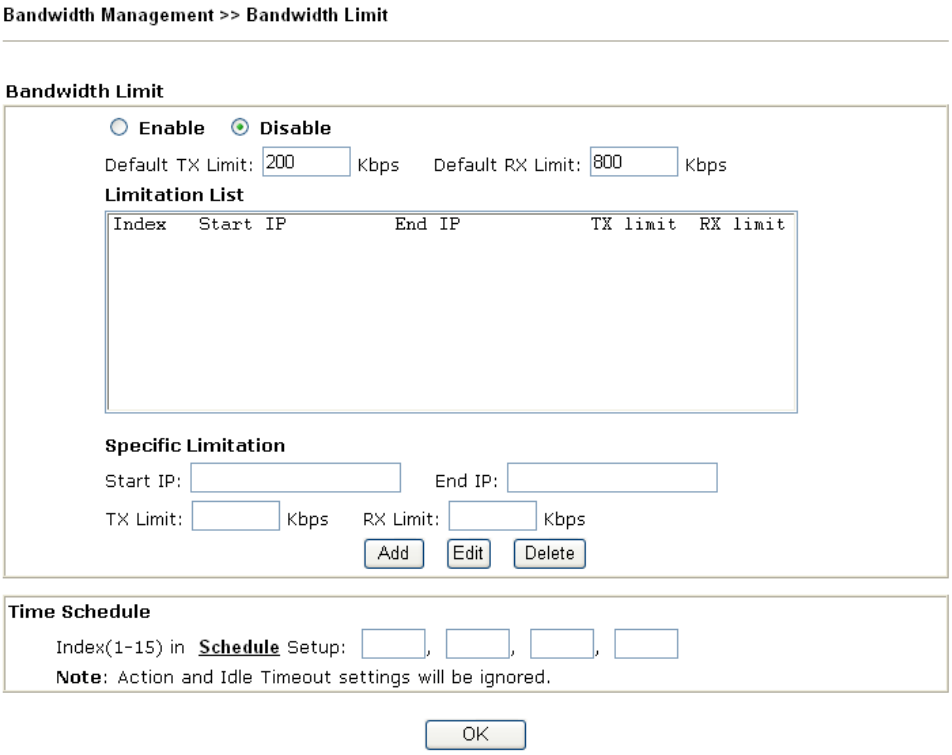
To activate the function of limit session, simply click **Enable** and set the default session limit.

Enable	Click this button to activate the function of limit session.
Disable	Click this button to close 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.
Start IP	Defines the start IP address for limit session.
End IP	Defines the end IP address for limit session.
Maximum Number	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	Delete the selected settings existing on the limitation list.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application – Schedule** web page and you can use the number that you have set in that web page.

3.8.2 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.

In the **Bandwidth Management** menu, click **Bandwidth Limit** to open the web page.



To activate the function of limit bandwidth, simply click **Enable** and set the default upstream and downstream limit.

Enable	Click this button to activate the function of limit bandwidth.
Disable	Click this button to close 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.
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	Allows you to edit the settings for the selected limitation.
Delete	Delete the selected settings existing on the limitation list.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application – Schedule** web page and you can use the number that you

have set in that web page.

3.8.3 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.

One reason for QoS is that numerous TCP-based applications tend to continually increase their transmission rate and consume all available bandwidth, which is called TCP slow start. If other applications are not protected by QoS, it will detract much from their performance in the overcrowded network. This is especially essential to those are low tolerant of loss, delay or jitter (delay variation).

Another reason is due to congestions at network intersections where speeds of interconnected circuits mismatch or traffic aggregates, packets will queue up and traffic can be throttled back to a lower speed. If there's no defined priority to specify which packets should be discarded (or in another term "dropped") from an overflowing queue, packets of sensitive applications mentioned above might be the ones to drop off. How this will affect application performance?

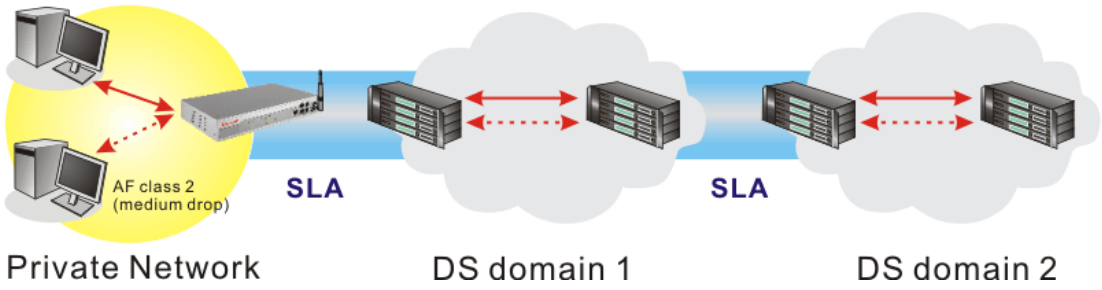
There are two components within Primary configuration of QoS deployment:

- Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- Scheduling: Based on classification of service level to assign packets to queues and associated service types

The basic QoS implementation in Vigor routers is to classify and schedule packets based on the service type information in the IP header. For instance, to ensure the connection with the headquarter, a teleworker may enforce an index of QoS Control to reserve bandwidth for HTTPS connection while using lots of application at the same time.

One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes possible with backward IP Precedence compatibility. In a QoS-enabled network, or Differentiated Service (DiffServ or DS) framework, a DS domain owner should sign a Service License Agreement (SLA) with other DS domain owners to define the service level provided toward traffic from different domains. Then each DS node in these domains will perform the priority treatment. This is called per-hop-behavior (PHB). The definition of PHB includes Expedited Forwarding (EF), Assured Forwarding (AF), and Best Effort (BE). AF defines the four classes of delivery (or forwarding) classes and three levels of drop precedence in each class.

Vigor routers as edge routers of DS domain shall check the marked DSCP value in the IP header of bypassing traffic, thus to allocate certain amount of resource execute appropriate policing, classification or scheduling. The core routers in the backbone will do the same checking before executing treatments in order to ensure service-level consistency throughout the whole QoS-enabled network.



However, each node may take different attitude toward packets with high priority marking since it may bind with the business deal of SLA among different DS domain owners. It's not easy to achieve deterministic and consistent high-priority QoS traffic throughout the whole network with merely Vigor router's effort.

In the **Bandwidth Management** menu, click **Quality of Service** to open the web page.

Bandwidth Management >> Quality of Service

General Setup

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup

Class Rule

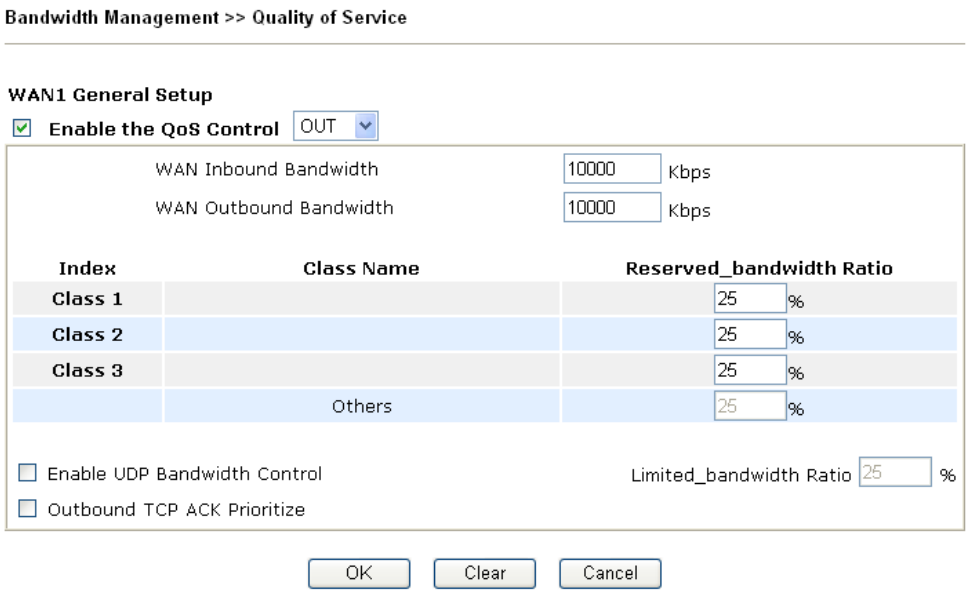
Index	Name	Rule	Service Type
Class 1		Edit	
Class 2		Edit	Edit
Class 3		Edit	

This page displays the QoS settings result of the WAN interface. Click the **Setup** link to access into next page for the general setup of WAN (1/2) interface. As to class rule, simply click the **Edit** link to access into next for configuration.

You can configure general setup for the WAN interface, edit the Class Rule, and edit the Service Type for the Class Rule for your request.

General Setup for WAN Interface

When you click **Setup**, you can configure the bandwidth ratio for QoS of the WAN interface. There are four queues allowed for QoS control. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. Yet, the last one is reserved for the packets which are not suitable for the user-defined class rules.



Enable the QoS Control The factory default for this setting is checked.
Please also define which traffic the QoS Control settings will apply to.
IN- apply to incoming traffic only.
OUT-apply to outgoing traffic only.
BOTH- apply to both incoming and outgoing traffic.
Check this box and click **OK**, then click **Setup** link again. You will see the **Online Statistics** link appearing on this page.

WAN Inbound Bandwidth It allows you to set the connecting rate of data input for WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 10000kbps for this box. The default value is 10000kbps.

WAN Outbound Bandwidth It allows you to set the connecting rate of data output for WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 256kbps for this box. The default value is 10000kbps.

Reserved Bandwidth Ratio It is reserved for the group index in the form of ratio of **reserved bandwidth to upstream speed** and **reserved bandwidth to downstream speed**.

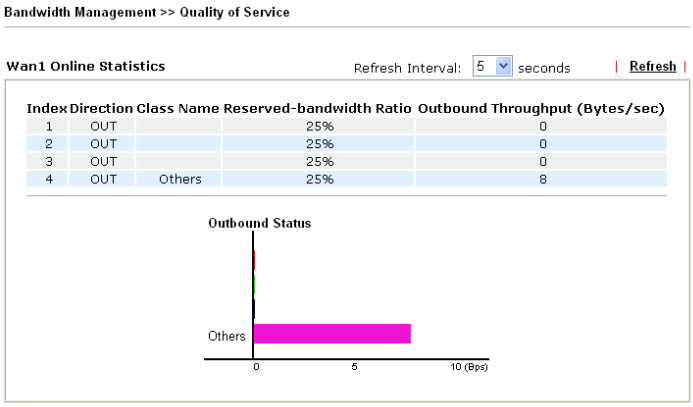
Enable UDP Bandwidth Control Check this and set the limited bandwidth ratio on the right field. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth.

Outbound TCP ACK Prioritize The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload faster to speed the network traffic.

Limited_bandwidth Ratio The ratio typed here is reserved for limited bandwidth of UDP application.

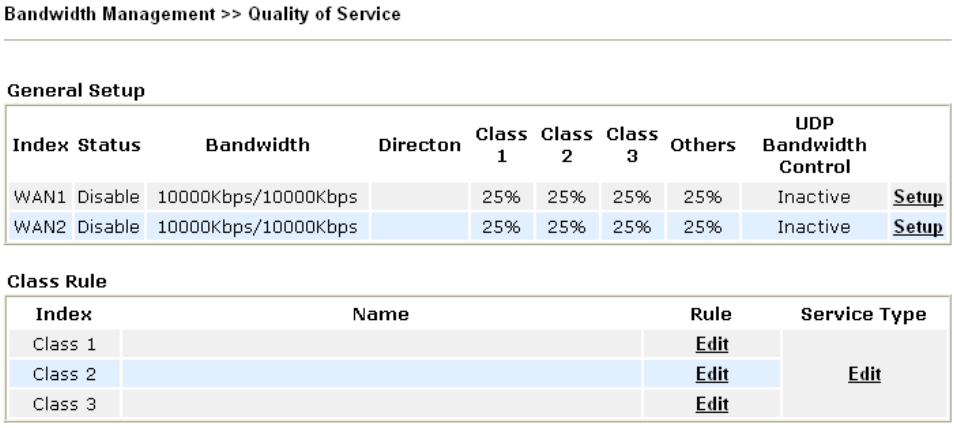
Online Statistics Display an online statistics for quality of service for your reference. This link will be seen only if you click **OK** in WAN1/WAN2 General Setup web page and click Setup again

(for WAN1/WAN2) on the **Bandwith Management>>Quality of Service**.

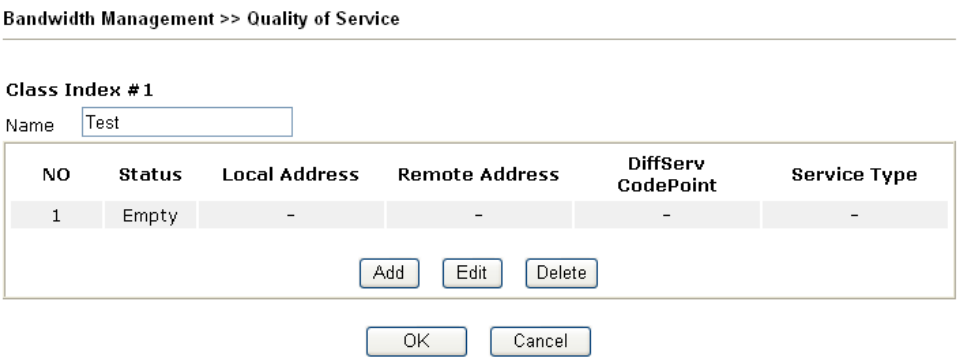


Edit the Class Rule for QoS

The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. To add, edit or delete the class rule, please click the **Edit** link of that one.



After you click the **Edit** link, you will see the following page. Now you can define the name for that Class. In this case, “Test” is used as the name of Class Index #1.



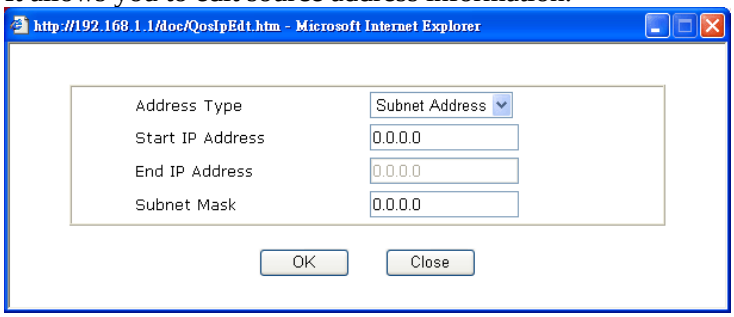
For adding a new rule, click **Add** to open the following page.

ACT — Check this box to invoke these settings.

Local Address — Click the **Edit** button to set the local IP address (on LAN) for the rule.

Remote Address — Click the **Edit** button to set the remote IP address (on Lan/WAN) for the rule.

Edit — It allows you to edit source address information.

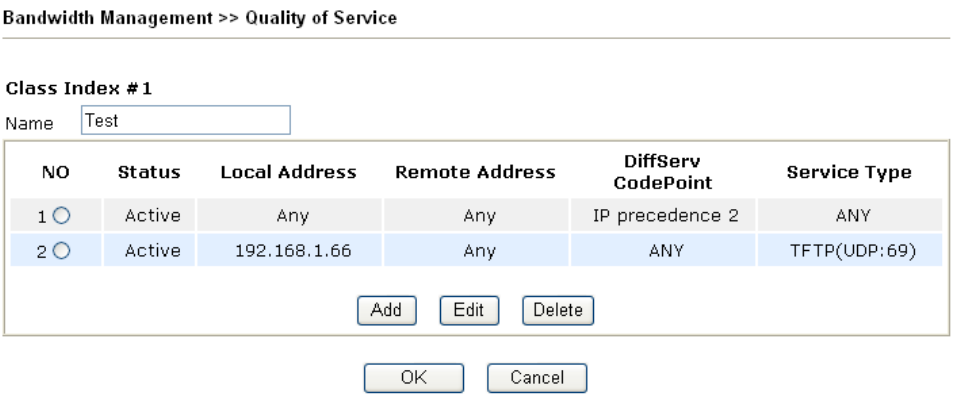


Address Type – Determine the address type for the source address.
For **Single Address**, you have to fill in Start IP address.
For **Range Address**, you have to fill in Start IP address and End IP address.
For **Subnet Address**, you have to fill in Start IP address and Subnet Mask.

DiffServ CodePoint — All the packets of data will be divided with different levels and will be processed according to the level type by the system. Please assign one of the level of the data for processing with QoS control.

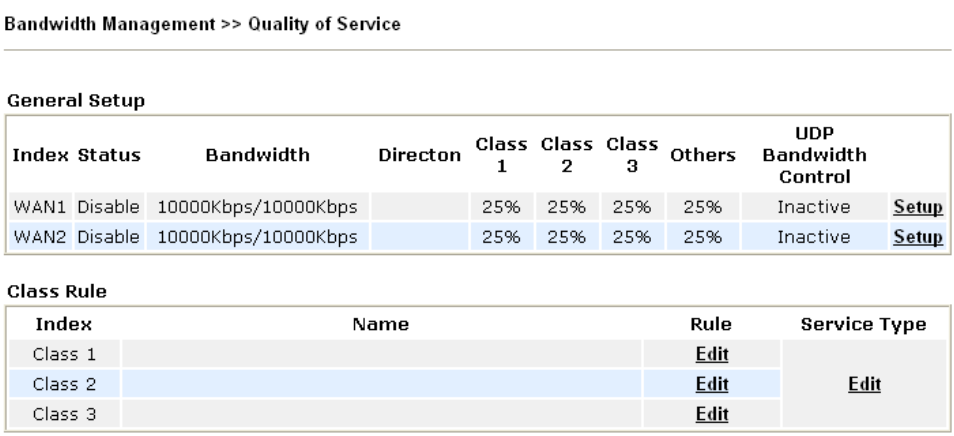
Service Type — It determines the service type of the data for processing with QoS control. It can also be edited. You can choose the predefined service type from the Service Type drop down list. Those types are predefined in factory. Simply choose the one that you want for using by current QoS.

By the way, you can set up to 20 rules for one Class. If you want to edit an existed rule, please select the radio button of that one and click **Edit** to open the rule edit page for modification.

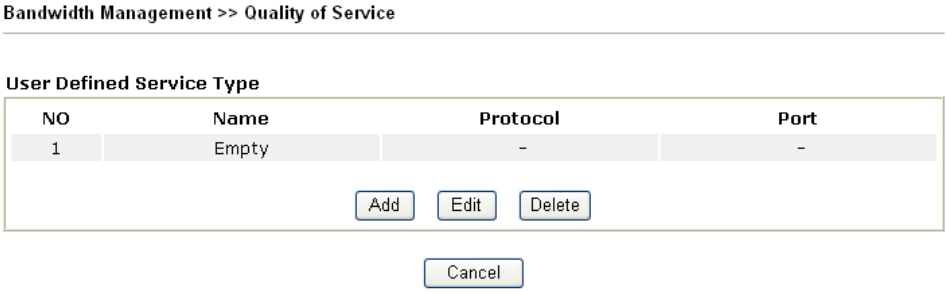


Edit the Service Type for Class Rule

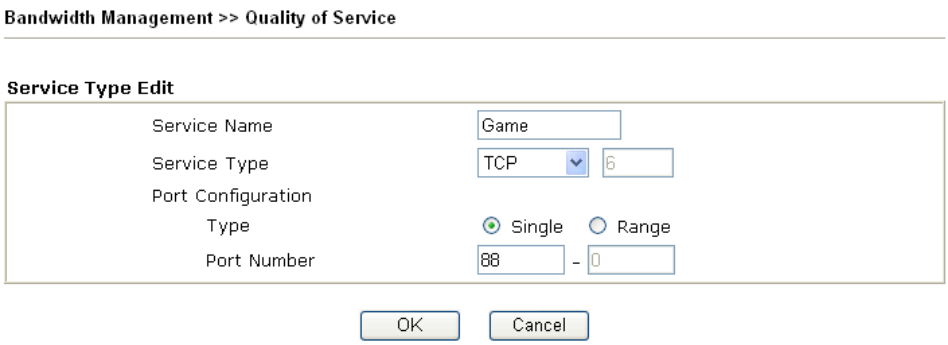
To add a new service type, edit or delete an existed service type, please click the Edit link under Service Type field.



After you click the **Edit** link, you will see the following page.



For adding a new service type, click **Add** to open the following page.



Service Name Type in a new service for your request.

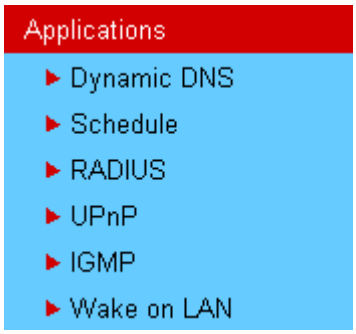
Service Type Choose the type (TCP, UDP or TCP/UDP) for the new service.

Port Configuration Click **Single** or **Range**. If you select Range, you have to type in the starting port number and the end porting number on the boxes below.
Port Number – Type in the starting port number and the end porting number here if you choose Range as the type.

By the way, you can set up to 40 service types. If you want to edit/delete an existed service type, please select the radio button of that one and click **Edit/Edit** for modification.

3.9 Applications

Below shows the menu items for Applications.



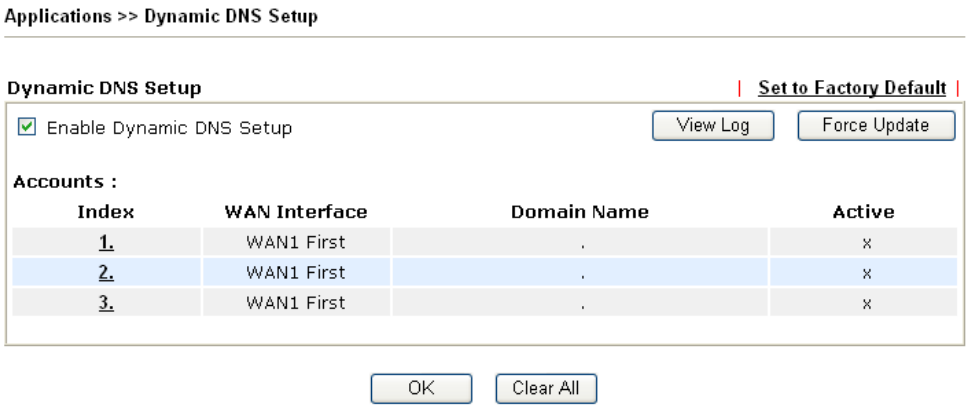
3.9.1 Dynamic DNS

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.

Enable the Function and Add a Dynamic DNS Account

1. Assume you have a registered domain name from the DDNS provider, say *hostname.dyndns.org*, and an account with username: *test* and password: *test*.
2. In the DDNS setup menu, check **Enable Dynamic DNS Setup**.



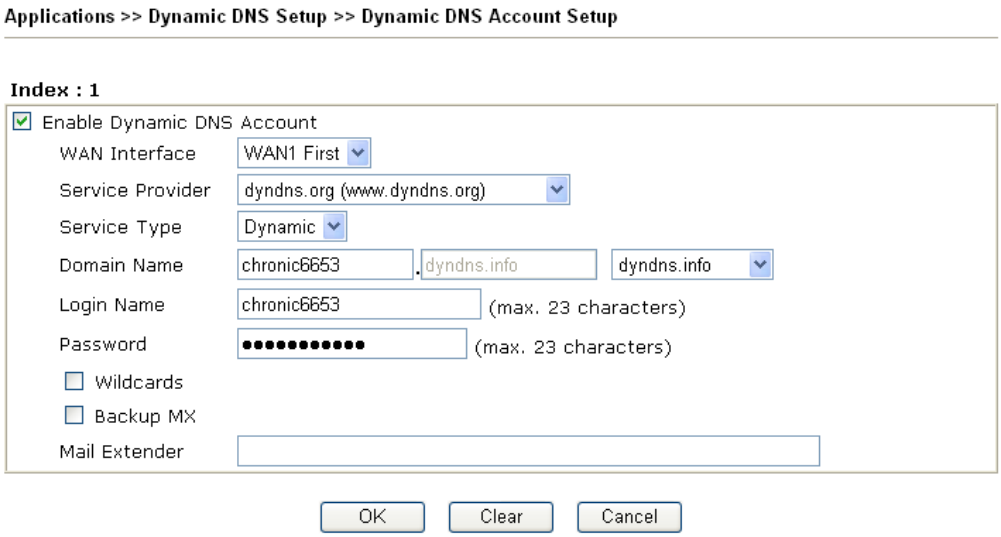
Set to Factory Default Clear all profiles and recover to factory settings.

Enable Dynamic DNS Setup Check this box to enable DDNS function.

Index Click the number below Index to access into the setting page of DDNS setup to set account(s).

WAN Interface	Display current WAN interface used for accessing Internet.
Domain Name	Display the domain name that you set on the setting page of DDNS setup.
Active	Display if this account is active or inactive.
View Log	Display DDNS log status.
Force Update	Force the router updates its information to DDNS server.

3. Select Index number 1 to add an account for the router. Check **Enable Dynamic DNS Account**, and choose correct Service Provider: dyndns.org, type the registered hostname: *hostname* and domain name suffix: dyndns.org in the **Domain Name** block. The following two blocks should be typed your account Login Name: *test* and Password: *test*.



Enable Dynamic DNS Account	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).
WAN Interface	Select the WAN interface order to apply settings here.
Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom, Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.
Domain Name	Type in the domain name that you applied previously. Use the drop down list to choose the desired domain.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.
Wildcards	It is not supported for all Dynamic DNS providers. Please get more detailed information from its website.
Backup MX	It is not supported for all Dynamic DNS providers. Please get more detailed information from its website.
Mail Extender	It allows you to control the delivery of mails for a given *domain* or *subdomain*. The entry you type here can be specified as a secondary mail exchanger. It means that

delivery will be attempted to your host first, and then to the host you specify here if that fails.

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

The Wildcard and Backup MX features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.

Disable the Function and Clear all Dynamic DNS Accounts

In the DDNS setup menu, uncheck **Enable Dynamic DNS Setup**, and push **Clear All** button to disable the function and clear all accounts from the router.

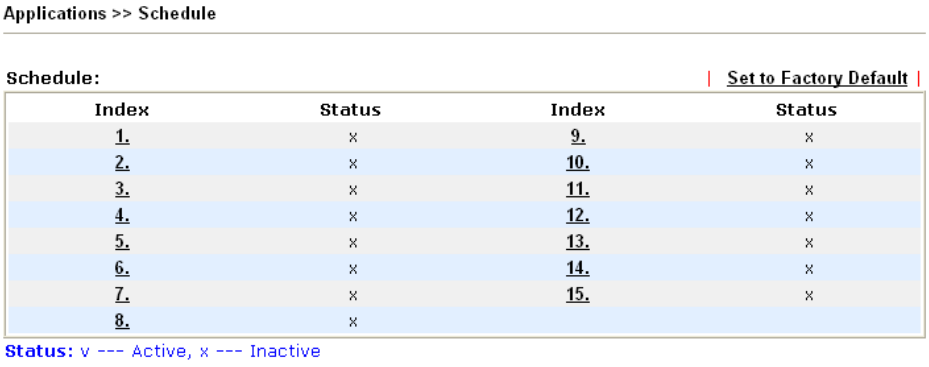
Delete a Dynamic DNS Account

In the DDNS setup menu, click the **Index** number you want to delete and then push **Clear All** button to delete the account.

3.9.2 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.



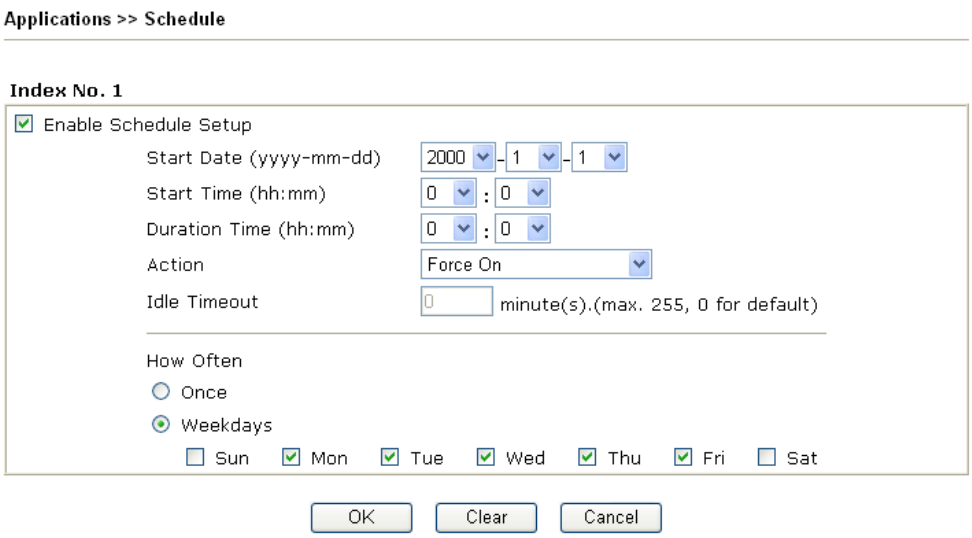
Set to Factory Default Clear all profiles and recover to factory settings.

Index Click the number below Index to access into the setting page of schedule.

Status Display if this schedule setting is active or inactive.

You can set up to 15 schedules. Then you can apply them to your **Internet Access** or **VPN and Remote Access >> LAN-to-LAN** settings.

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.



Enable Schedule Setup	Check to enable the schedule.
Start Date (yyyy-mm-dd)	Specify the starting date of the schedule.
Start Time (hh:mm)	Specify the starting time of the schedule.
Duration Time (hh:mm)	Specify the duration (or period) for the schedule.
Action	Specify which action Call Schedule should apply during the period of the schedule. **Force On -**Force the connection to be always on. **Force Down -**Force the connection to be always down. **Enable Dial-On-Demand -**Specify the connection to be dial-on-demand and the value of idle timeout should be specified in **Idle Timeout** field. **Disable Dial-On-Demand -**Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.
Idle Timeout	Specify the duration (or period) for the schedule. **How often -**Specify how often the schedule will be applied **Once -**The schedule will be applied just once **Weekdays -**Specify which days in one week should perform the schedule.

Example

Suppose you want to control the PPPoE Internet access connection to be always on (Force On) from 9:00 to 18:00 for whole week. Other time the Internet access connection should be disconnected (Force Down).

Office Hour:

(Force On)

Mon - Sun **9:00 am** **to** **6:00 pm**

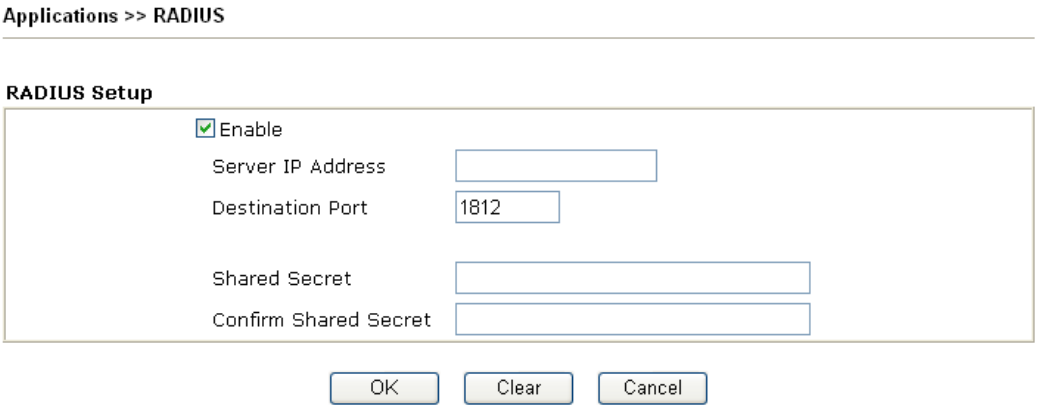
1. Make sure the PPPoE connection and **Time Setup** is working properly.
2. Configure the PPPoE always on from 9:00 to 18:00 for whole week.

3. Configure the **Force Down** from 18:00 to next day 9:00 for whole week.
4. Assign these two profiles to the PPPoE Internet access profile. Now, the PPPoE Internet connection will follow the schedule order to perform **Force On** or **Force Down** action according to the time plan that has been pre-defined in the schedule profiles.

3.9.3 RADIUS

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.

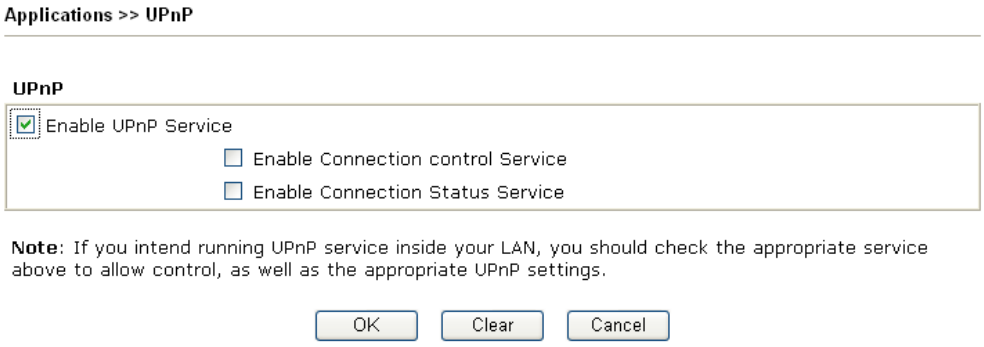
The built-in RADIUS client feature enables the router to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.



Enable	Check to enable RADIUS client feature
Server IP Address	Enter the IP address of RADIUS server
Destination 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.
Confirm Shared Secret	Re-type the Shared Secret for confirmation.

3.9.4 UPnP

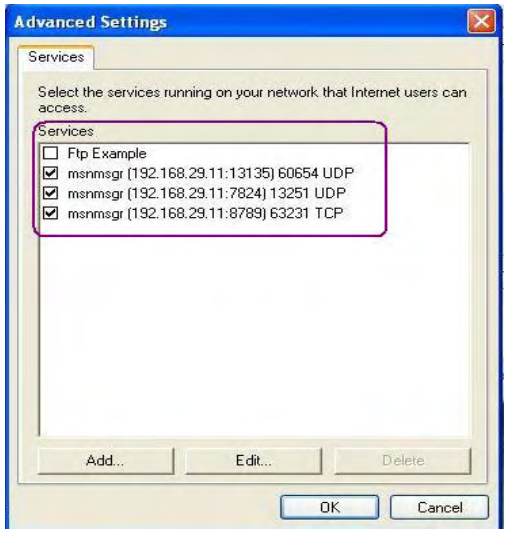
The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on 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 provides the associated support for MSN Messenger to allow full use of the voice, video and messaging features.



Enable UPNP Service Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

After setting **Enable UPNP Service** 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

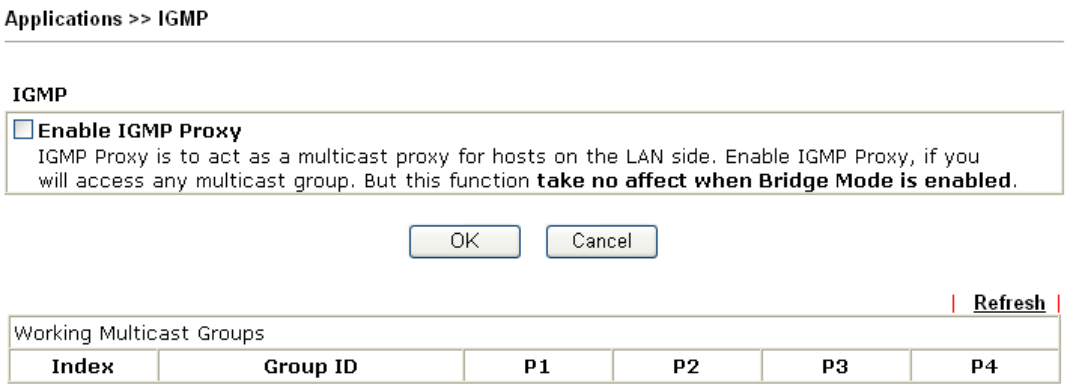
Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

- 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.

3.9.5 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. For invoking IGMP Snooping function, you have to check the Enable IGMP Proxy box first for activating the IGMP proxy function.



Enable IGMP Proxy Check this box to enable this function. The application of multicast will be executed through WAN port.

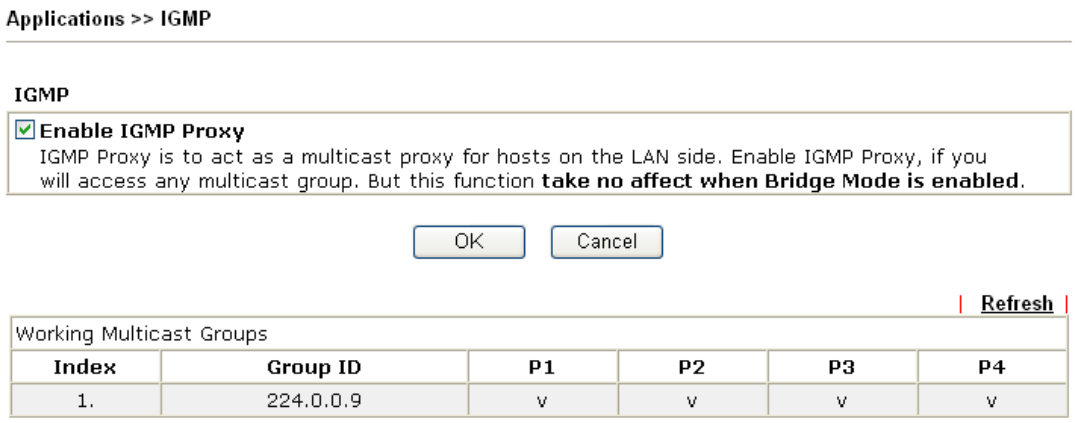
Enable IGMP Snooping Check this box to enable this function. The application of multicast will be executed for the clients in LAN.

Group ID This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.

P1 to P4 It indicates the LAN port used for the multicast group.

Refresh Click this link to renew the working multicast group status.

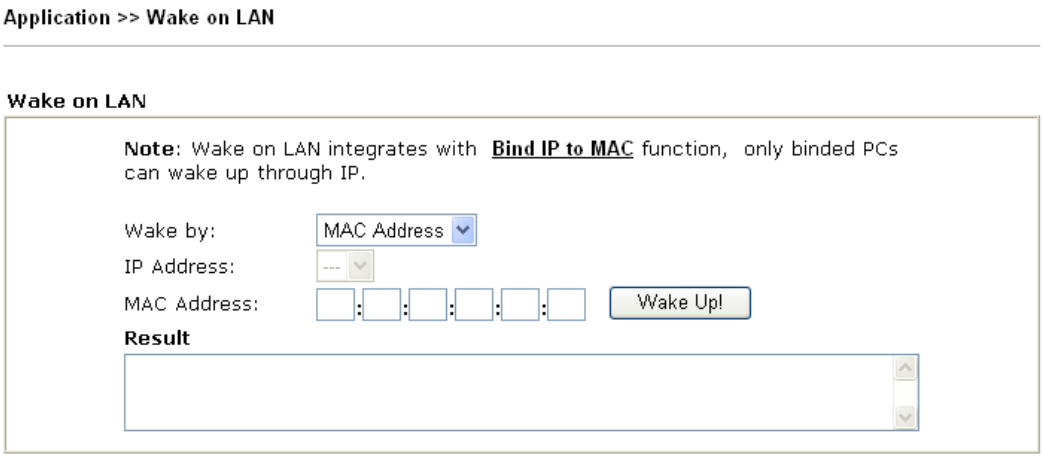
If you check Enable IGMP Proxy, you will get the following page. All the multicast groups will be listed and all the LAN ports (P1 to P4) are available for use.



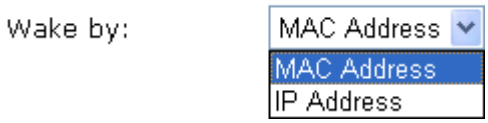
3.9.6 Wake On LAN

A PC client on LAN can be woken up by the router it connects. When a user wants to wake up a specified PC through the router, he/she must type correct MAC address of the specified PC on this web page of **Wake On LAN** of this router.

In addition, such PC must have installed a network card supporting WOL function. By the way, WOL function must be set as “Enable” on the BIOS setting.



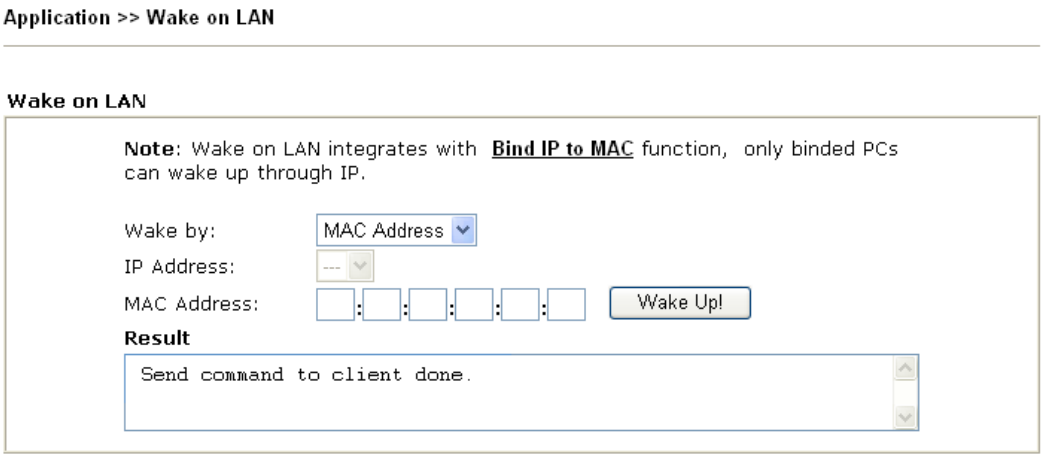
Wake by Two types provide for you to wake up the binded IP. If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the correct IP address.



IP Address The IP addresses that have been configured in **LAN>>Bind IP to MAC** will be shown in this drop down list. Choose the IP address from the drop down list that you want to wake up.

MAC Address Type any one of the MAC address of the binded PCs.

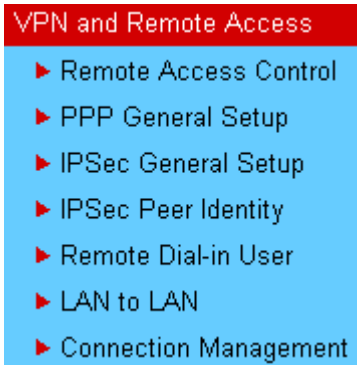
Wake Up Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.



3.10 VPN and Remote Access

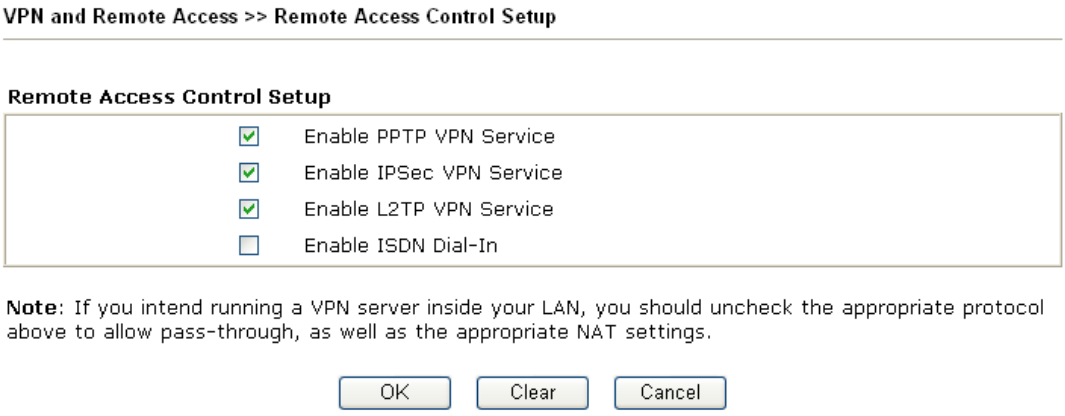
A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point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

Below shows the menu items for VPN and Remote Access.



3.10.1 Remote Access Control

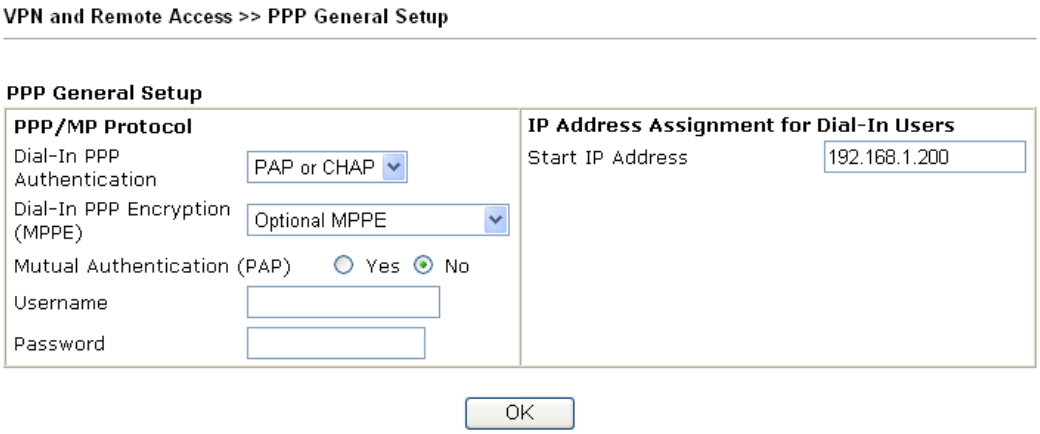
Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port.



The Vigor router will not accept the ISDN dial-in connection if the box of **Enable ISDN Dial-in** is not checked.

3.10.2 PPP General Setup

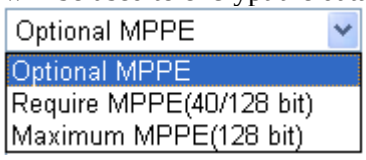
This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPSec.



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 Optional 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.

Mutual Authentication (PAP)
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.

Start IP Address
Enter a start IP address 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. But, you have to notice that the first two IP addresses of 192.168.1.200 and 192.168.1.201 are reserved for ISDN remote dial-in user.

3.10.3 IPSec General Setup

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

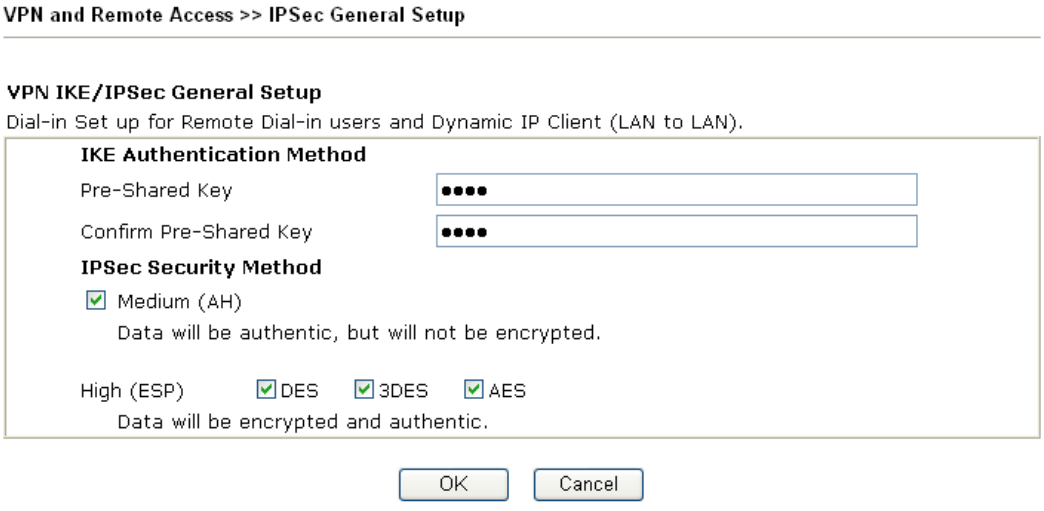
There are two phases of IPSec.

- 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 either a Pre-Shared Key or Digital Signature (x.509). 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.



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 -Currently only support Pre-Shared Key authentication.

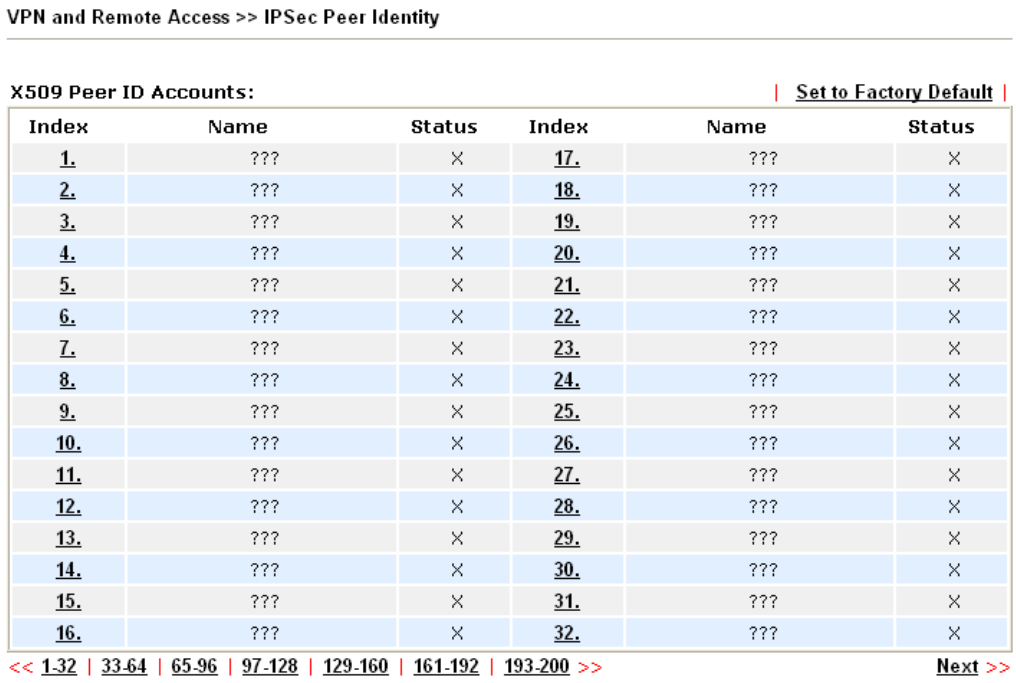
Pre-Shared Key- Specify a key for IKE authentication
Confirm Pre-Shared Key-Confirm the pre-shared key.

IPSec Security Method

Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
High - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

3.10.4 IPSec Peer Identity

To use digital certificate for peer authentication in either LAN-to-LAN connection or Remote User Dial-In connection, here you may edit a table of peer certificate for selection. As shown below, the router provides **200** entries of digital certificates for peer dial-in users.

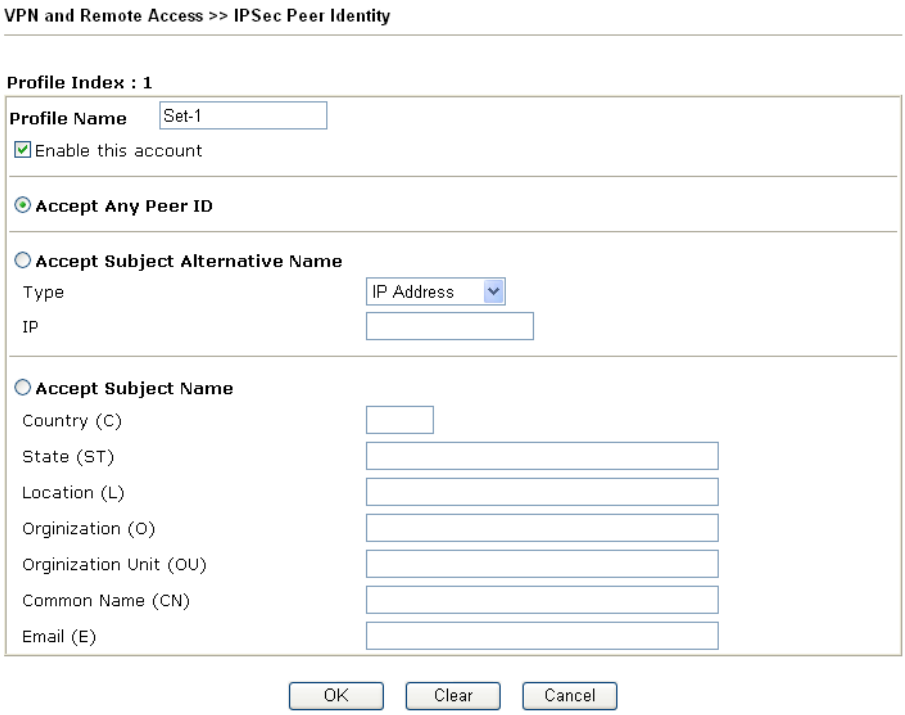


Set to Factory Default Click it to clear all indexes.

Index Click the number below Index to access into the setting page of IPSec Peer Identity.

Name Display the profile name of that index.

Click each index to edit one peer digital certificate. There are three security levels of digital signature authentication: Fill each necessary field to authenticate the remote peer. The following explanation will guide you to fill all the necessary fields.

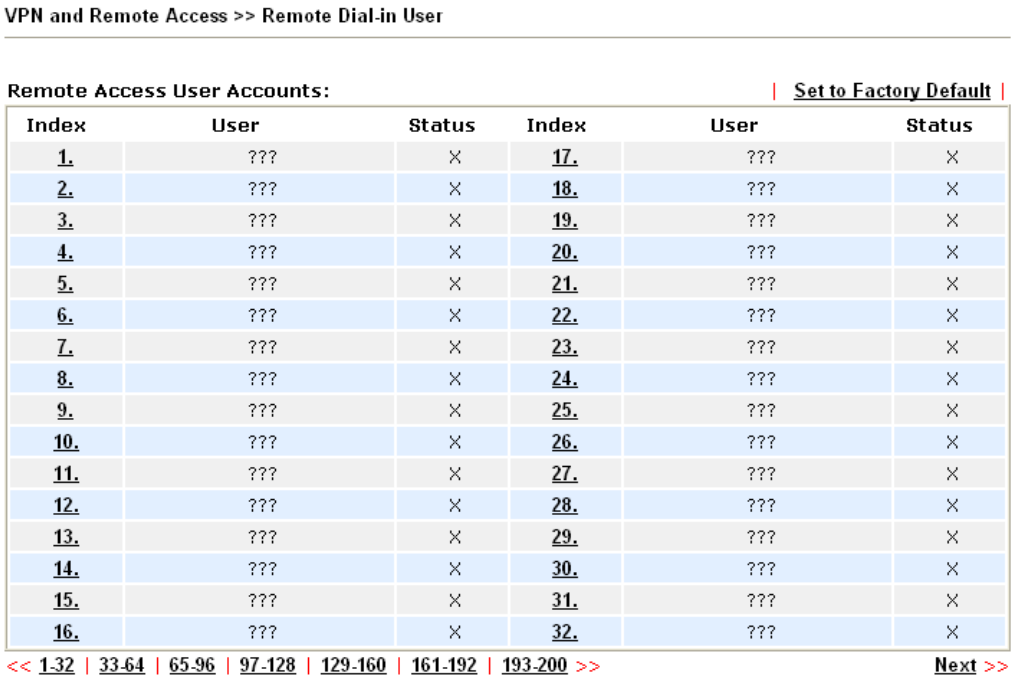


Profile Name	Type in a name in this file.
Accept Any Peer ID	Click to accept any peer regardless of its identity.
Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be **IP Address, Domain,** or **E-mail** address. The box under the Type will appear according to the type you select and ask you to fill in corresponding setting.
Accept Subject Name	Click to check the specific fields of digital signature to accept the peer with matching value. The field includes **Country (C), State (ST), Location (L), Organization (O), Organization Unit (OU), Common Name (CN),** and **Email (E)**.

3.10.5 Remote Dial-in User

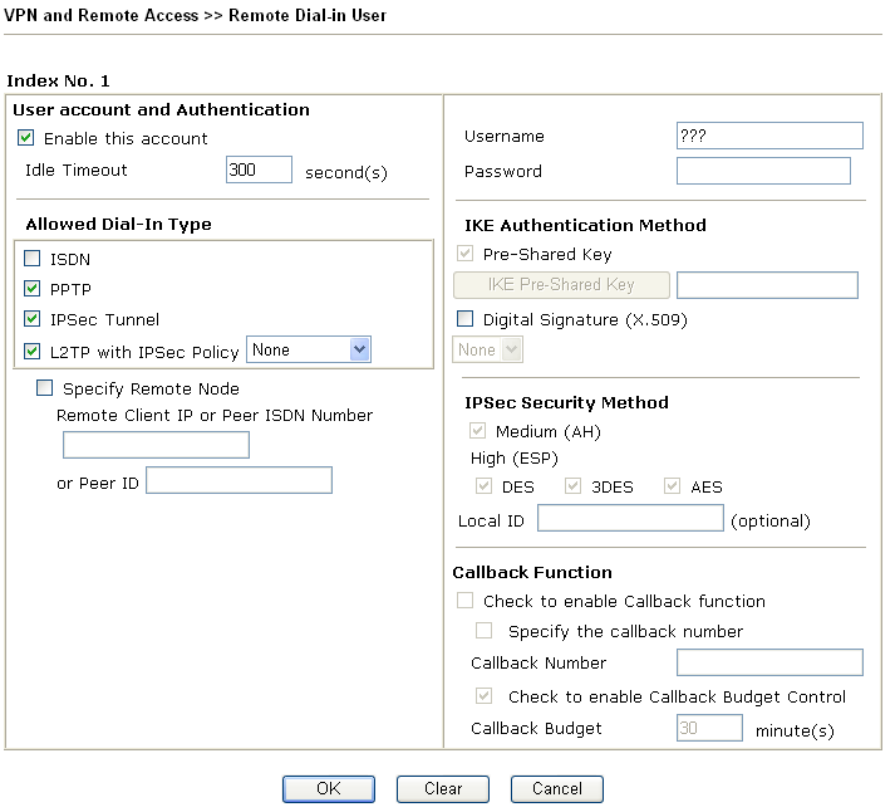
You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via ISDN or build the VPN connection. You may set parameters including specified connection peer ID, connection type (VPN connection - including PPTP, IPSec Tunnel, and L2TP by itself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

The router provides **200** 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.



Set to Factory Default	Click to clear all indexes.
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.



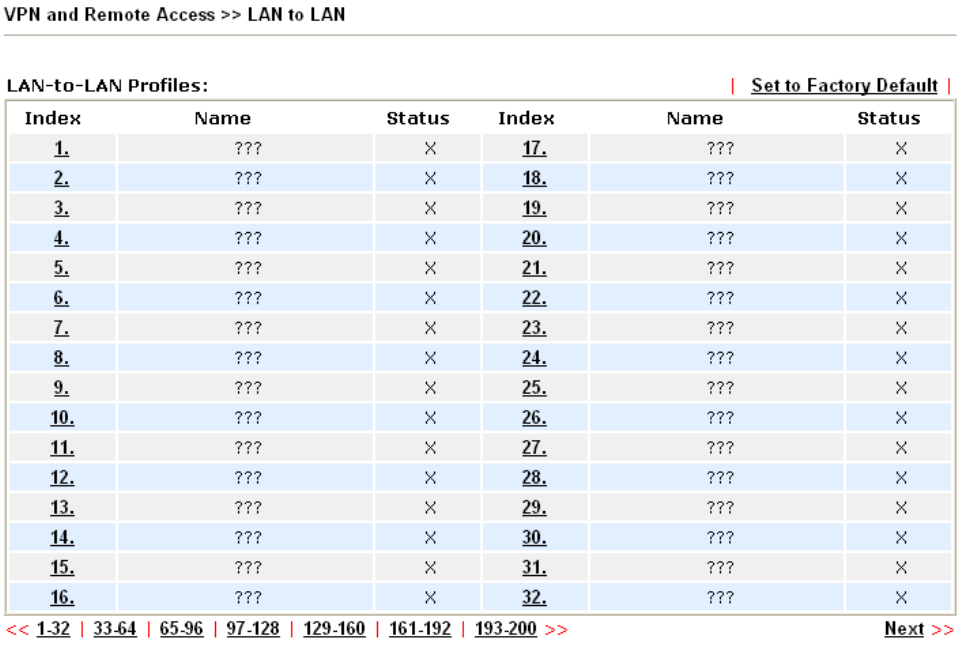
Enable this account	Check the box to enable this function. **Idle Timeout-** If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.
ISDN	Allow the remote ISDN dial-in connection. You can further set up Callback function below. You should set the User Name and Password of remote dial-in user below. This feature is for ***i*** model only.
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	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 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 ISDN, PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select ISDN, 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. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without 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. **Digital Signature (X.509) –** Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the **VPN and Remote Access >>IPSec Peer Identity.**
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method. **Medium -Authentication Header (AH)** means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it. **High-Encapsulating Security Payload (ESP)** means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES. **Local ID -** 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.
Callback Function	The callback function provides a callback service only for the ISDN dial-in user (for *i* model only). The remote user will be charged the connection fee by the telecom. **Check to enable Callback function**-Enables the callback function. **Specify the callback number**-The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number. **Check to enable callback budget control**-By default, the callback function has a time restriction. Once the callback budget has been exhausted, the callback mechanism will be disabled automatically. **Callback Budget (Unit: minutes)**- Specify the time budget for the dial-in user. The budget will be decreased automatically per callback connection.

3.10.6 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 provides up to **200** profiles, which also means supporting **200** VPN tunnels simultaneously. The following figure shows the summary table.



VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles: | Set to Factory Default |

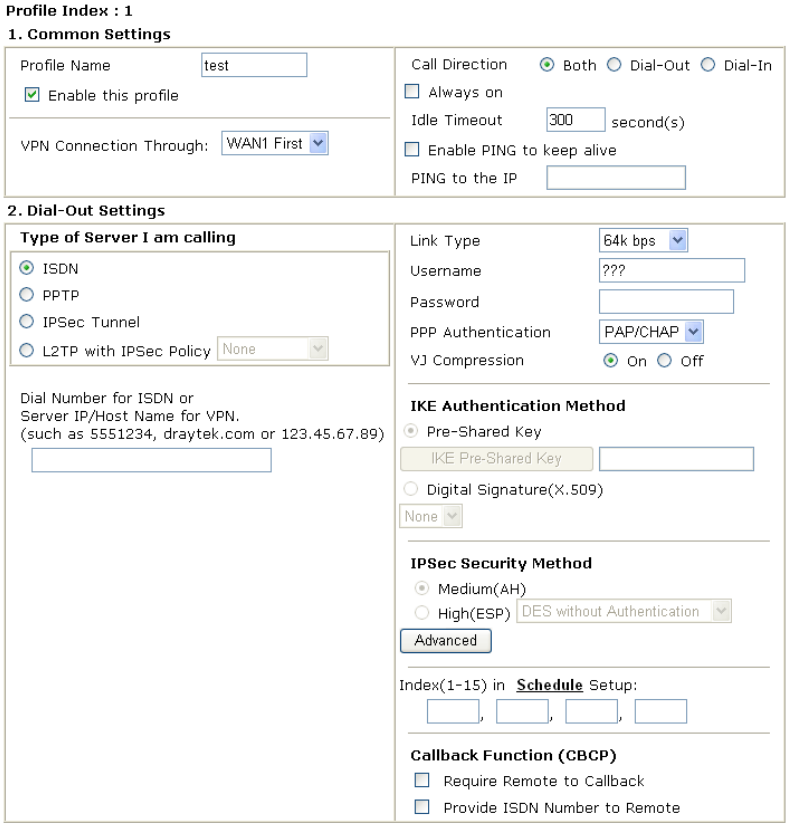
Index	Name	Status	Index	Name	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.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

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 | 193-200 >> Next >>

Set to Factory Default	Click to clear all indexes.
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.

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.

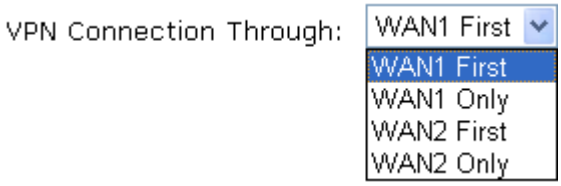
For the web page is too long, we divide the page into several sections for explanation.



Profile Name Specify a name for the profile of the LAN-to-LAN connection.

Enable this profile Check here to activate this profile.

VPN Connection Through Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.



WAN1 First - While connecting, the router will use WAN1 as the first channel for VPN connection. If WAN1 fails, the router will use another WAN interface instead.
WAN1 Only - While connecting, the router will use WAN1 as the only channel for VPN connection.
WAN2 First - While connecting, the router will use WAN2 as the first channel for VPN connection. If WAN2 fails, the router will use another WAN interface instead.
WAN2 Only - While connecting, the router will use WAN2 as the only channel for VPN connection.

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 or Idle Timeout **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.
Enable PING to keep alive	This function is to help the router to determine the status of IPSec VPN connection, especially useful in the case of abnormal VPN IPSec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.
PING to the IP	Enter the IP address of the remote host that located at the other-end of the VPN tunnel.

> **Enable PING to Keep Alive** is used to handle abnormal IPSec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial.
> Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).

ISDN	Build ISDN LAN-to-LAN connection to remote network. You should set up Link Type and identity like User Name and Password for the authentication of remote server. You can further set up Callback (CBCP) function below. This feature is useful for *i* model only.
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 …	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.
Server IP/Host Name for..	You can specify the IP address of the remote dial-out user.
User Name	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
PPP Authentication	This field is applicable when you select ISDN, 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 ISDN, 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.
Digital Signature (X.509) - Select one predefined Profiles set in the **VPN and Remote Access >>IPSec Peer Identity**.

IPSec Security Method

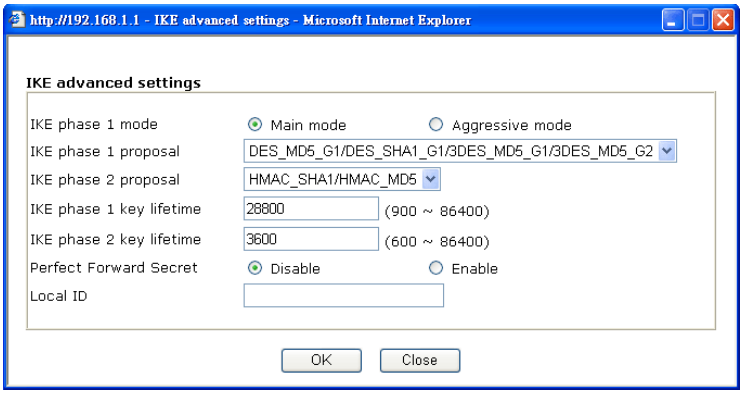
This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.

Medium (AH - Authentication Header) means data will be authenticated, but not be encrypted. By default, this option is active.

High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below:
DES without Authentication -Use DES encryption algorithm and not apply any authentication scheme.
DES with Authentication-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
3DES without Authentication-Use triple DES encryption algorithm and not apply any authentication scheme.
3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
AES without Authentication-Use AES encryption algorithm and not apply any authentication scheme.
AES with Authentication-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

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 proposal-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 2 proposal-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.

Perfect Forward Secret (PFS)-The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.

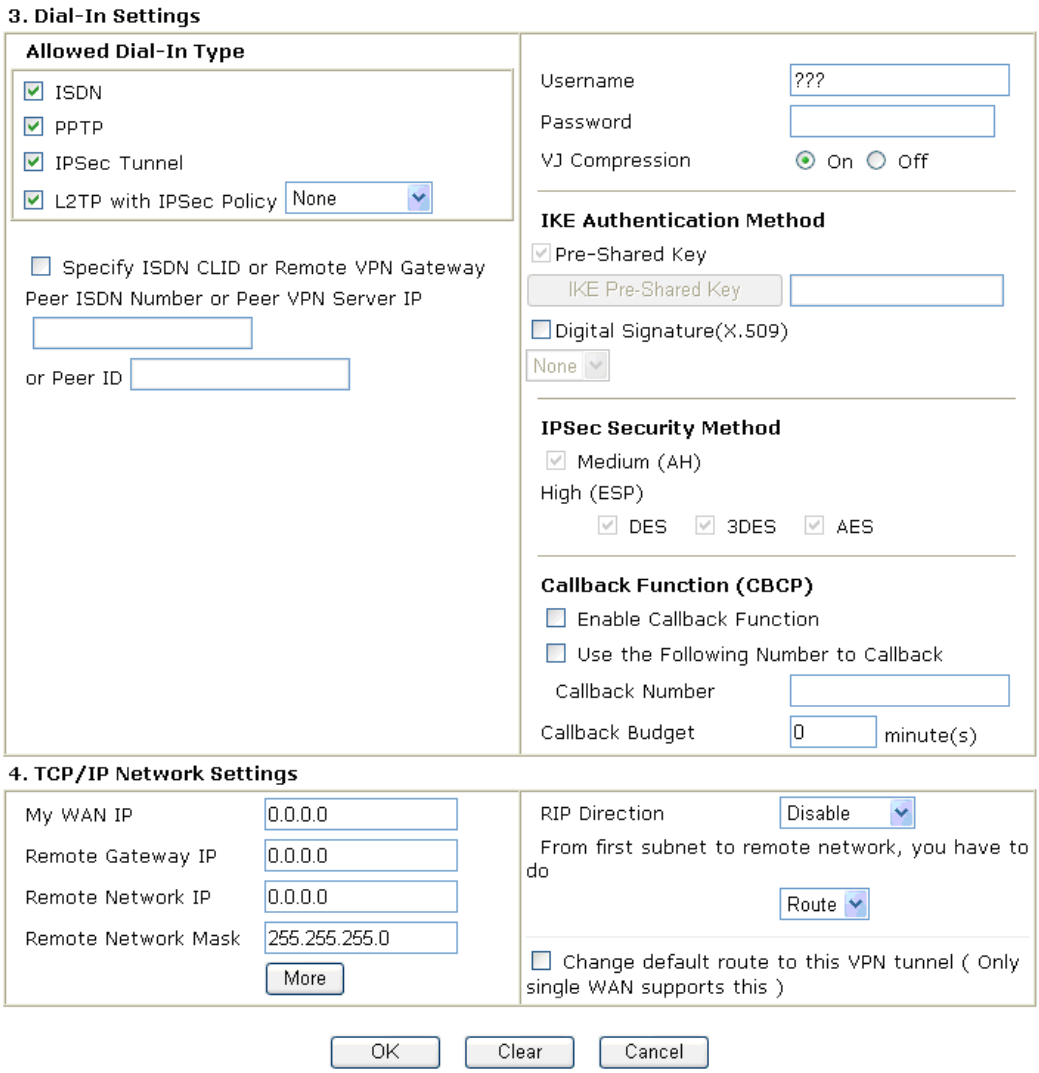
Local ID-In **Aggressive** mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.

Callback Function (for *i* models only)

The callback function provides a callback service as a part of PPP suite only for the ISDN dial-in user. The router owner will be charged the connection fee by the telecom.

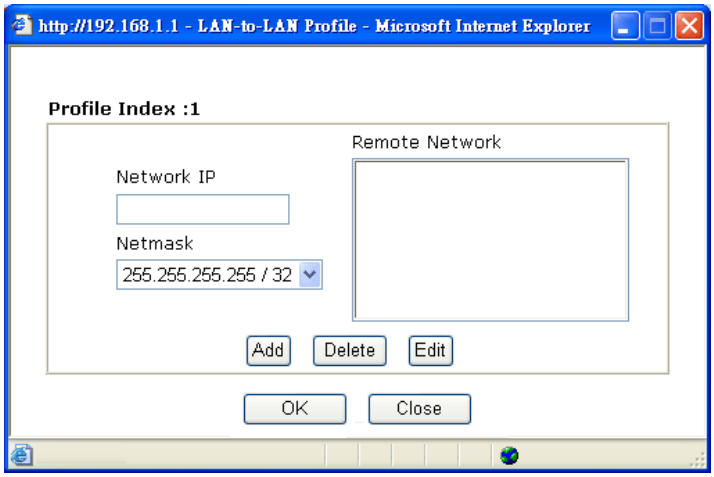
Require Remote to Callback-Enable this to let the router to require the remote peer to callback for the connection afterwards.

Provide ISDN Number to Remote-In the case that the remote peer requires the Vigor router to callback, the local ISDN number will be provided to the remote peer. Check here to allow the Vigor router to send the ISDN number to the remote router. This feature is useful for *i* model only.



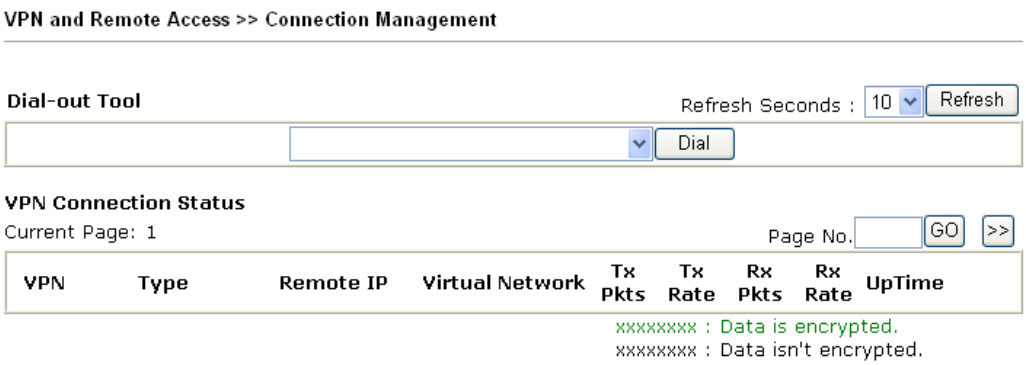
Allowed Dial-In Type	Determine the dial-in connection with different types.
ISDN	Allow the remote ISDN LAN-to-LAN connection. You should set the User Name and Password of remote dial-in user below. This feature is useful for *i* model only. In addition, you can further set up Callback function below.
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	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 CLID or 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. Enter Peer ISDN number if you select ISDN above (This feature is useful for *i* model only.). 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 ISDN, PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
VJ Compression	VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select ISDN, 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. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without 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. **Digital Signature (X.509) –** Check the box of Digital Signature to invoke this function and select one predefined Profiles set in the **VPN and Remote Access >>IPSec Peer Identity**.
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. **Medium-** Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. **High-** Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
Callback Function	The callback function provides a callback service only for the ISDN LAN-to-LAN connection (this feature is useful for *i* model only). The remote user will be charged the connection fee by the telecom. **Check to enable Callback function**-Enables the callback function. **Callback number**-The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number. **Callback budget**- By default, the callback function has limitation of callback period. Once the callback budget is exhausted, the function will be disabled automatically.

	Callback Budget (Unit: minutes)- Specify the time budget for the dial-in user. The budget will be decreased automatically per callback connection. The default value 0 means no limitation of callback period.
My WAN IP	This field is only applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select ISDN, PPTP or L2TP.
Remote Gateway IP	This field is only applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select ISDN, PPTP or L2TP.
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.
More	Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router. 
RIP Direction	The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.
From first subnet to remote network, you have to do	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 (Only single WAN supports this)	Check this box to change the default route with this VPN tunnel. Be aware that this setting is available only for one WAN interface is enabled. It is not available when both WAN interfaces are enabled.

3.10.7 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.



Dial	Click this button to execute dial out function.
Refresh Seconds	Choose the time for refresh the dial information among 5, 10, and 30.
Refresh	Click this button to refresh the whole connection status.

3.11 Certificate Management

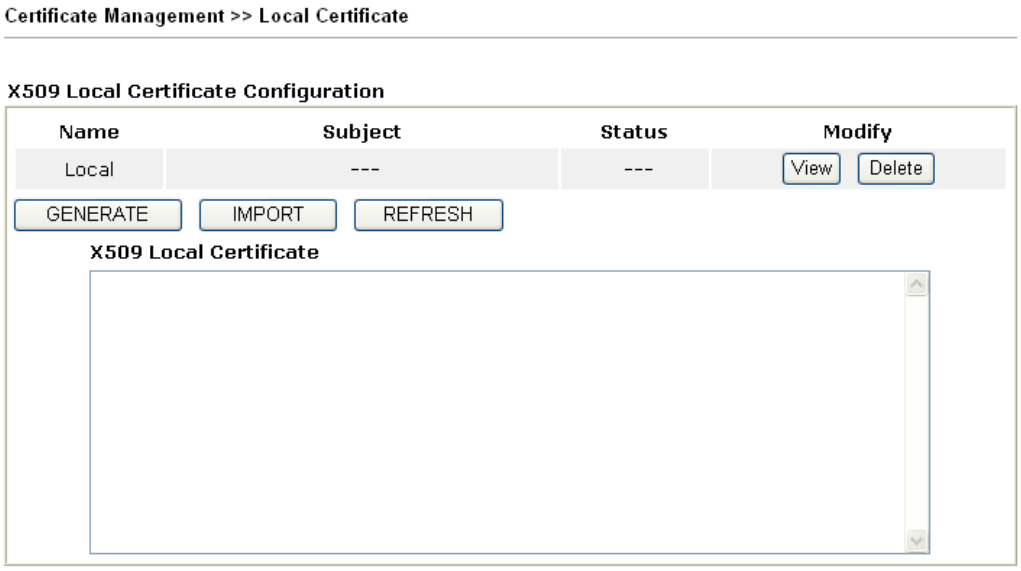
A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Here Vigor router support digital certificates conforming to standard X.509.

Any entity wants to utilize digital certificates should first request a certificate issued by a CA server. It should also retrieve certificates of other trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers.

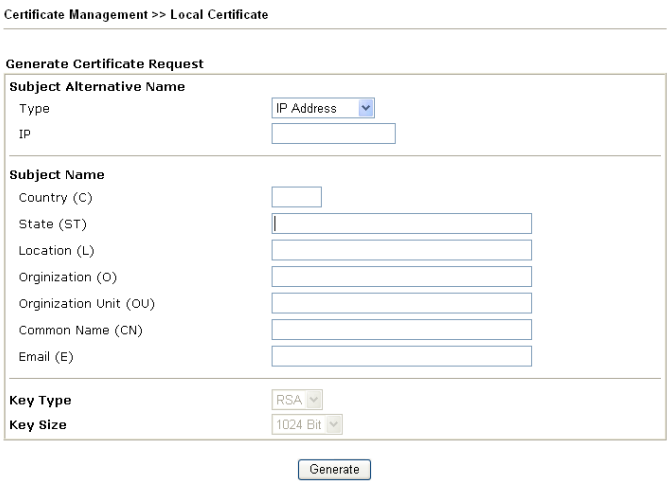
Here you can manage generate and manage the local digital certificates, and set trusted CA certificates. Remember to adjust the time of Vigor router before using the certificate so that you can get the correct valid period of certificate.

Below shows the menu items for Certificate Management.

3.11.1 Local Certificate



Generate Click this button to open **Generate Certificate Request** window.



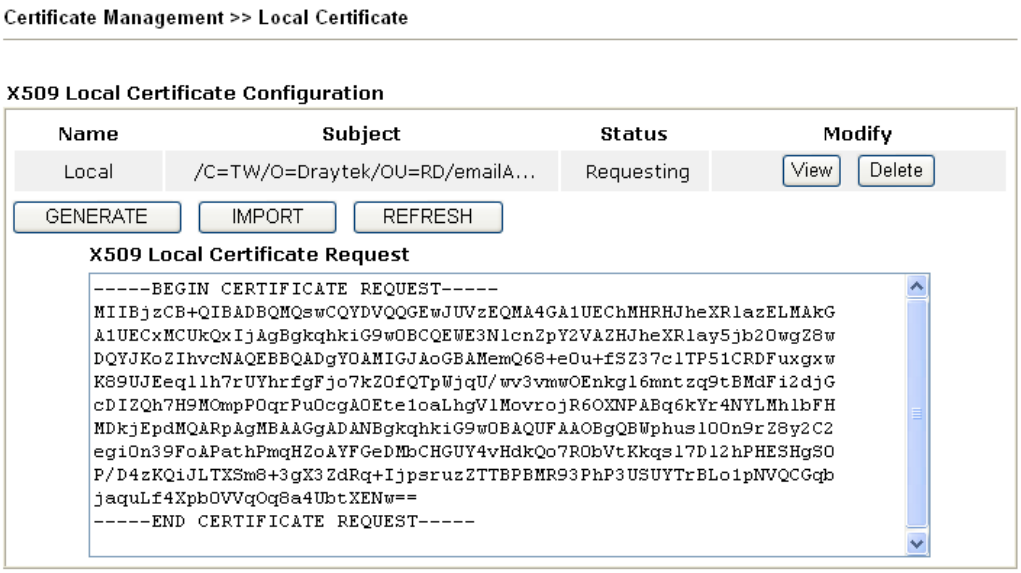
Type in all the information that the window request. Then click **Generate** again.

Import Click this button to import a saved file as the certification information.

Refresh Click this button to refresh the information listed below.

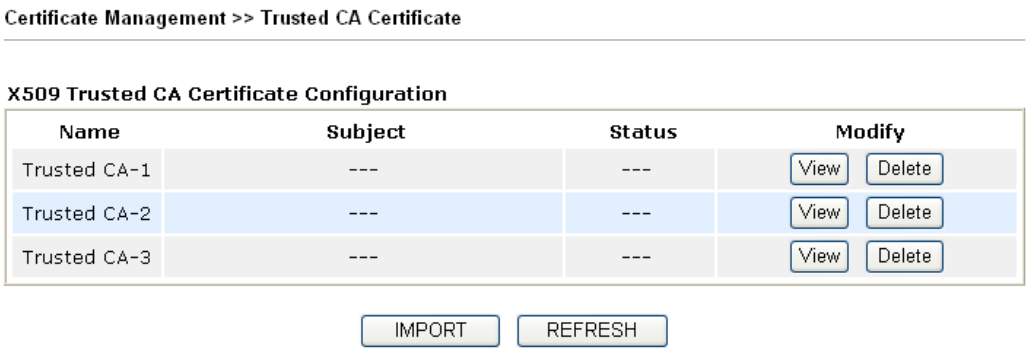
View Click this button to view the detailed settings for certificate request.

After clicking **Generate**, the generated information will be displayed on the window below:

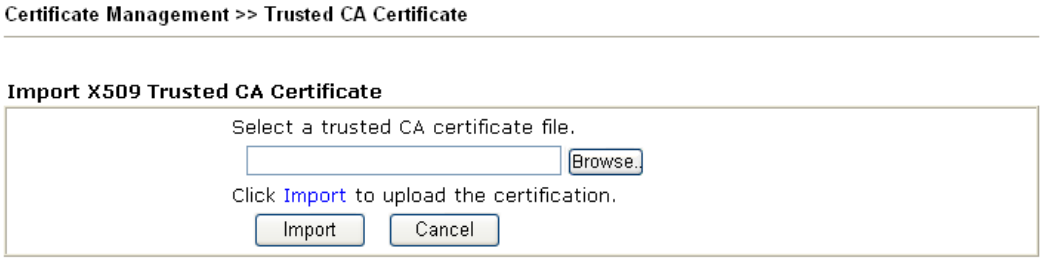


3.11.2 Trusted CA Certificate

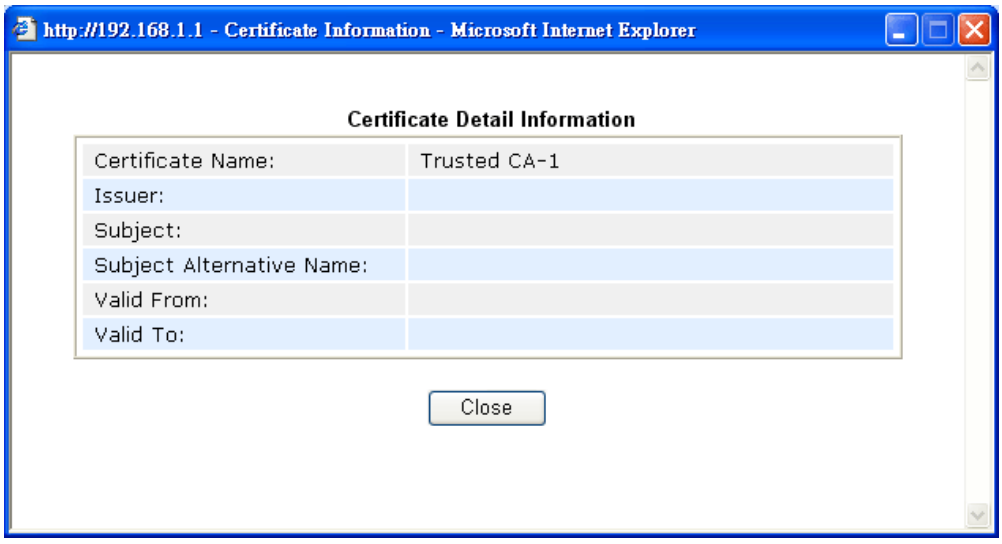
Trusted CA certificate lists three sets of trusted CA certificate.



To import a pre-saved trusted CA certificate, please click **IMPORT** to open the following window. Use **Browse…** to find out the saved text file. Then click Import. The one you imported will be listed on the Trusted CA Certificate window. Then click **Import** to use the pre-saved file.



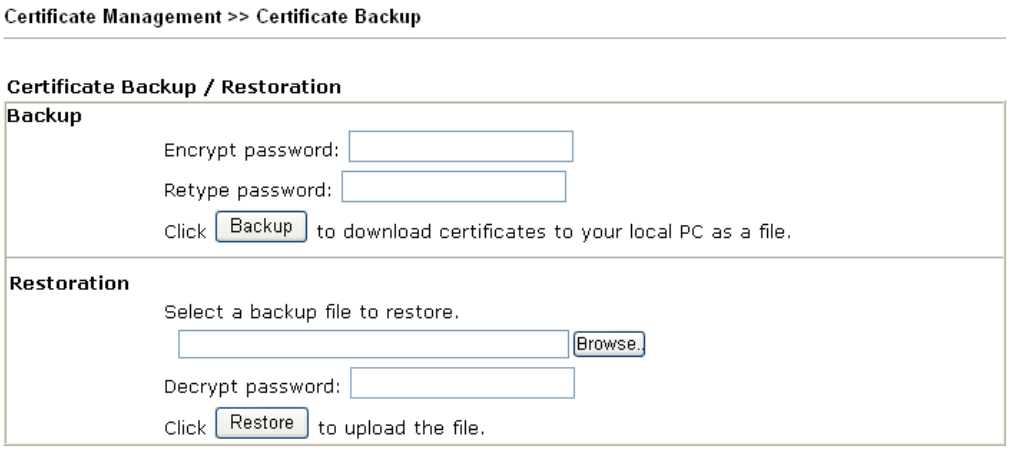
For viewing each trusted CA certificate, click **View** to open the certificate detail information window. If you want to delete a CA certificate, choose the one and click **Delete** to remove all the certificate information.



3.11.3 Certificate Backup

Local certificate and Trusted CA certificate for this router can be saved within one file. Please click **Backup** on the following screen to save them. If you want to set encryption password for these certificates, please type characters in both fields of **Encrypt password** and **Retype password**.

Also, you can use **Restore** to retrieve these two settings to the router whenever you want.



3.12 Web Access Control

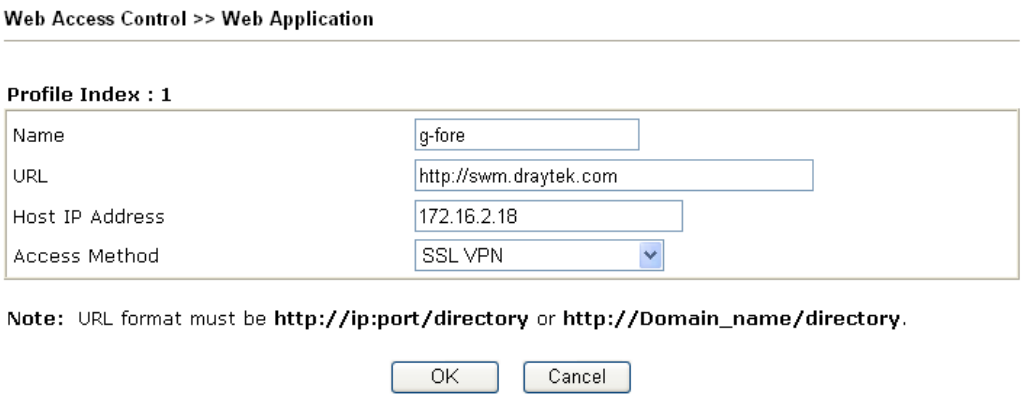
Web Access Control is used to access web servers on LAN side from browser. With such function, user(s) or administrator (s) can register and access the specified web server on LAN behind the router through any web browser.

3.12.1 Web Application

Such page allows you to set interior web server profiles.

Set to Factory Default	Clear all profiles.
Index	Click the link to access into next web page for configure web application server profile. You can set about 30 profiles for such device.
Name	Display the name of the server profile you typed for web application.
URL	Display the URL content for the server you want to control for the specified web application.
Active	Display the access method you specified for such web application profile.

When you click the number link under Index, you will see the following page for configuring web application.

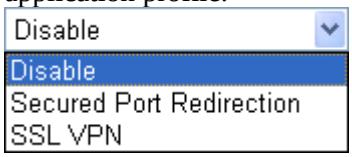


Name Please type a name (no more than 15 characters) for web server on LAN.

URL Display the URL content for the server (on LAN) you want to access for the specified web application. For example, you want to access a special system which is loated on http://swm.draytek.com, please type http://swm.draytek.com.

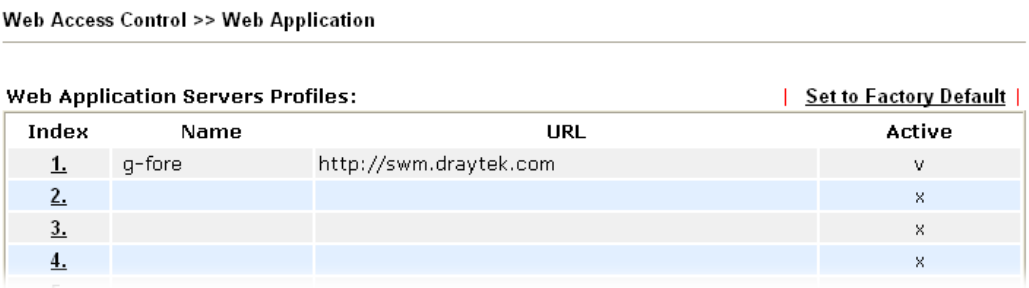
Host IP Address When the above URL does not contain IP address, you have to fill correspoinding host IP to that URL. If the above URL contains IP address, such as http://172.16.3.5/xxxx, it is not necessary to type anything here.

Active Display the access method you specified for such web application profile.



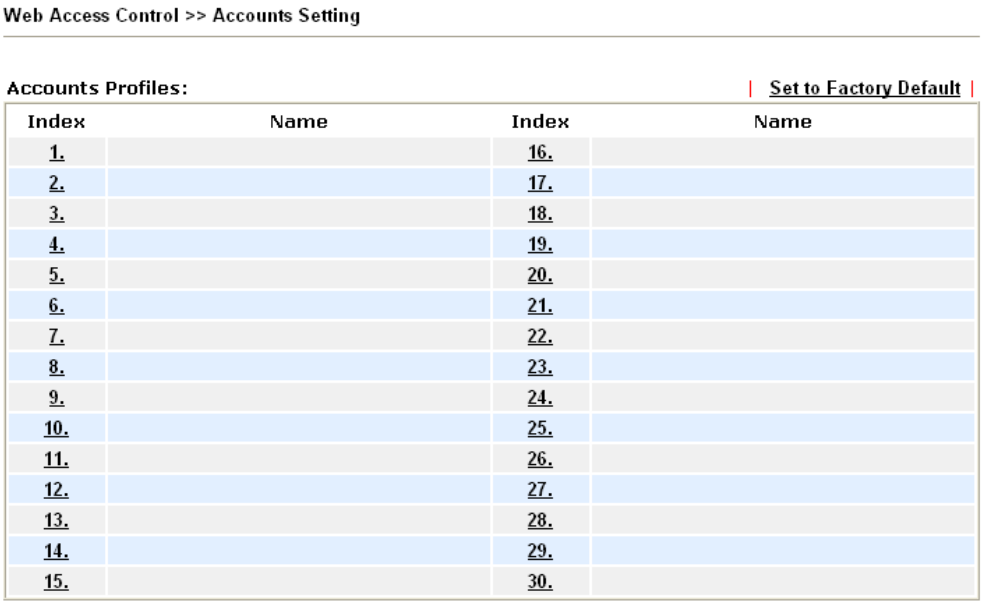
Disable – It means no action will be done.
Secured Port Redirection – Choose this action if SSL VPN is not supported due to NTML authentication required by the web server.
SSL VPN – Using this function is recommended.

After you click OK, a new profile will be set. See the following example.



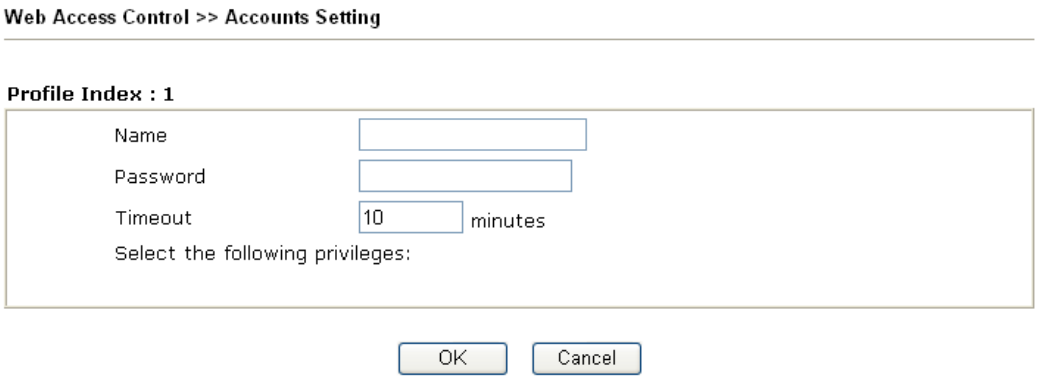
3.12.2 User Account

To access into the web server, user(s)or administrator(s) must set user account.



Set to Factory Default	Clear all profiles.
Index	Click the link to access into next web page for configure web application server profile. You can set about 30 profiles for accounts.
Name	Display the name of the account profile you typed for web application.

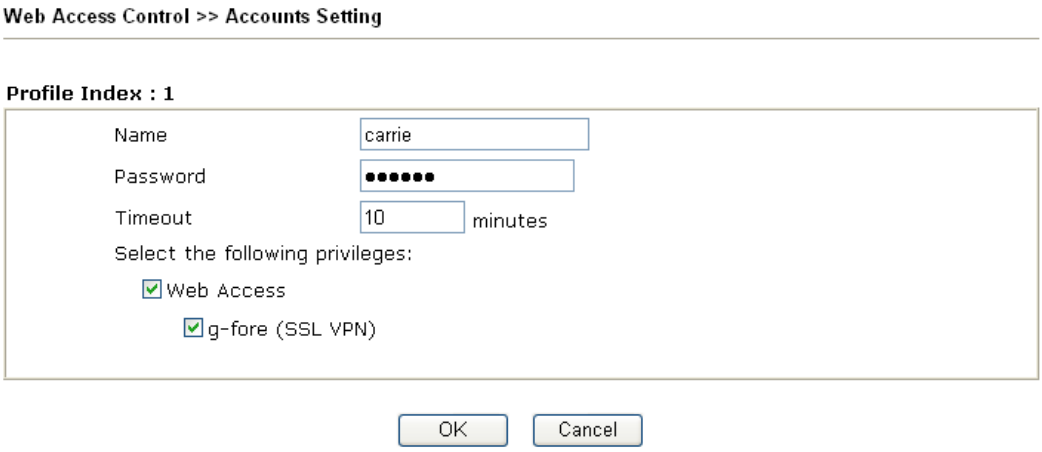
When you click the number link under Index, you will see the following page for configuring account settings.



Name	Please type a name (no more than 15 characters) for using when you want to access into web server as authentication.
Password	Type the password for such account name as authentication.
Timeout	For network security, if there is no operation during the period of the time set here, the system will break down the network connection.
Select the following priviledges	If there is no web application set previously, nothing will be shown here. If yes, you can check all of them or any of them

for accessing with the account specified.

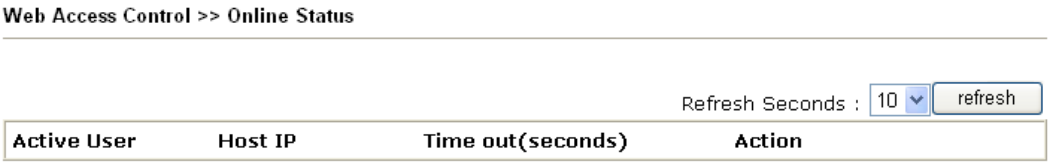
Below shows an example. Under **Select the following priviledges**, you can see one sub-item (g-fore, configured in Web Application) for you to choose for accessing later.



Next time, when you want to access g-fore from any computer, simply type URL specified for g-fore(e.g., 172.16.2.18) on the command line of browser. A pop-up window will appear and ask you to enter your user name and password. You must type the name and password that set in user account web page.

3.12.3 Online User Status

Such page displays online user status at present.



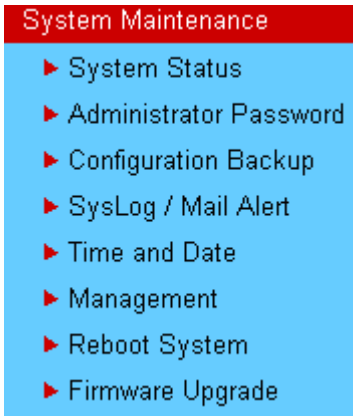
If you have visited or accessed into the web server that you specified in Web Application, Online User Status will show the basic information as the following example.

Active User	Display name of the user that accesses the web server currently.
Host IP	Display the IP address of the host.
Time out	Display the remaining time that the connection will be dropped if there is no action on the web server.
Action	Click the **Drop** button to terminate the web server connection.
Refresh	Click it to reload the page.

3.13 System Maintenance

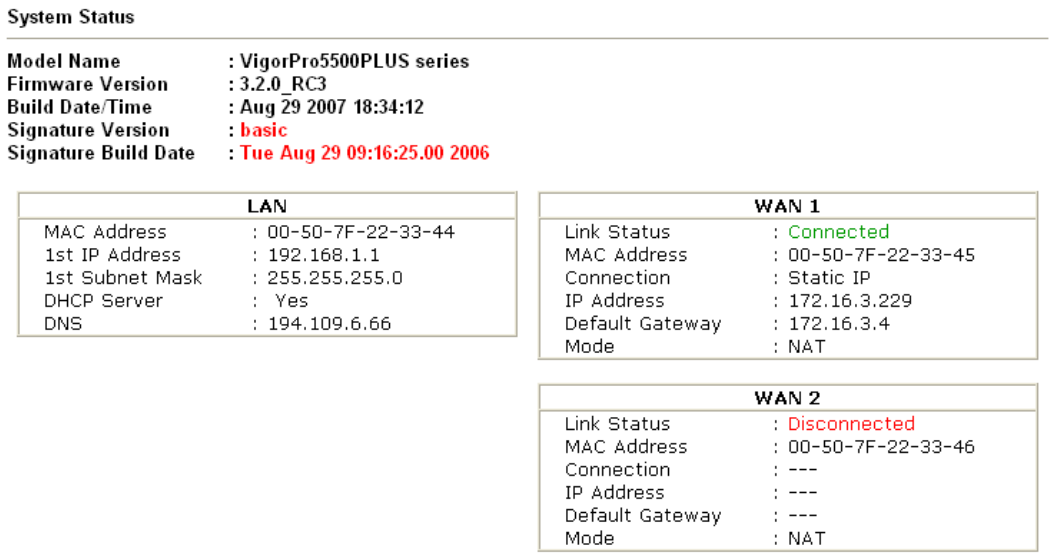
For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog, Time setup, Reboot System, Firmware Upgrade.

Below shows the menu items for System Maintenance.



3.13.1 System Status

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



Model Name	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.
MAC Address	Display the MAC address of the LAN Interface.
1st IP Address	Display the IP address of the LAN interface.
1st Subnet Mask	Display the subnet mask address of the LAN interface.

DHCP Server	Display the current status of DHCP server of the LAN interface.
DNS	Display the assigned IP address of the primary DNS.
Link Status	Display the connection status of WAN interface.
MAC Address	Display the MAC address of the WAN Interface.
Connection	Display the chosen WAN mode.
IP Address	Display the IP address of the WAN interface.
Default Gateway	Display the assigned IP address of the default gateway.

3.13.2 Administrator Password

This page allows you to set new password.

Old Password	Type in the old password. The factory default setting for password is blank.
New Password	Type in new password in this filed.
Confirm Password	Type in the new password again.

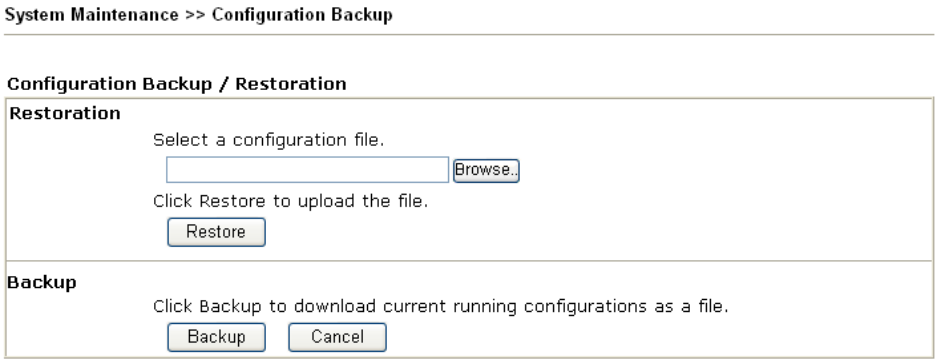
When you click OK, the login window will appear. Please use the new password to access into the web configurator again.

3.13.3 Configuration Backup

Backup the Configuration

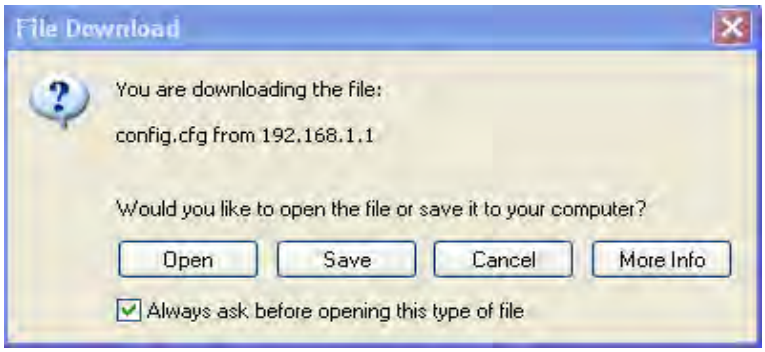
Follow the steps below to backup your configuration.

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

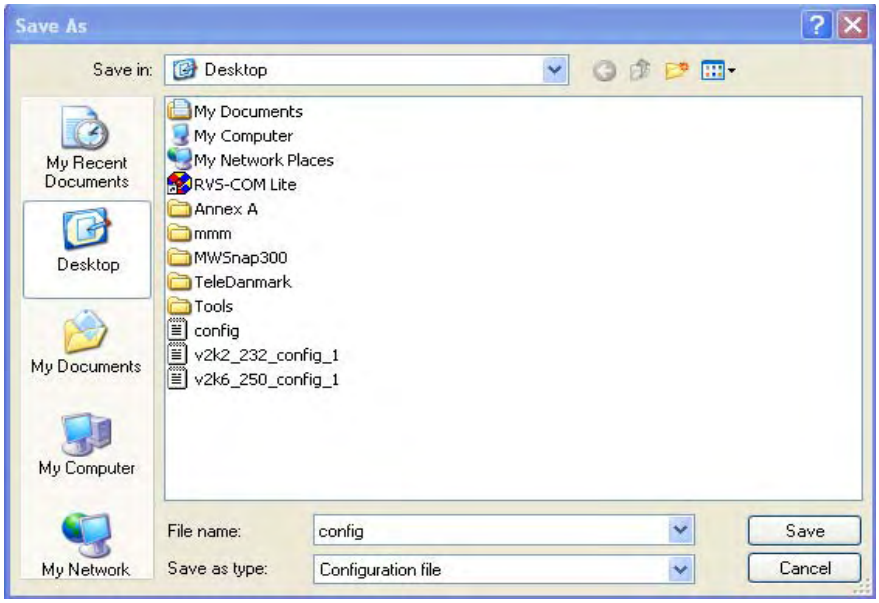


2. Click **Backup** button to get into the following dialog. Click **Save** button to open

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.



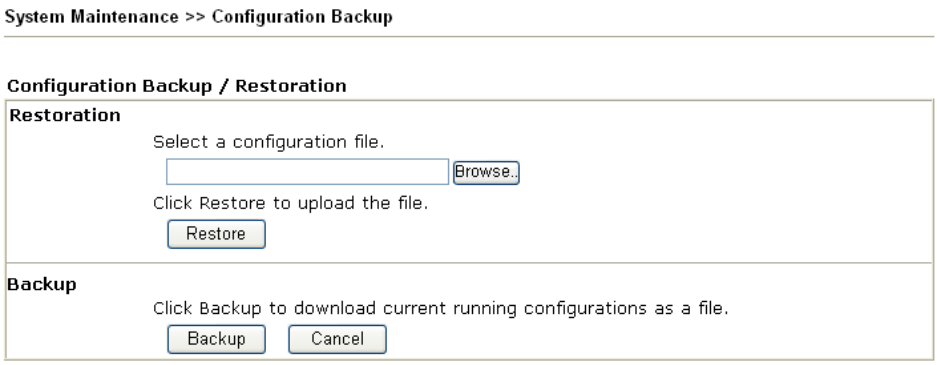
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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

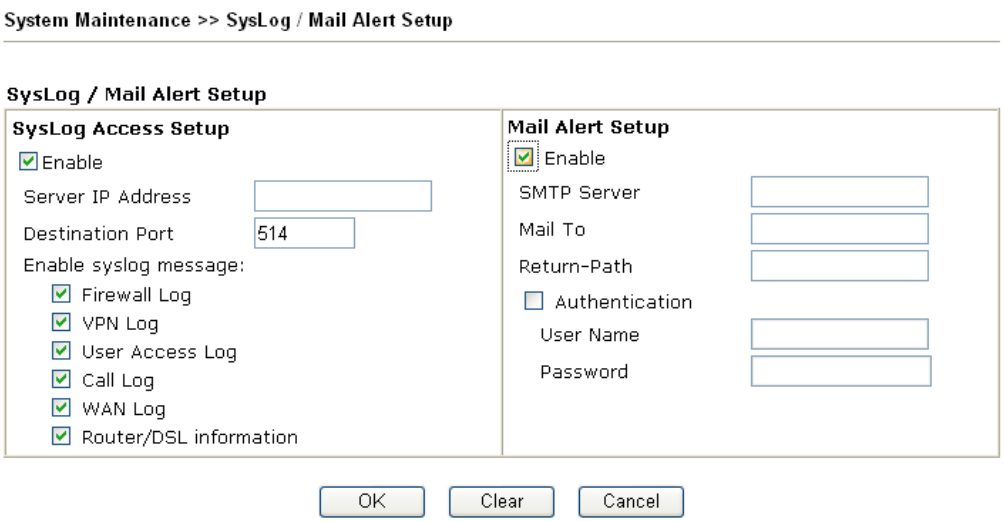
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.



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

3.13.4 Syslog/Mail Alert

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

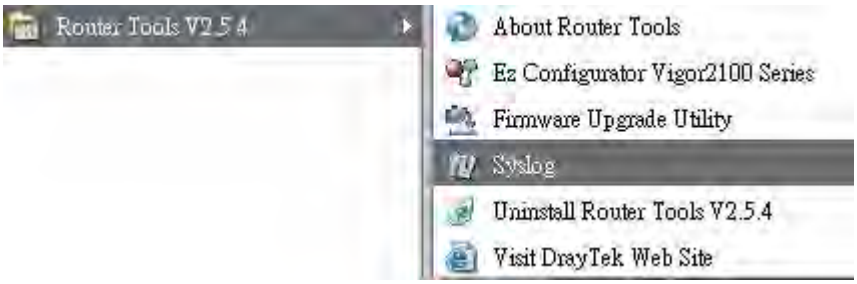


Enable	Click "**Enable**" to activate this function.
Syslog Server IP	The IP address of the Syslog server.
Destination Port	Assign a port for the Syslog protocol.
Enable syslog message	Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.
SMTP Server	The IP address of the SMTP server.
Mail To	Assign a mail address for sending mails out.
Return-Path	Assign a path for receiving the mail from outside.
Authentication	Check this box to activate this function while using e-mail application.
User Name	Type the user name for authentication.
Password	Type the password for authentication.

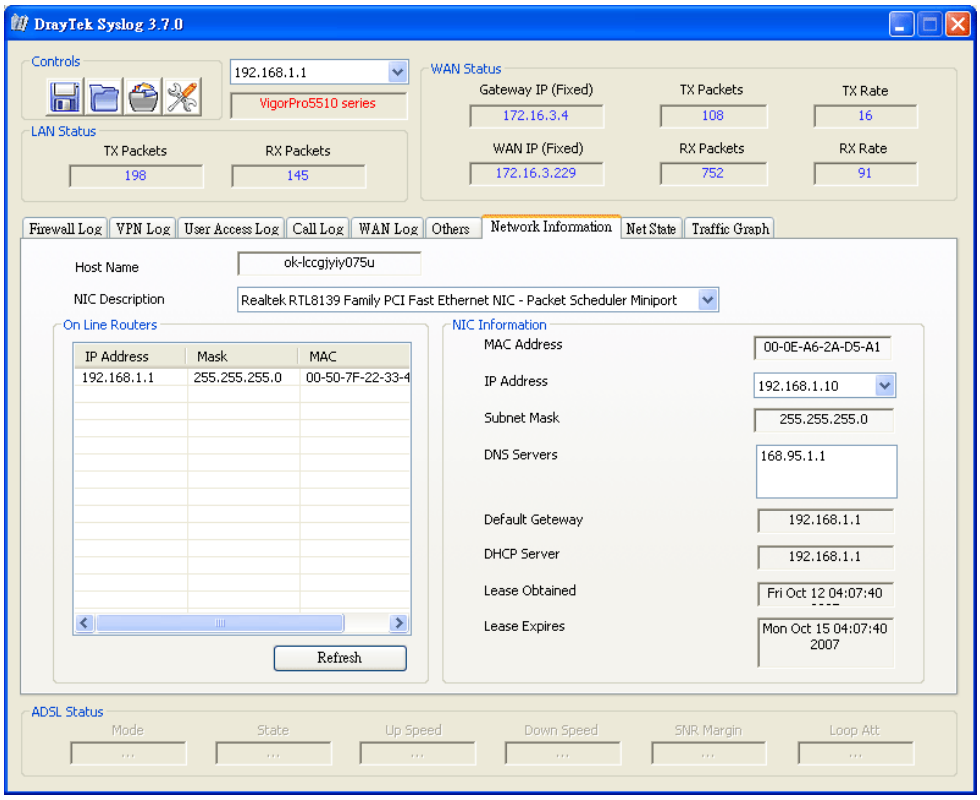
Click **OK** to save these settings.

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.

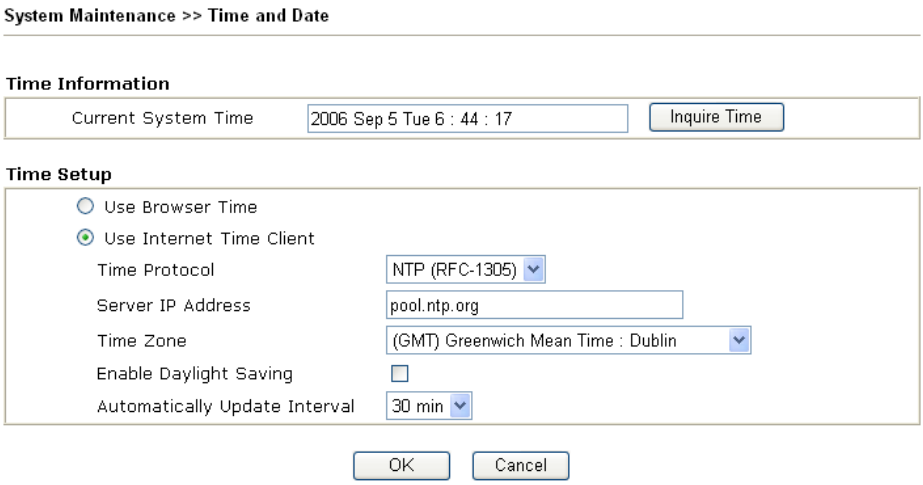


3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.



3.13.5 Time and Date

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

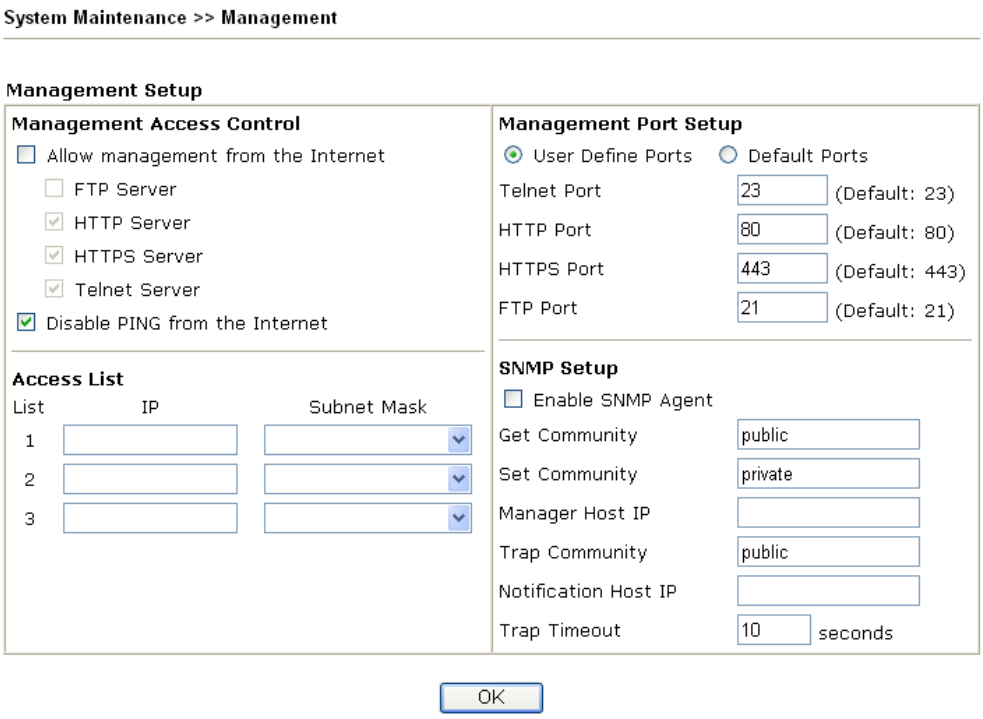


Current System Time	Click **Inquire Time** to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time Protocol	Select a time protocol.
Server IP Address	Type the IP address of the time server.
Time Zone	Select the time zone where the router is located.
Automatically Update Interval	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

3.13.6 Management

This page allows you to manage the settings for access control, access list, port setup, and SNMP setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session. The default value is 5060 and this must match with the peer Registrar when making VoIP calls.

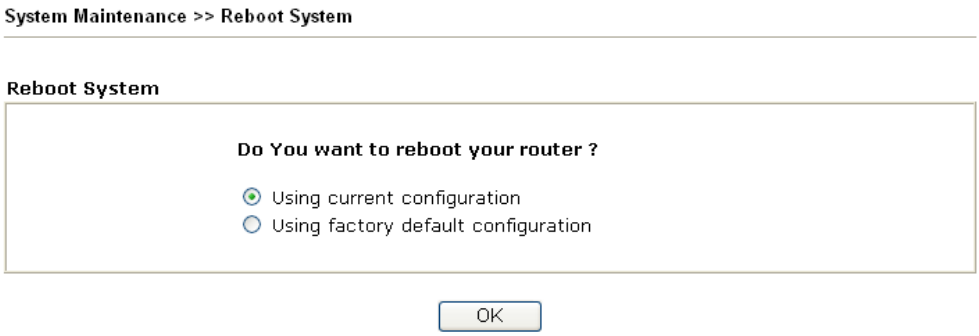


Allow management from the Internet	Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
Disable PING from the Internet	Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.
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.
User Define Ports	Check to specify user-defined port numbers for the Telnet and HTTP servers.
Default Ports	Check to use standard port numbers for the Telnet and HTTP servers.
Enable SNMP Agent	Check it to enable this function.
Get Community	Set the name for getting community by typing a proper character. The default setting is **public.**
Set Community	Set community by typing a proper name. The default setting is **private.**
Manager Host IP	Set one host as the manager to execute SNMP function. Please type in IP address to specify certain host.

Trap Community	Set trap community by typing a proper name. The default setting is **public.**
Notification Host IP	Set the IP address of the host that will receive the trap community.
Trap Timeout	The default setting is 10 seconds.

3.13.7 Reboot System

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



If you want to reboot the router using the current configuration, check **Using current configuration** and click **OK**. To reset the router settings to default values, check **Using factory default configuration** and click **OK**. The router will take 5 seconds to reboot the system.

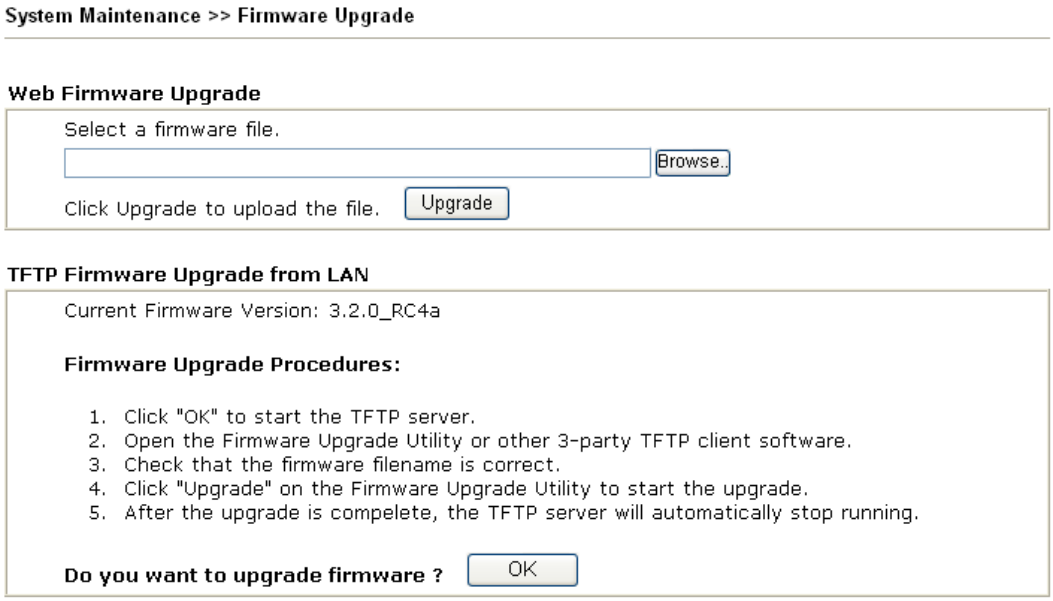
Note: When the system pops up Reboot System web page after you configure web settings, please click **OK** to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

3.13.8 Firmware Upgrade

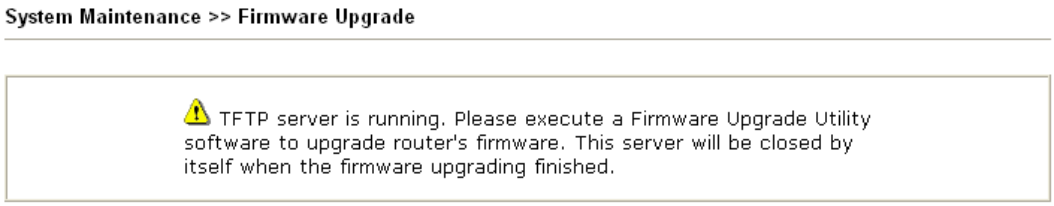
Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

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

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



Click **OK**. The following screen will appear. Please execute the firmware upgrade utility first.

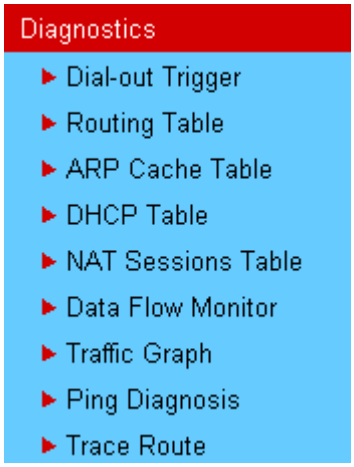


For the detailed information about firmware update, please go to Chapter 4.

3.14 Diagnostics

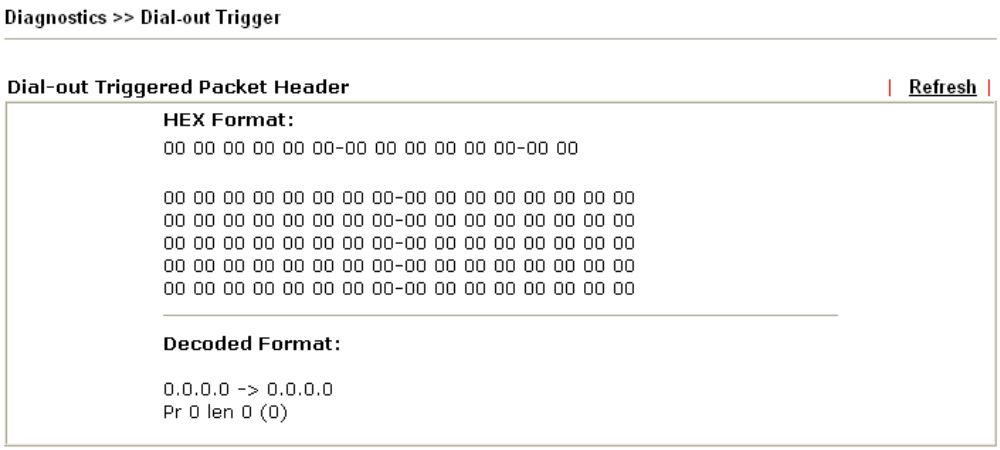
Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router.

Below shows the menu items for Diagnostics.



3.14.1 Dial-out Trigger

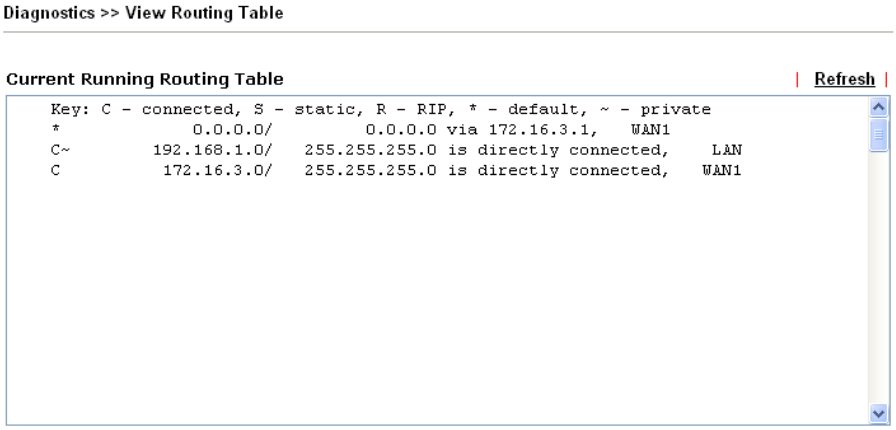
Click **Diagnostics** and click **Dial-out Trigger** to open the web page. The internet connection (e.g., ISDN, PPPoE, PPPoA, etc) is triggered by a package sending from the source IP address.



Decoded Format	It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.
Refresh	Click it to reload the page.

3.14.2 Routing Table

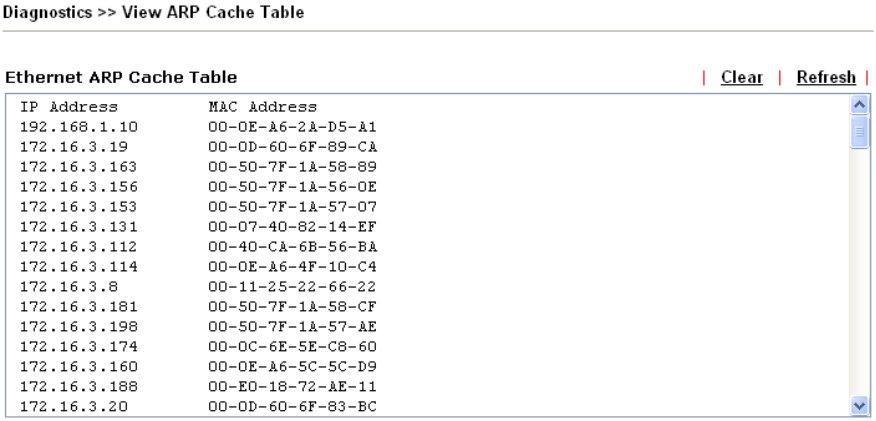
Click **Diagnostics** and click **Routing Table** to open the web page.



Refresh Click it to reload the page.

3.14.3 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.



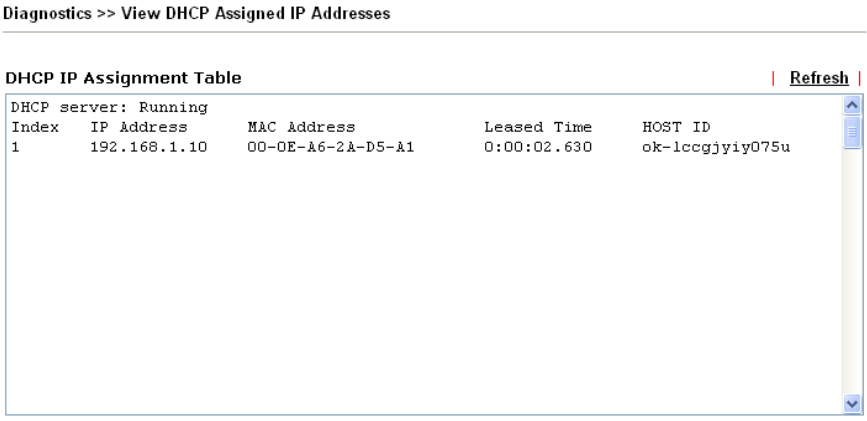
Refresh Click it to reload the page.

Clear Click it to clear the whole table.

3.14.4 DHCP Table

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

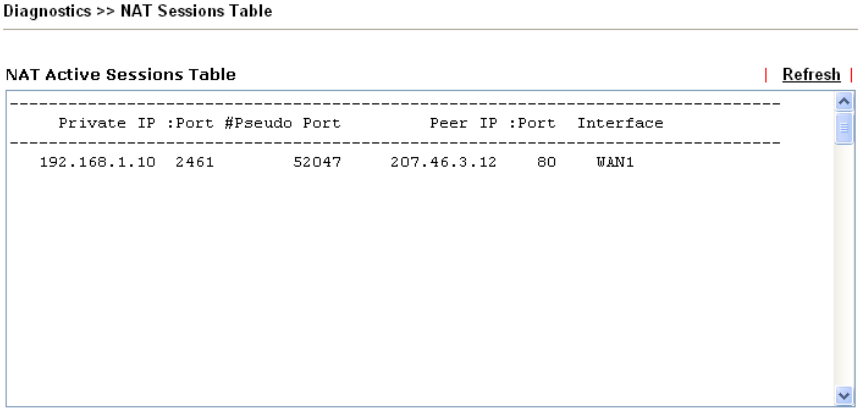
Click **Diagnostics** and click **DHCP Table** to open the web page.



Index	It displays the connection item number.
IP Address	It displays the IP address assigned by this router for specified PC.
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.
Leased Time	It displays the leased time of the specified PC.
HOST ID	It displays the host ID name of the specified PC.
Refresh	Click it to reload the page.

3.14.5 NAT Sessions Table

Click **Diagnostics** and click **NAT Sessions Table** to open the setup page.



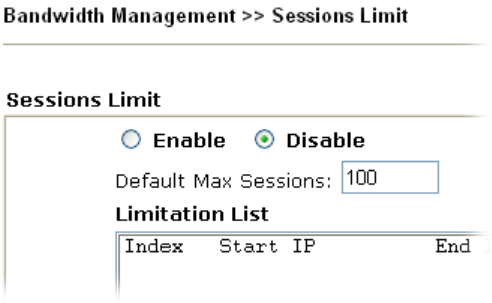
Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the router used for NAT.
Peer IP :Port	It indicates the destination IP address and port of remote host.

Interface It indicates the interface of the WAN connection.

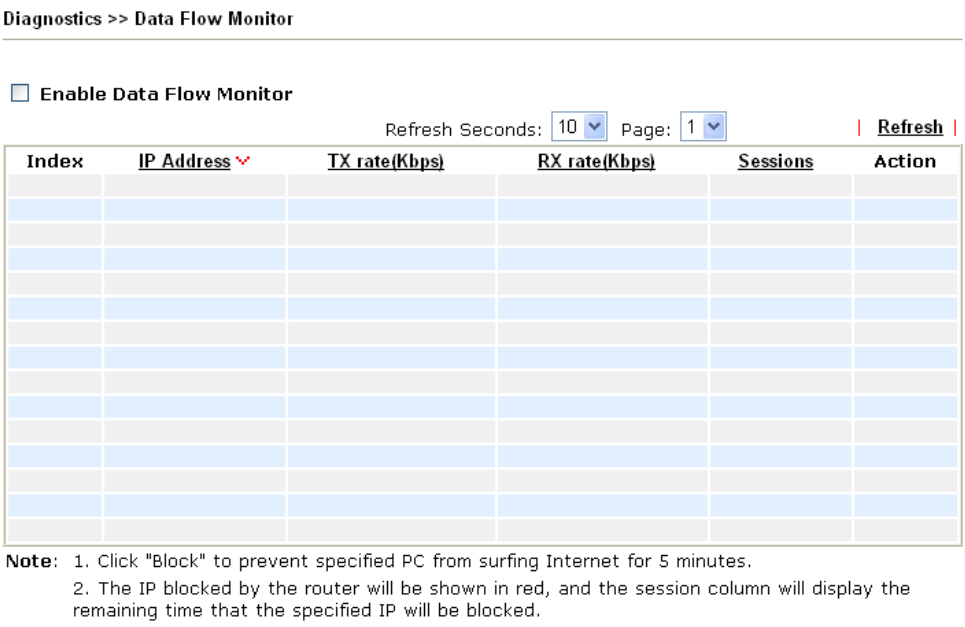
Refresh Click it to reload the page.

3.14.6 Data Flow Monitor

This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds. The IP address listed here is configured in Bandwidth Management. You have to enable IP bandwidth limit and IP session limit before invoke Data Flow Monitor. If not, a notification dialog box will appear to remind you enabling it.

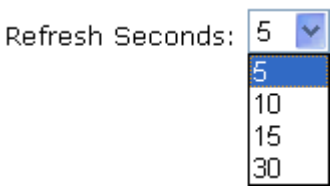


Click **Diagnostics** and click **Data Flow Monitor** to open the web page. You can click **IP Address**, **TX rate**, **RX rate** or **Session** link for arranging the data display.



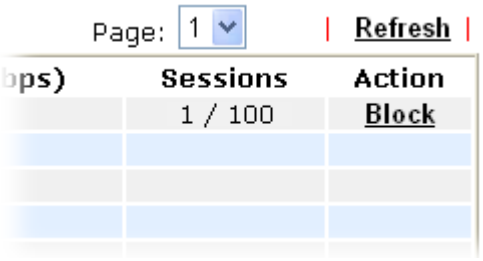
Enable Data Flow Monitor Check this box to enable this function.

Refresh Seconds Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.

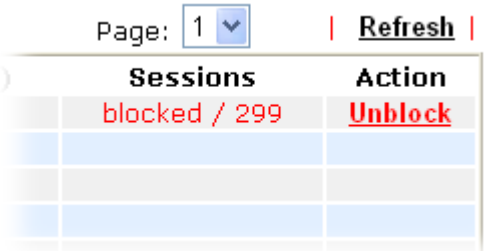


Refresh Click this link to refresh this page manually.

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 that you specified in Limit Session web page.
Action	**Block** - can prevent specified PC accessing into Internet within 5 minutes.

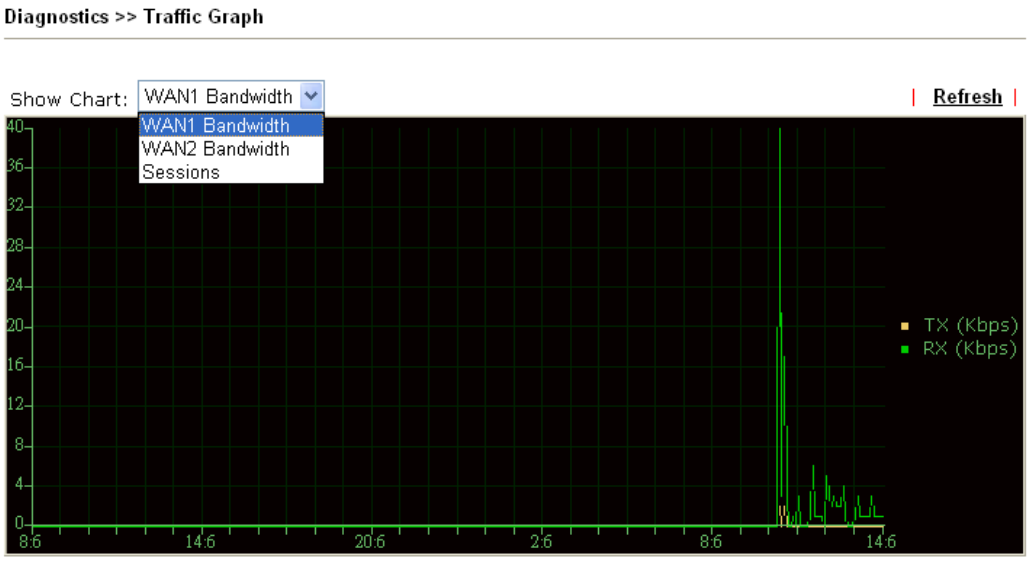


Unblock – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column.



3.14.7 Traffic Graph

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

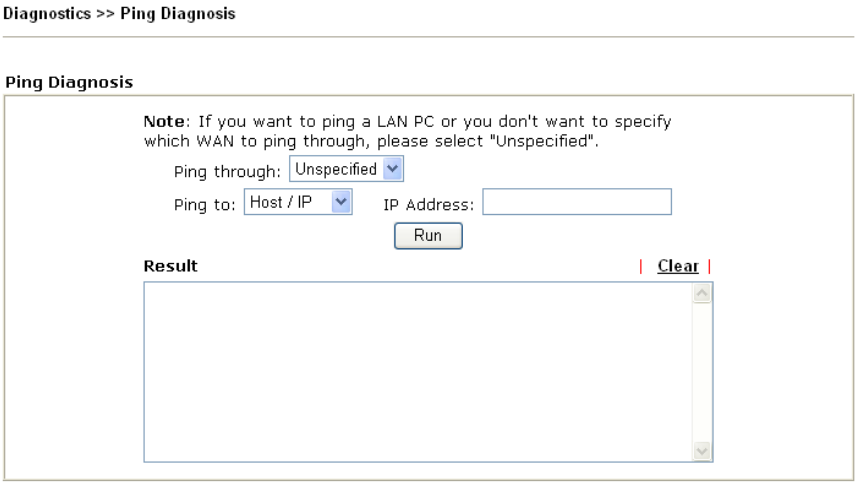


The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

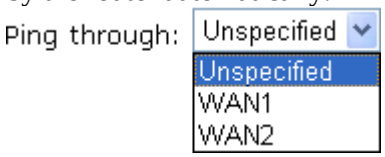
For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.

3.14.8 Ping Diagnosis

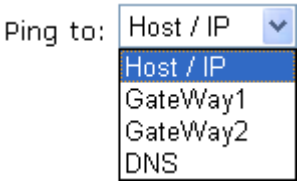
Click **Diagnostics** and click **Ping Diagnosis** to pen the web page.



Ping through Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the router automatically.



Ping to Use the drop down list to choose the destination that you want to ping.



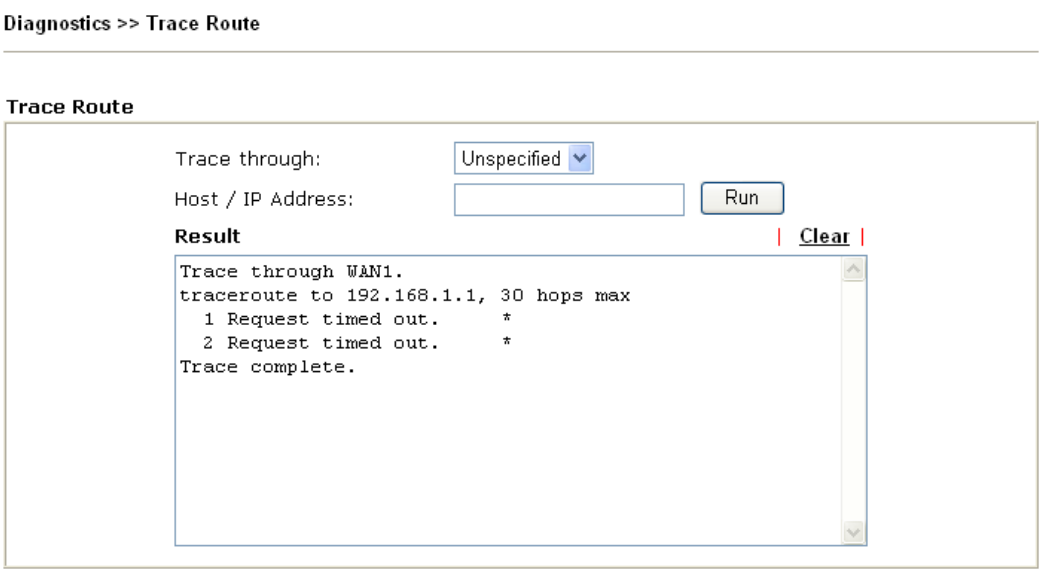
IP Address Type in the IP address of the Host/IP that you want to ping.

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.

3.14.9 Trace Route

Click **Diagnostics** and click **Trace Route** to open the web page. This page allows you to trace the routes from router to the host. Simply type the IP address of the host in the box and click **Run**. The result of route trace will be shown on the screen.



Trace through Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the router automatically.

Host/IP Address It indicates the IP address of the host.

Run Click this button to start route tracing work.

Clear Click this link to remove the result on the window.

4 Registration for the Router

To use the anti-intrusion and anti-virus features of VigorPro series router, you have to create a new account, finish the registration for that account by using the router and complete the registration for the Vigor router. After finishing the registration of the router, you can download the newly update types and rules of anti-intrusion and anti-virus during the valid time of the license key you purchased.

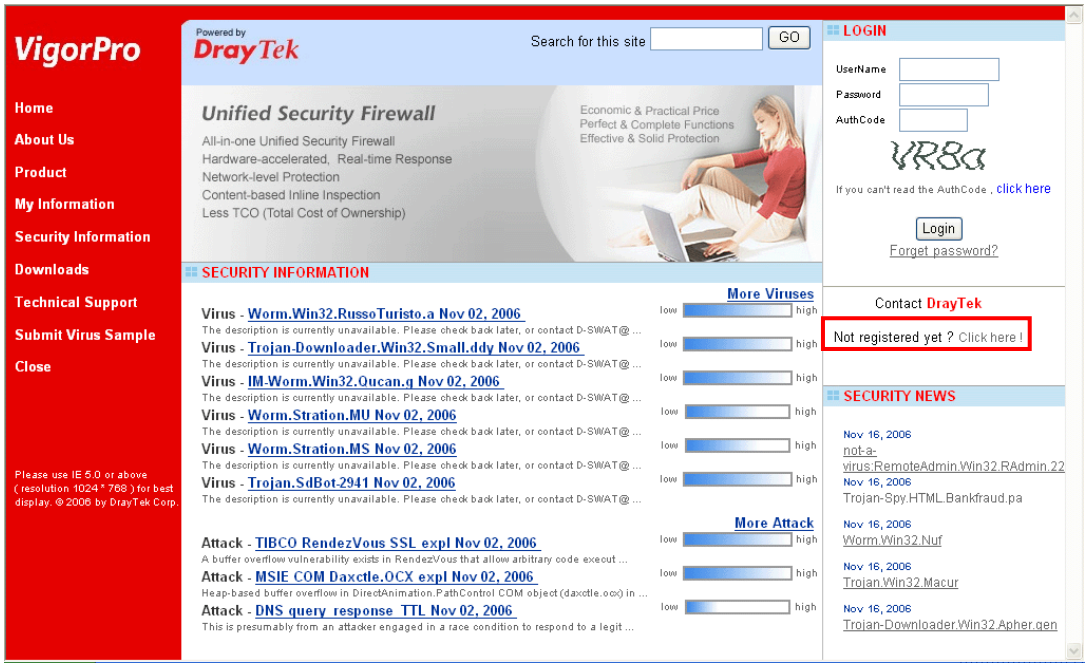
There are two ways to create and activate new account. One is created by accessing www.vigorpro.com (refer to section 4.1), the other is from router's web configurator (refer to section 4.2).

After activating the new account, you have to register your router from router's web configurator (refer to section 4.3). Follow the steps listed below to finish the registration and activation.

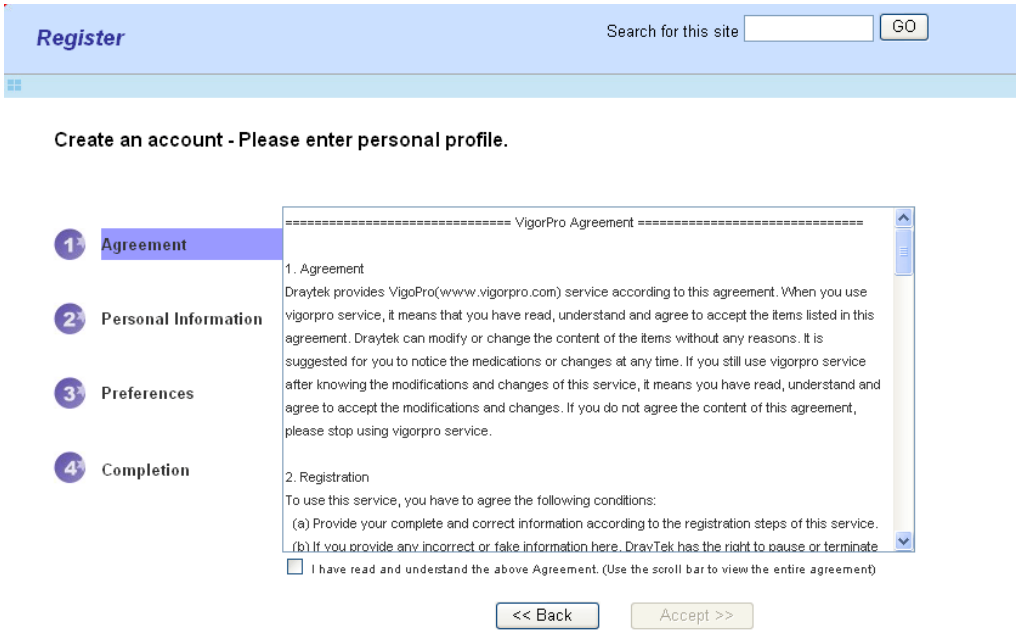
4.1 Creating and Activating an Account from VigorPro Website

To activate anti-virus/anti-intrusion function, you need to register an account on www.vigorpro.com firstly. Please follow the steps below to create a new account.

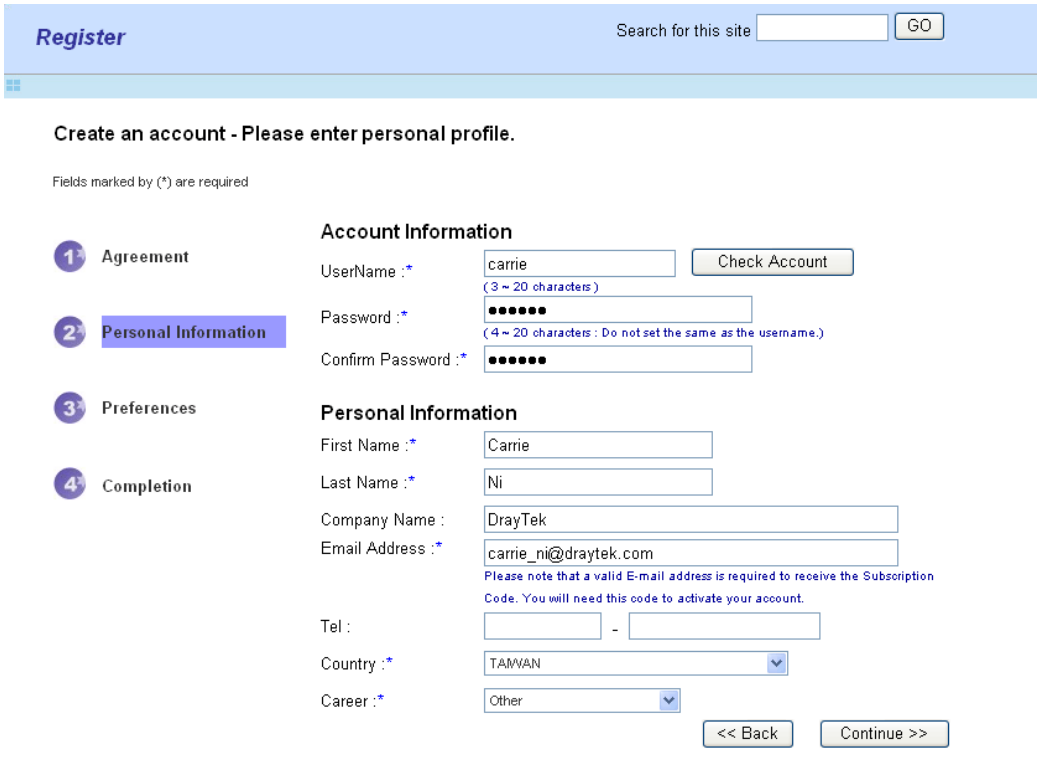
1. Open your browser with URL: **www.vigorpro.com**. Find the line of **Not registered yet?**. Then, click the link **Click here!** to access into next page.



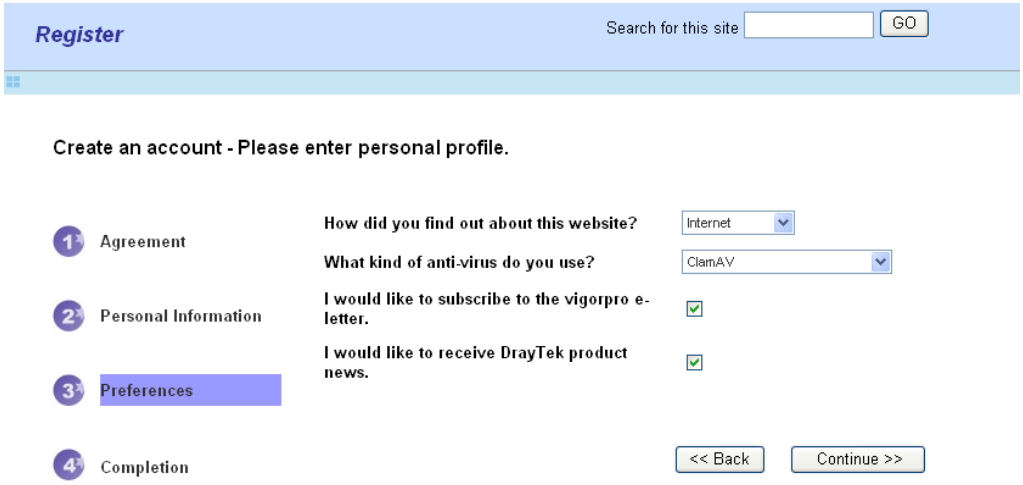
2. Check to confirm that you accept the Agreement and click **Accept**.



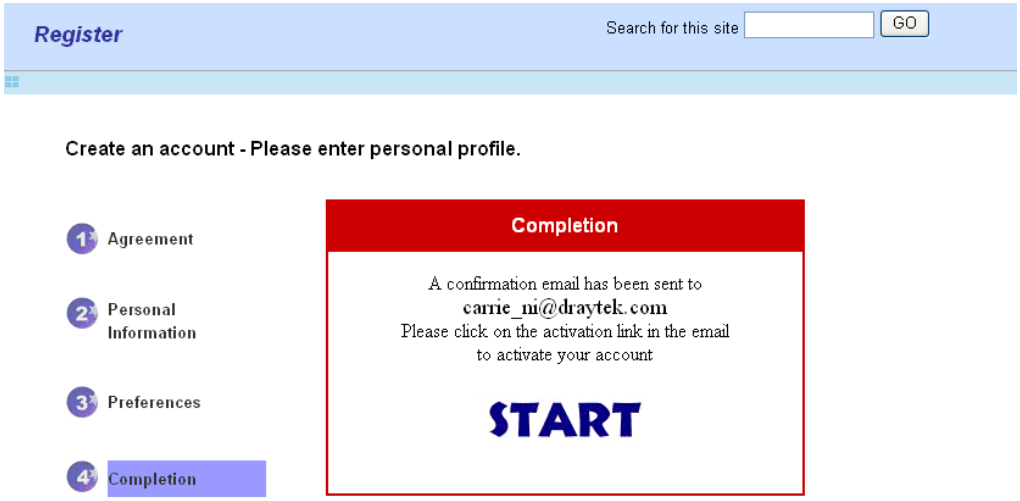
3. Type your personal information in this page and then click **Continue**.



4. Choose proper selection for your computer and click **Continue**.



5. Now you have created an account successfully.



6. Check to see the confirmation email with the title of **New Account Confirmation Letter from www.vigorpro.com**.

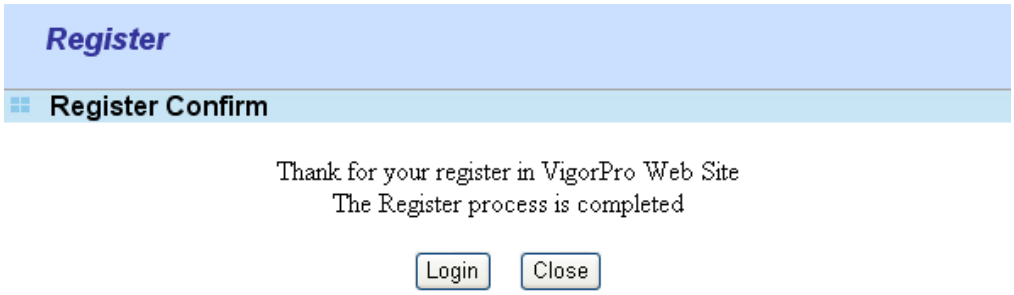
****** This is an automated message from www.vigorpro.com. ******

Thank you (carrie) for creating an account.

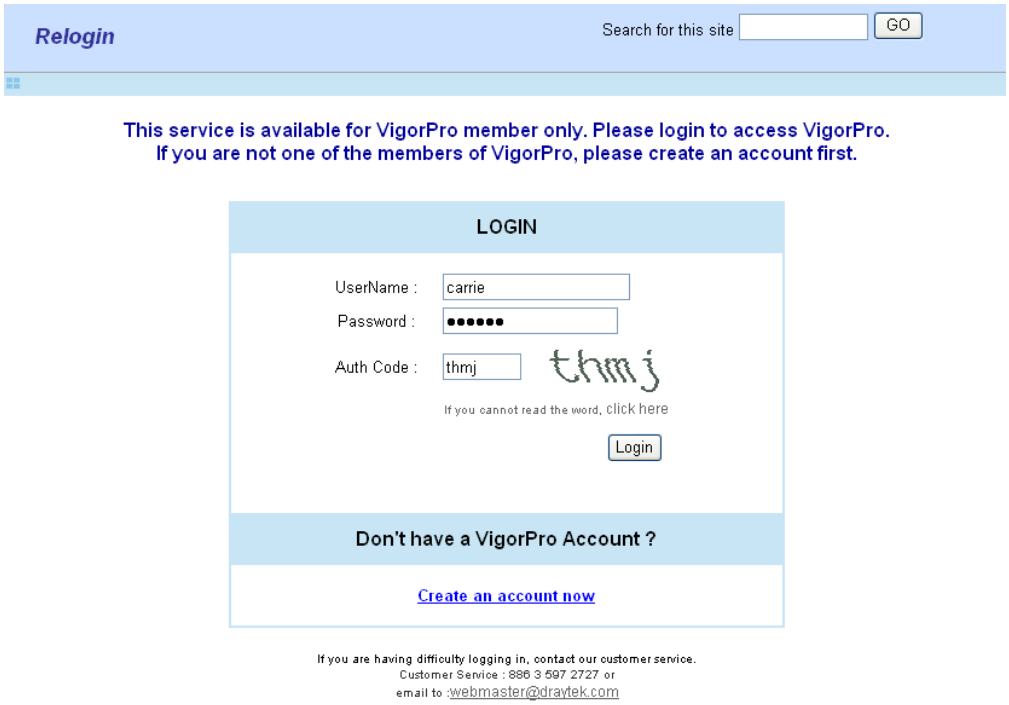
Please click on the activation link below to activate your account

Link : Activate my Account

7. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.



8. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**. Then type the code in the box of AuthCode according to the value displayed on the right side of it.

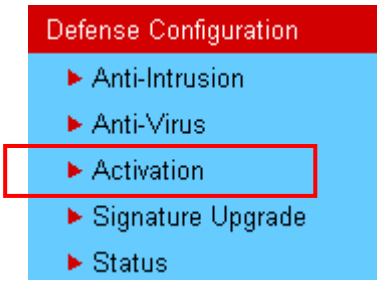


9. Now, click **Login**. Your account has been activated.

4.2 Creating and Activating an Account from Router Web Configurator

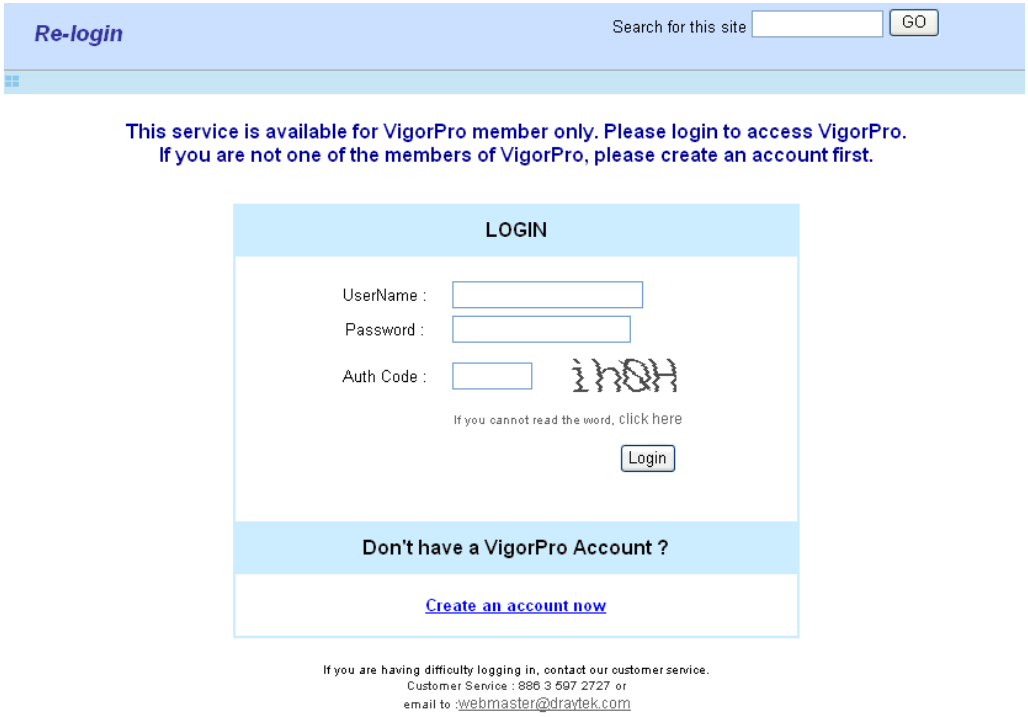
You, also can created and register a new account from the web configurator of the VigorPro router.

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. Do not type any word on the window and click **OK**.
2. From the router's web page, please open **Defense Configuration >>Activation**. You will see the following web page.

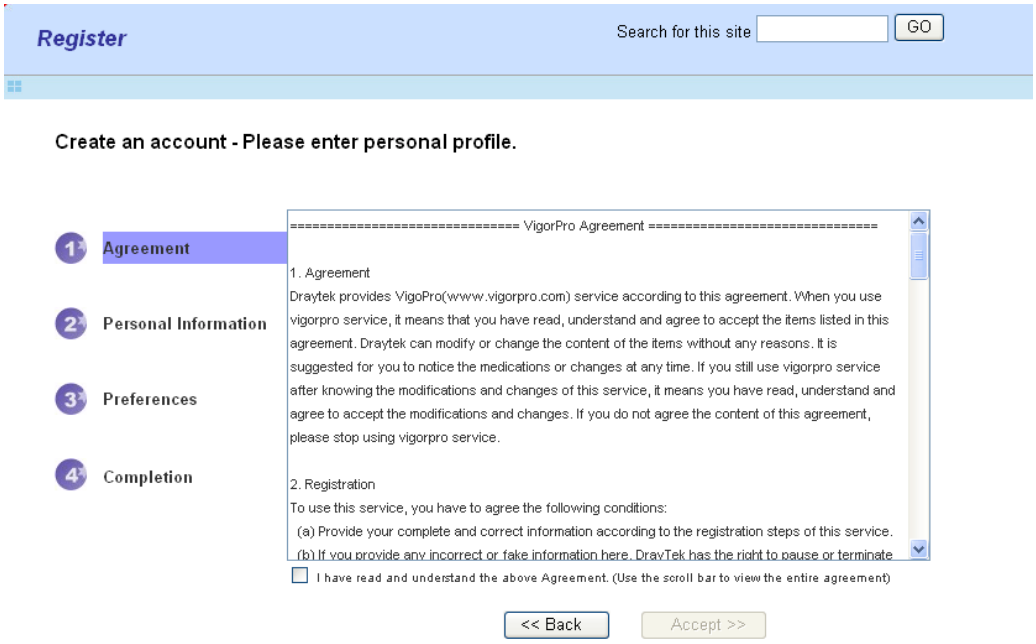


3. Click the **Activate** link from the **Activation** web page.

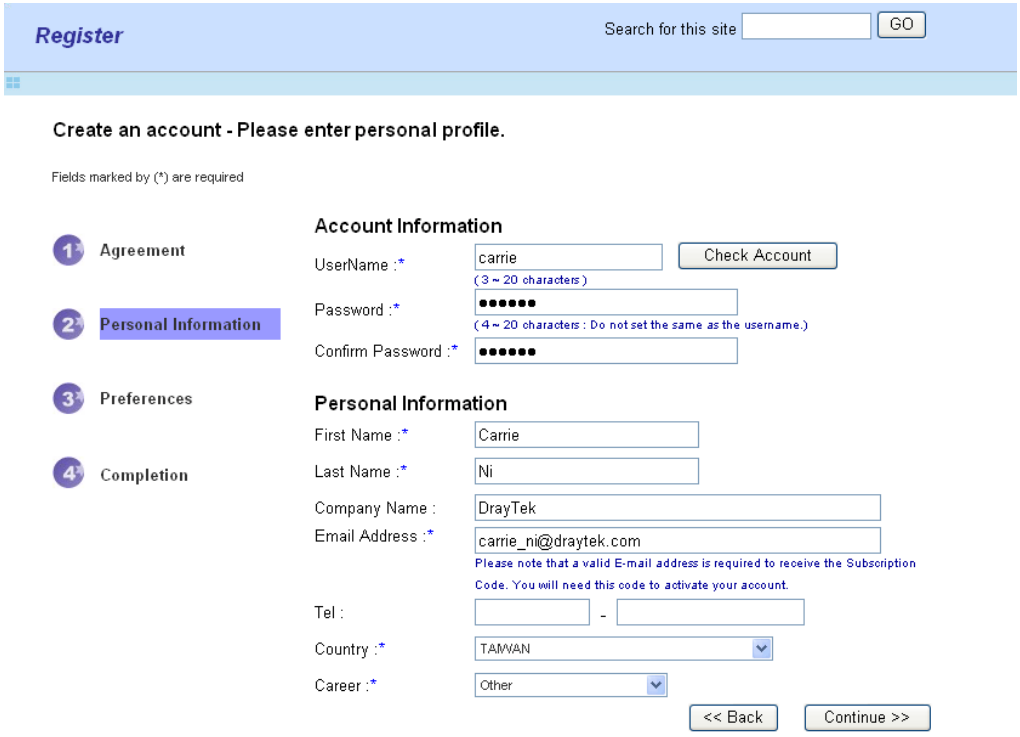
4. A **Re-login** page will be shown on the screen.



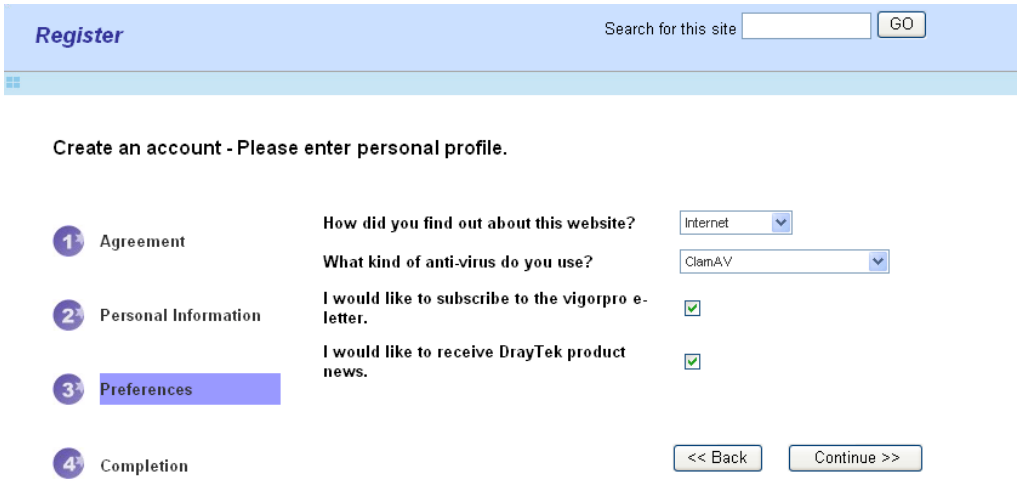
5. Locate and click **Create an account now link** on the bottom of this page. You will access into the following page. Check the box below to confirm that you accept the Agreement and click **Accept**.



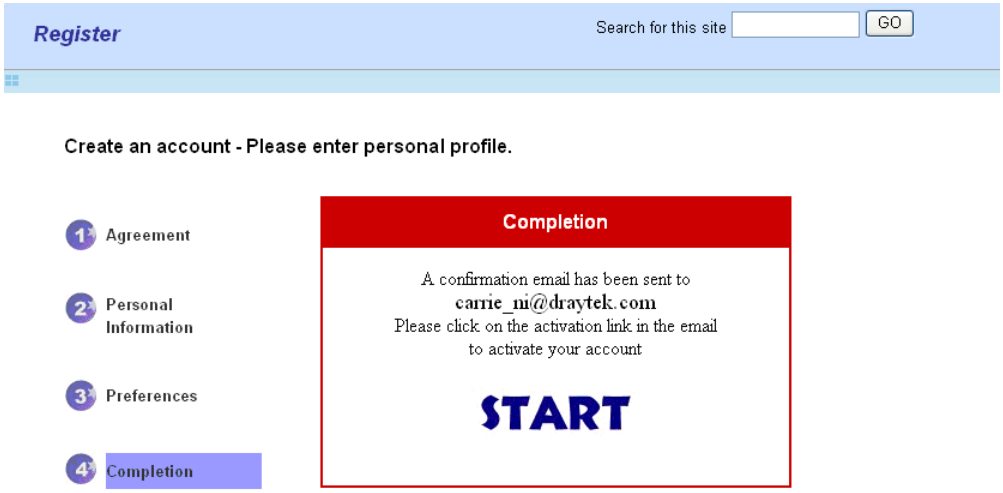
6. Type your personal information in this page and then click **Continue**.



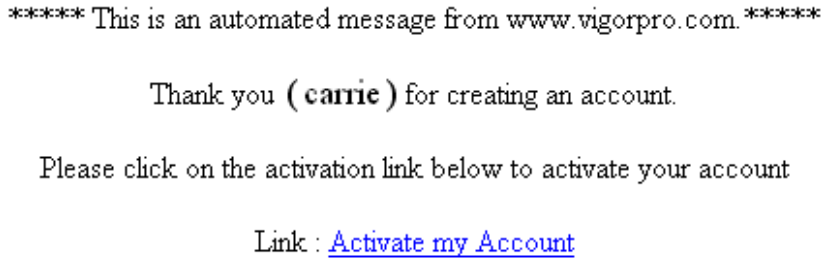
7. Choose proper selection for your computer and click **Continue**.



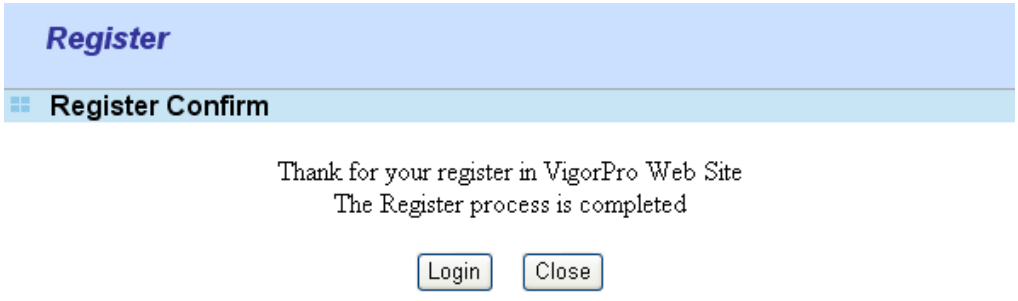
8. Now you have created an account successfully.



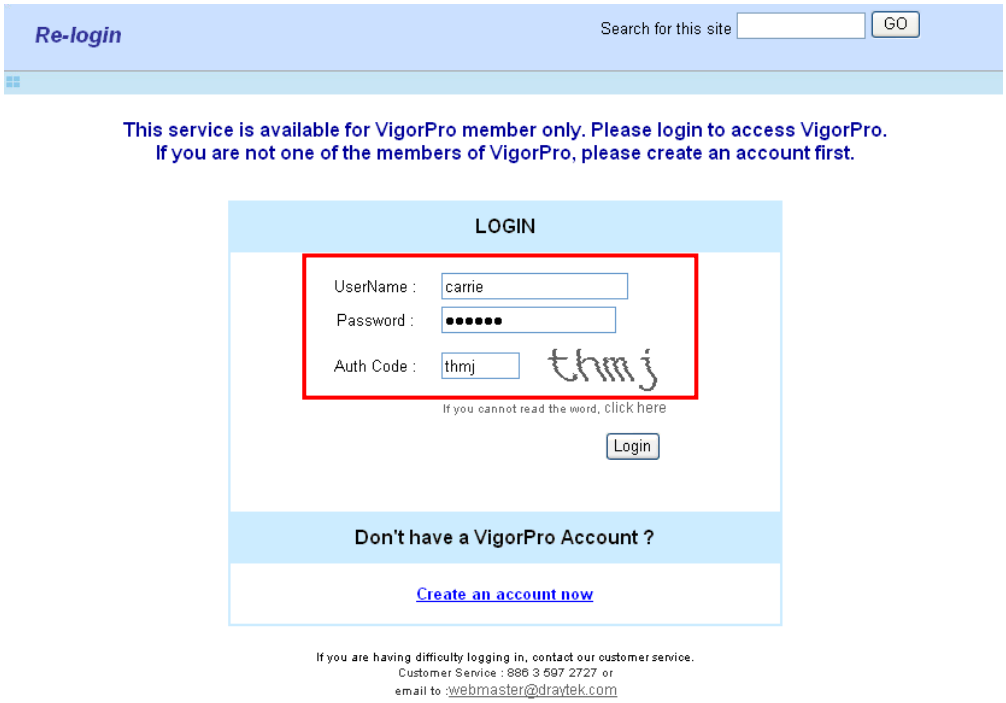
9. Check to see the confirmation email with the title of **New Account Confirmation Letter from www.vigorpro.com**.



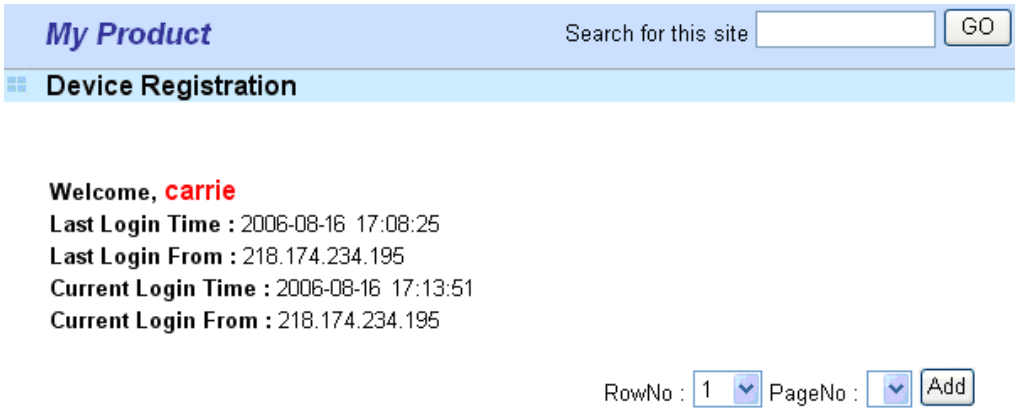
10. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.



11. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**. Then type the code in the box of AuthCode according to the value displayed on the right side of it.



12. Now, click **Login**. Your account has been activated. And the following page will be shown automatically.



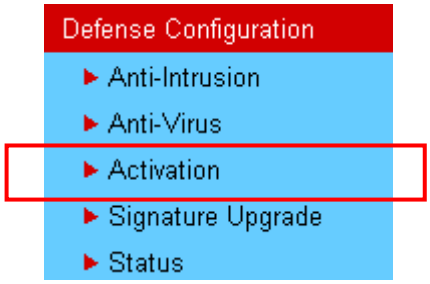
DrayTek will maintain a database of MAC address/serial number of shipped goods. Only products with shipping records can be registered. If your VigorPro 5510 cannot hook up to your account, please contact your reseller or DrayTek's technical support.

4.3 Registering Your Vigor Router

You have activated the new account for the router. Now, it is the time for you to register your vigor router. Open **Defense Configuration >>Activation.** Registering Vigor router should be done just for once. **If the router has been registered previously, the system will not allow you to register the router again.** After finishing the router registration, you can activate Anti-Virus and Anti-Intrusion respectively.

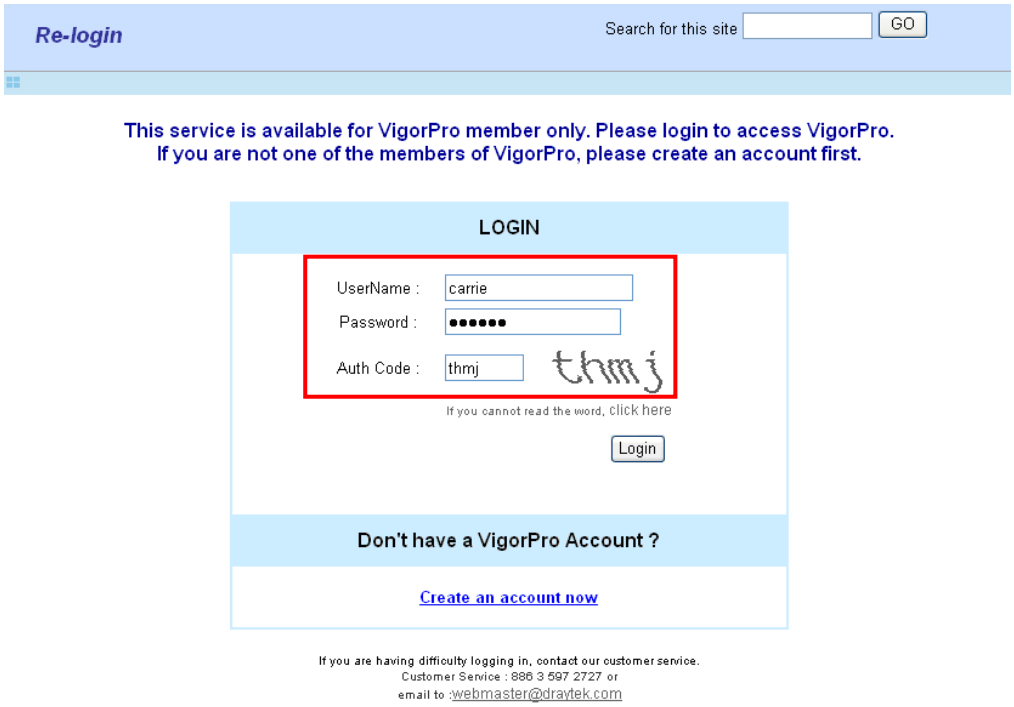
1. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for username and password. Do not type any word on the window and click **OK**.

2. From the router's web page, please open **Defense Configuration >>Activation**. You will see the following web page.

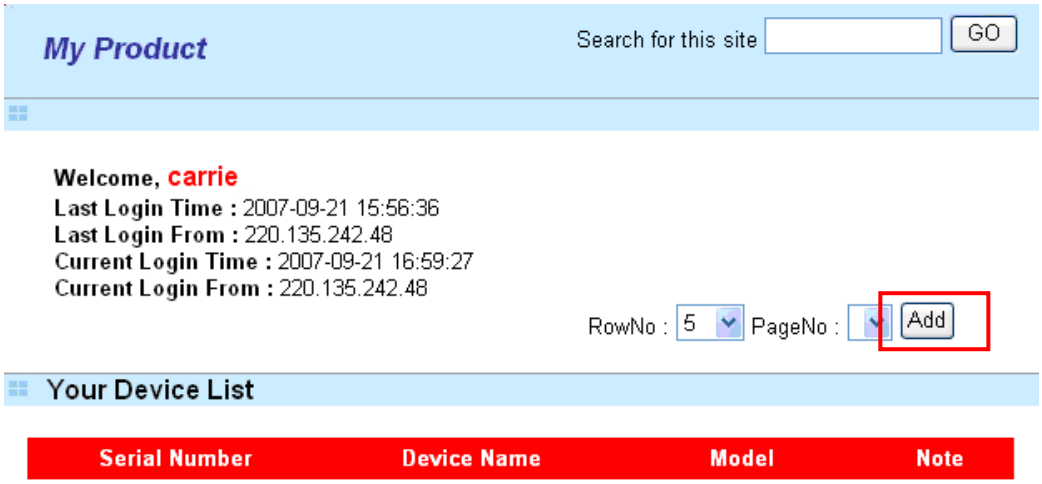


3. Click any he **Activate** link from the **Activation** web page.

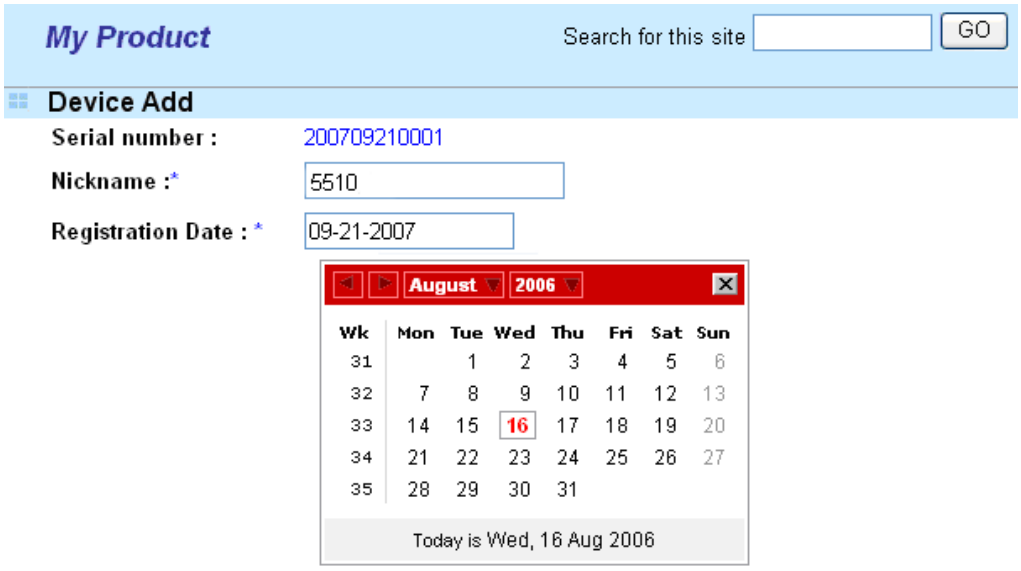
4. A **Re-login** page will be shown on the screen. Please type the account and password that you created previously. And click **Login**.



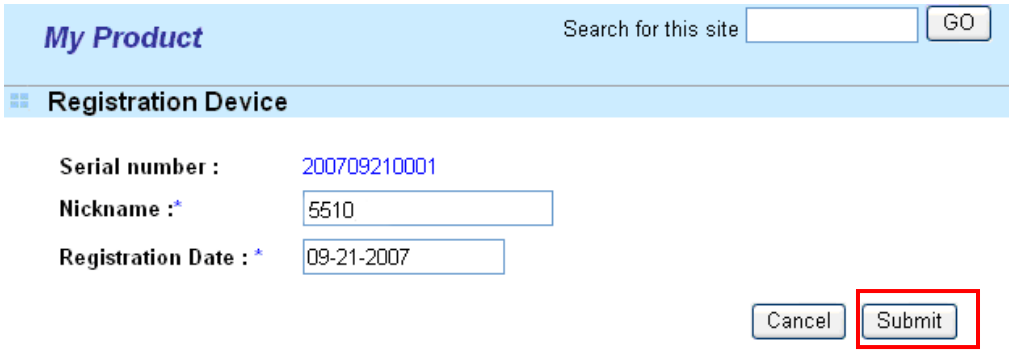
5. The following page will be displayed after you logging in VigorPro server. From this page, please click **Add**.



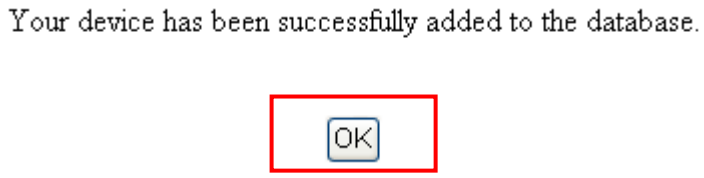
6. When the following page appears, please type in Nick Name (for the router) and choose the right purchase date from the popup calendar (it appears when you click on the box of Purchase Date).



7. After adding the basic information for the router, please click **Submit**.



8. Now, your router information has been added to the database. Click **OK** to leave this web page and return to **My Product** web page.

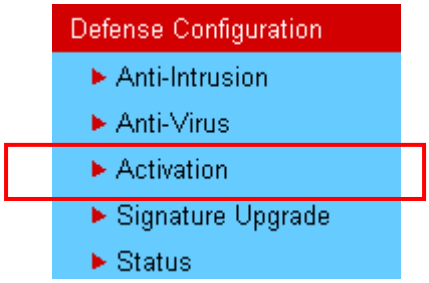


Now, you have finished the procedure for registering your router.

4.4 Activating Anti-Virus/Anti-Intrusion Service

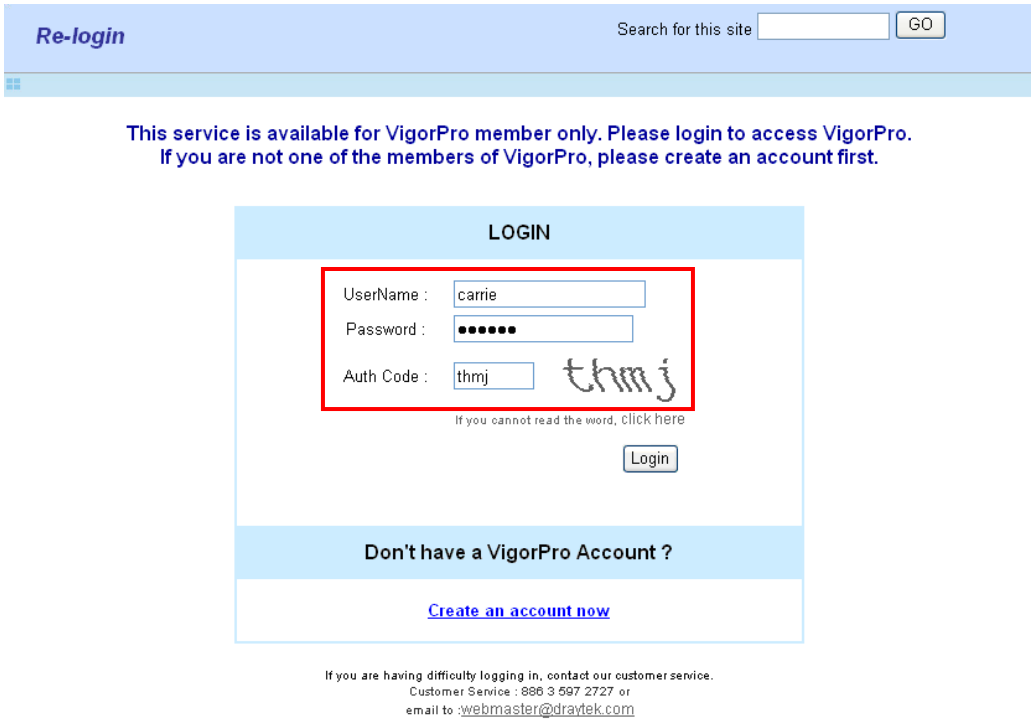
After registering your vigor router, you have to follow the steps listed below to activate anti-virus/anti-intrusion service to obtain full security for your computer.

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. From the router's web page, please open **Defense Configuration >>Activation**. You will see the following web page.

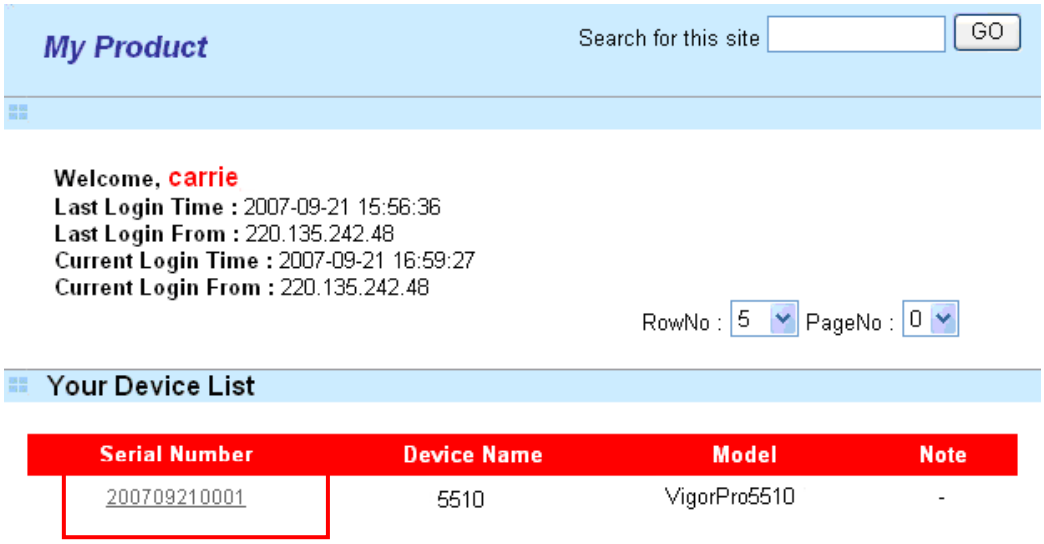


3. Click the **Activate** link to activate Anti-Intrusion/Anti-Virus service.

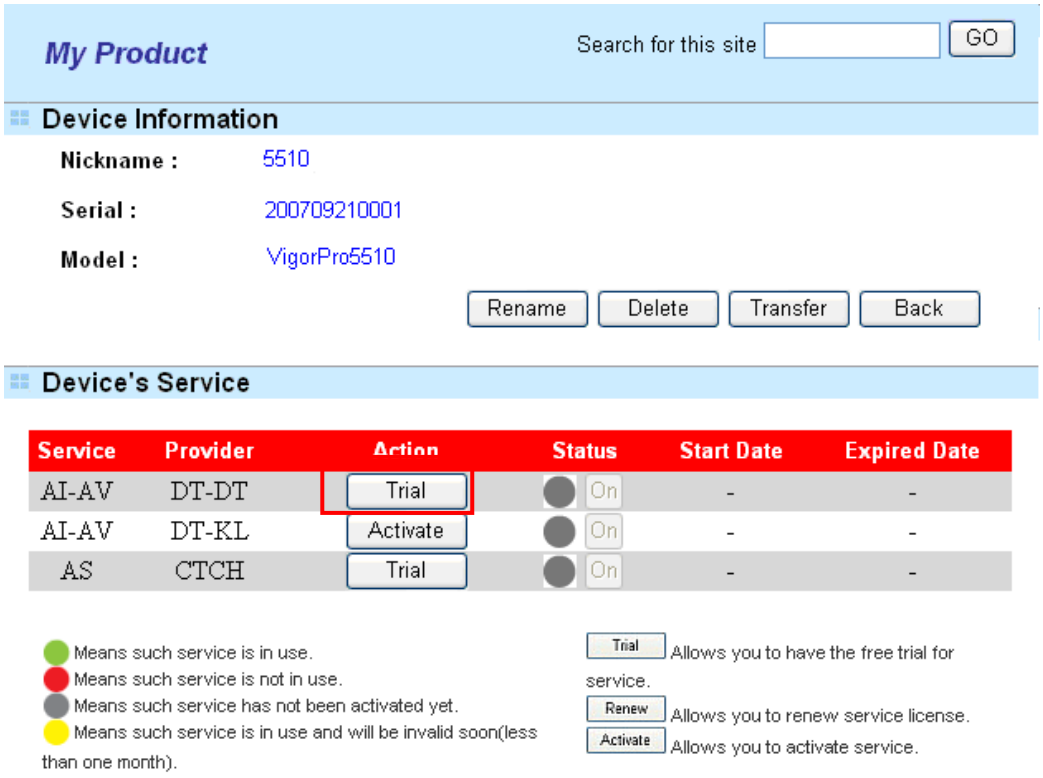
4. A **Re-login** page will be shown on the screen. Please type the account and password that you created previously. And click **Login**.



5. On the web page of **My Product**, you can find a list of the devices that you add with the above steps. Currently, you just have added VigorPro 5510. Please click the serial number link.

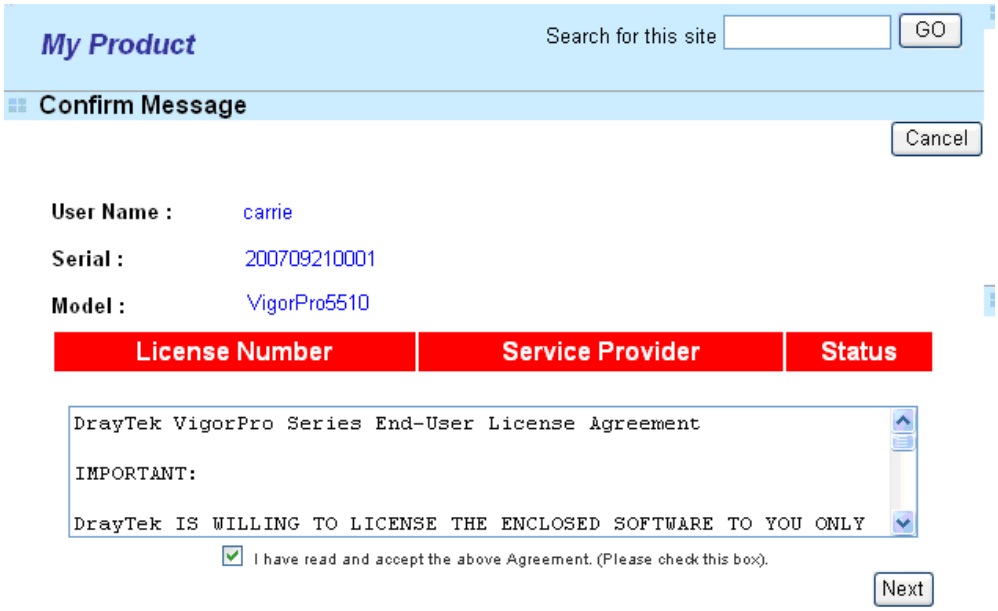


6. From the **Device's Service** section, click the **Trial** button for AI-AV (Anti-Intrusion & Anti-Virus) service with provider **DT-DT**.



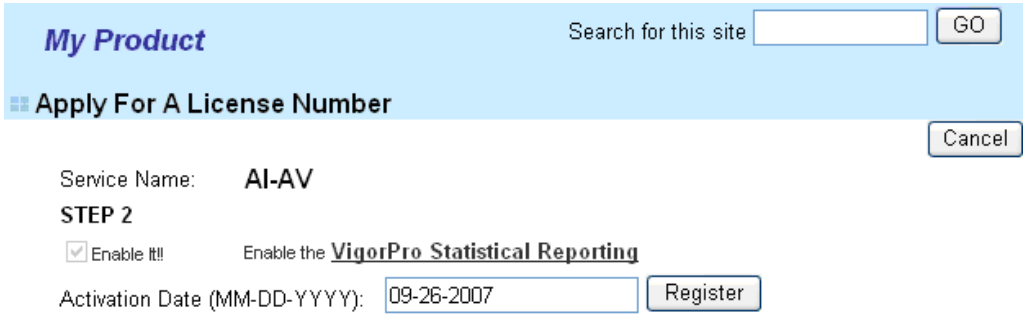
Rename	It allows you to change the account name.
Delete	It allows you to delete account name used currently.
Transfer	It allows you to transfer the VigorPro device together with applied license to someone who has already registered another account in www.vigorpro.com. Be sure to press this button to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

7. 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**.



Note: DT-DT means you can acquire the anti-intrusion and anti-virus services from DrayTek Corporation.

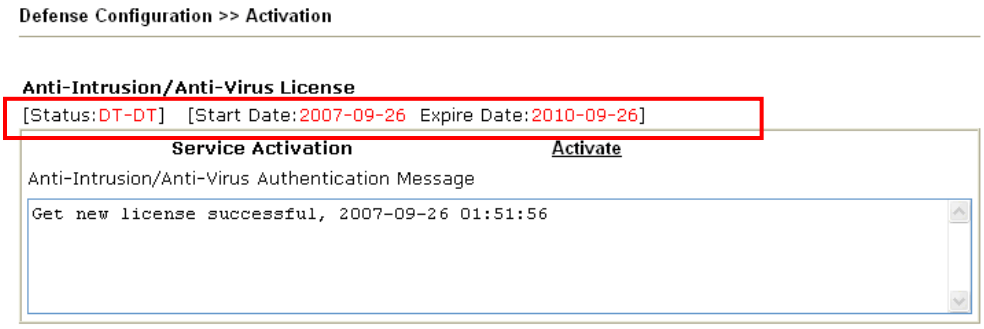
8. When this page appears, click **Register**.



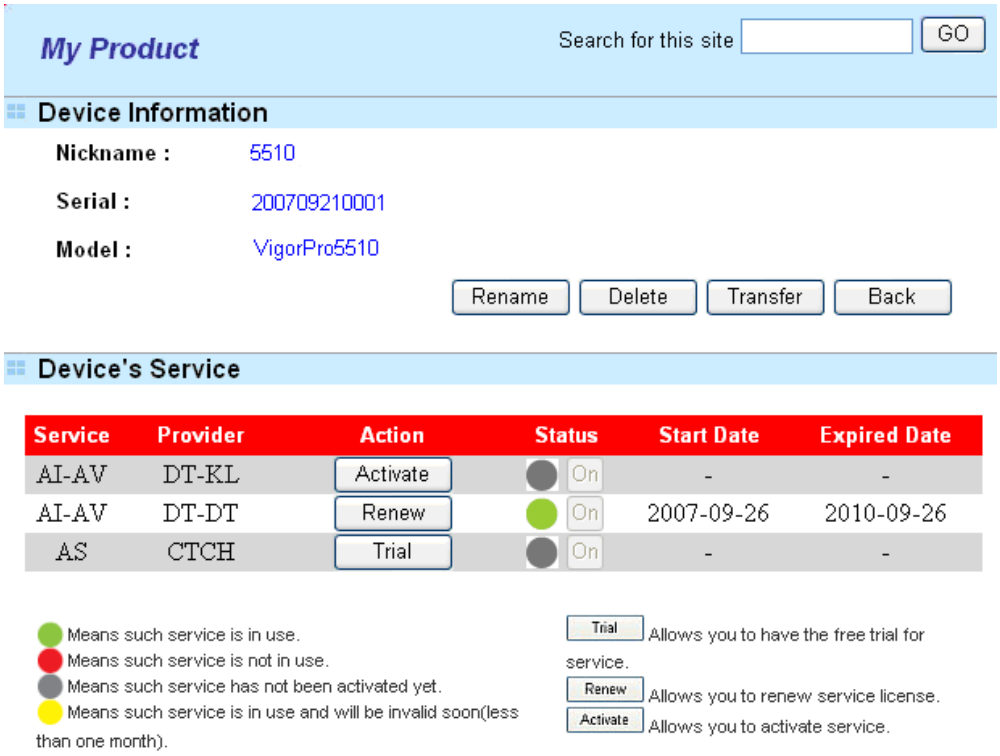
9. Next, the DrayTek Service Activation screen will be shown as the following:

10. Click **Close**.

11. Open **Defense Configuration>>Activation** page of the router's web configurator. The start date and expire date for the license are shown in this page.



12. Click **Activate** to access into VigorPro website again. Open the following page. You will see the AI-AV (with provider DT-DT) has been activated and in use.



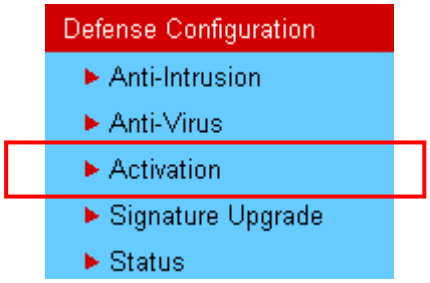
Now, you have finished Anti-Intrusion/Anti-Virus configuration.

4.5 Applying a New License for Anti-Intrusion/Anti-Virus

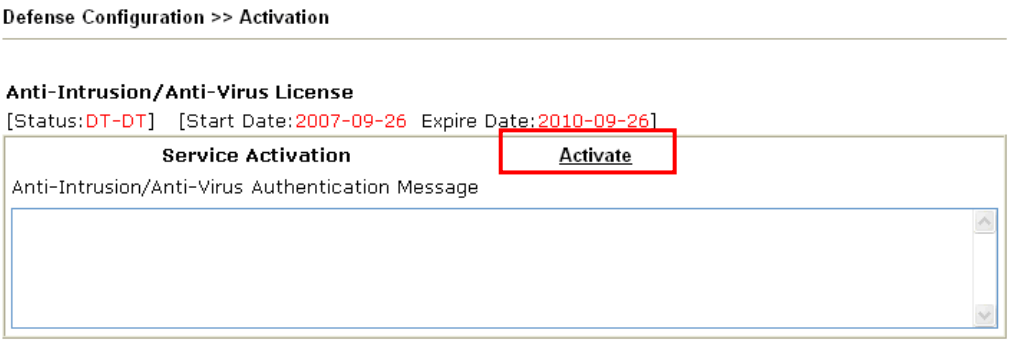
When thirty days for free of charge expires, you can apply for a new license by following the steps below:

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. Do not type any word on the window and click **OK**.

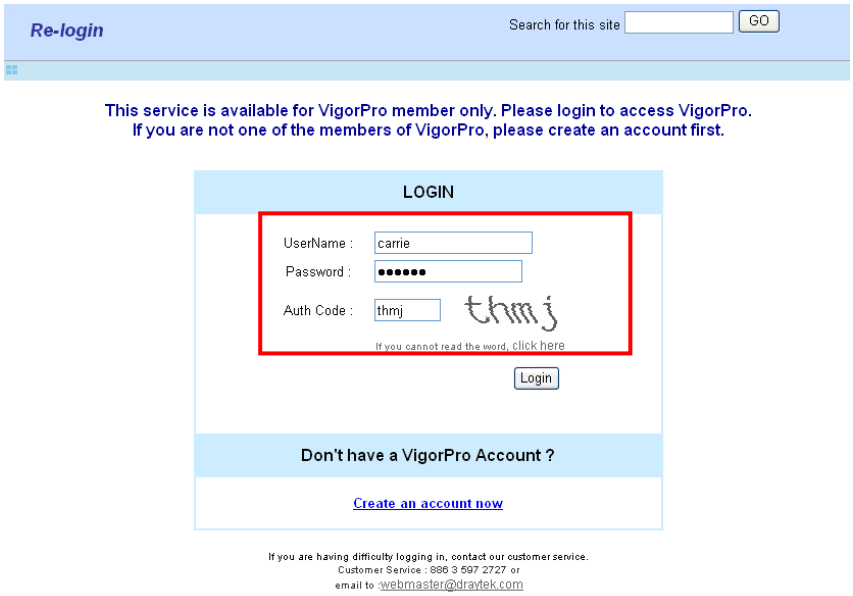
2. From the router's web page, please open **Defense Configuration >>Activation**. You will see the following web page



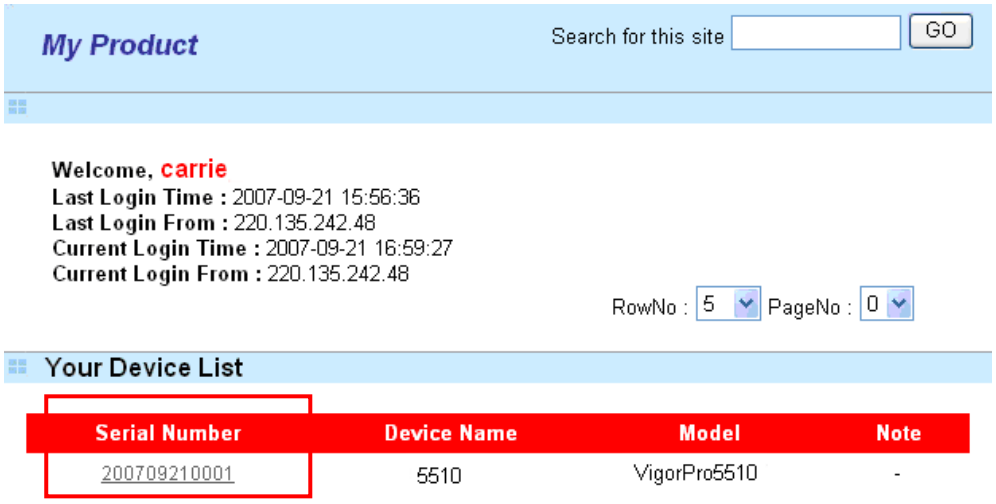
3. Click the **Activate** link.



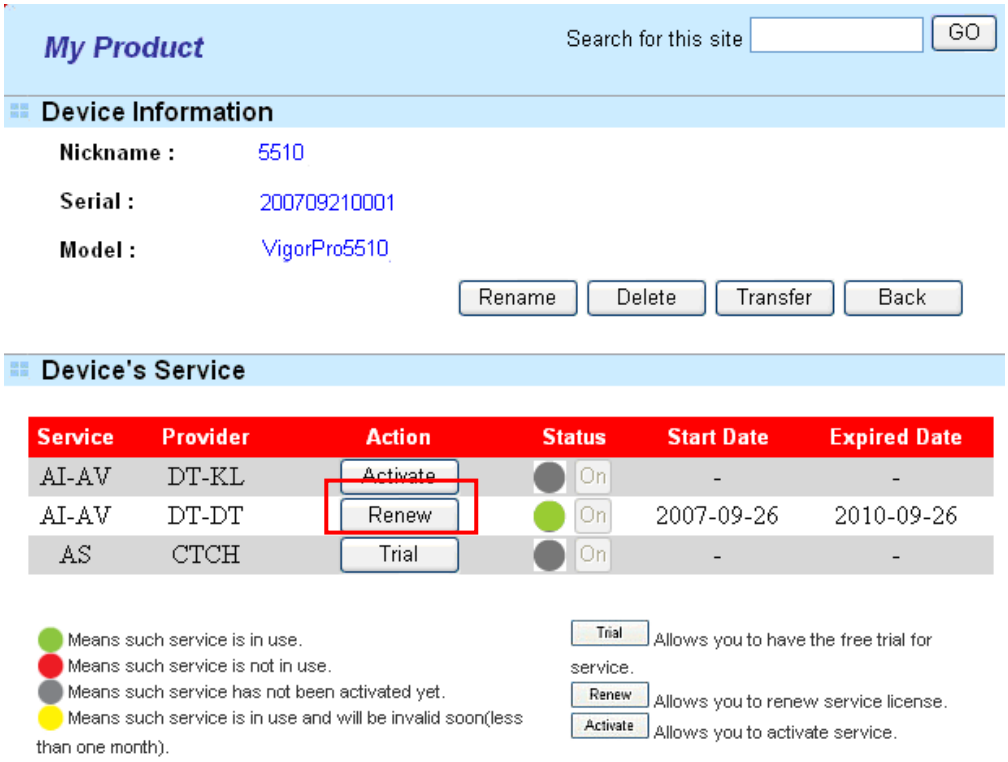
4. A **Re-login** page will be shown on the screen. Please type the account and password that you created previously. And click **Login**.



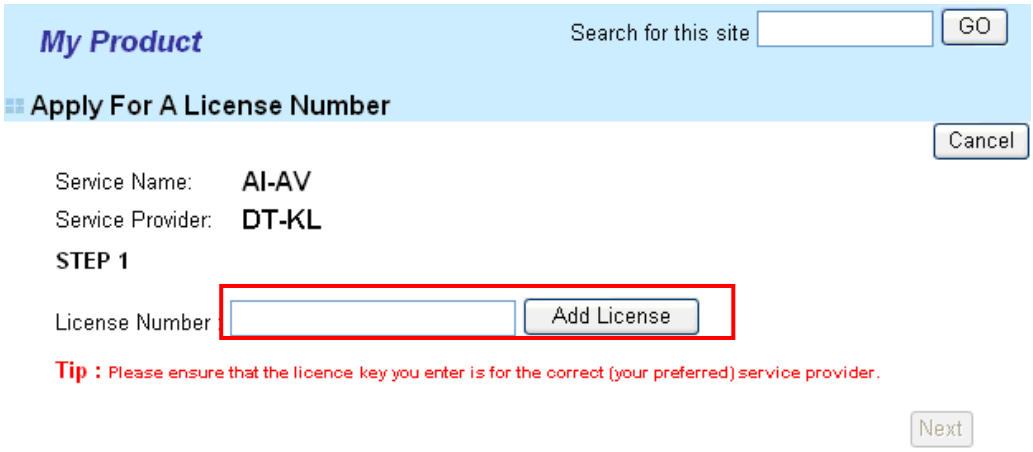
5. On the web page of **My Product**, you can find a list of the devices that you add with the above steps. Currently, you just have added VigorPro 5510. Please click the serial number link.



6. From the **Device's Service** section, click the **Renew** button for AI-AV (Anti-Intrusion & Anti-Virus) service (service provider is DT-DT).

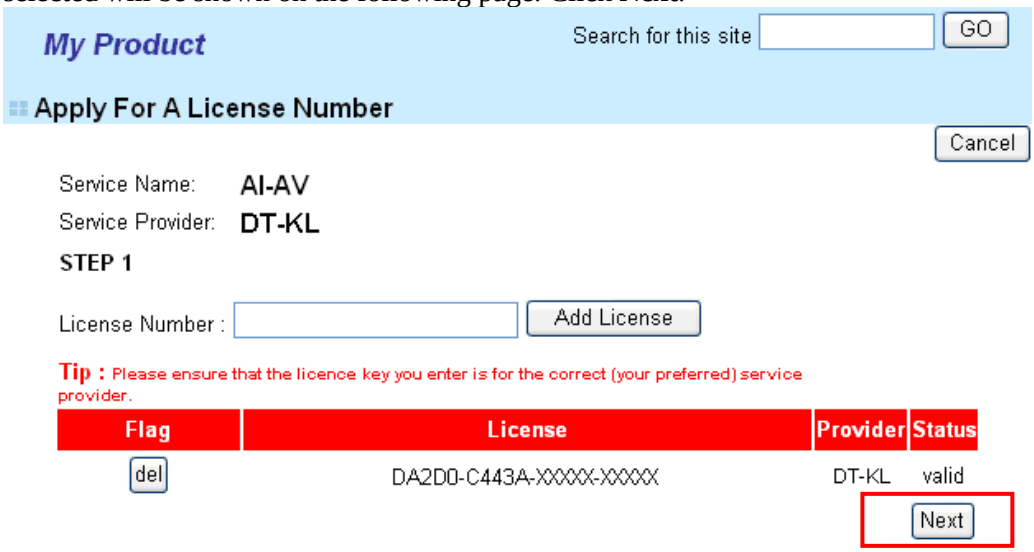


7. In the following page, please type in license number shown on the License Key card. Enter the number and click **Add License.**

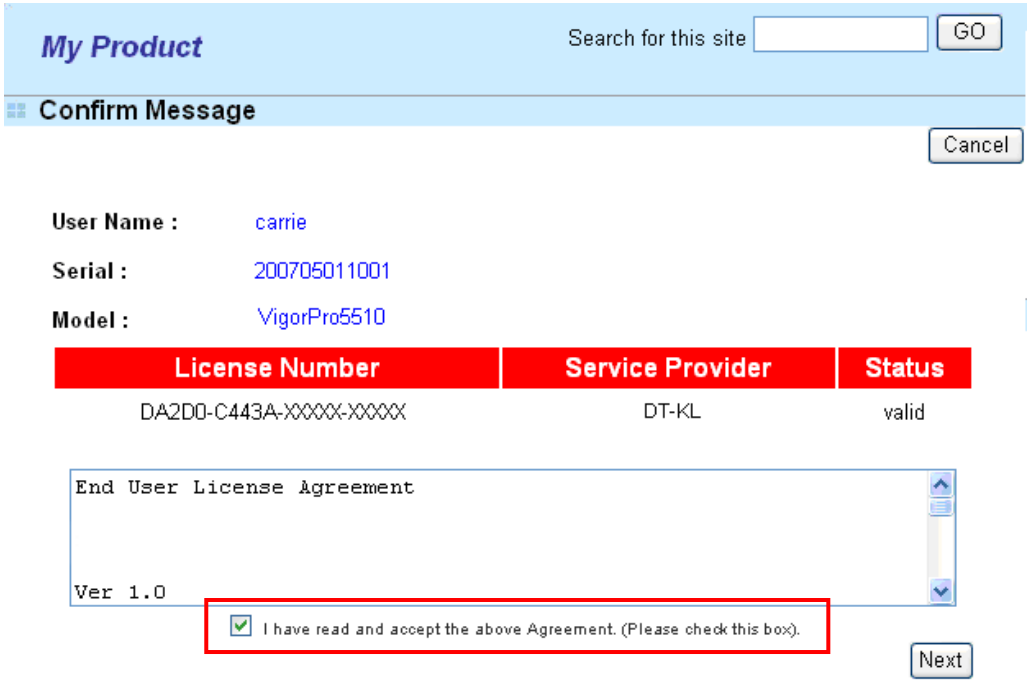


Note: DT-KL allows you to acquire the anti-intrusion service from DrayTek and anti-virus service from Kaspersky. DT-DT allows you to acquire the anti-intrusion and anti-virus services from DrayTek Corporation.

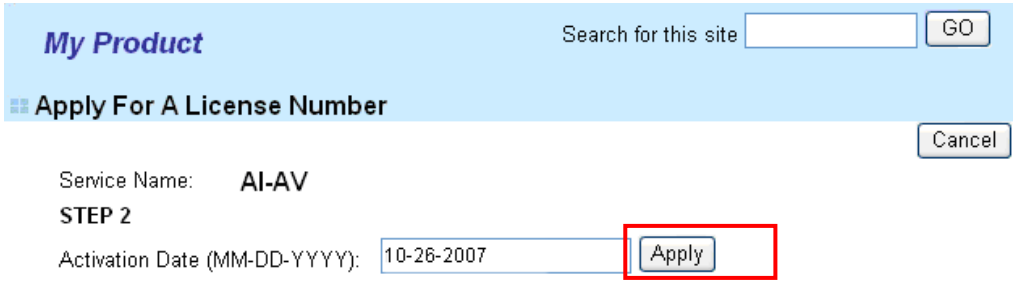
8. After typing the license key, click **Add License**. The basic information for the one you selected will be shown on the following page. Click **Next**.



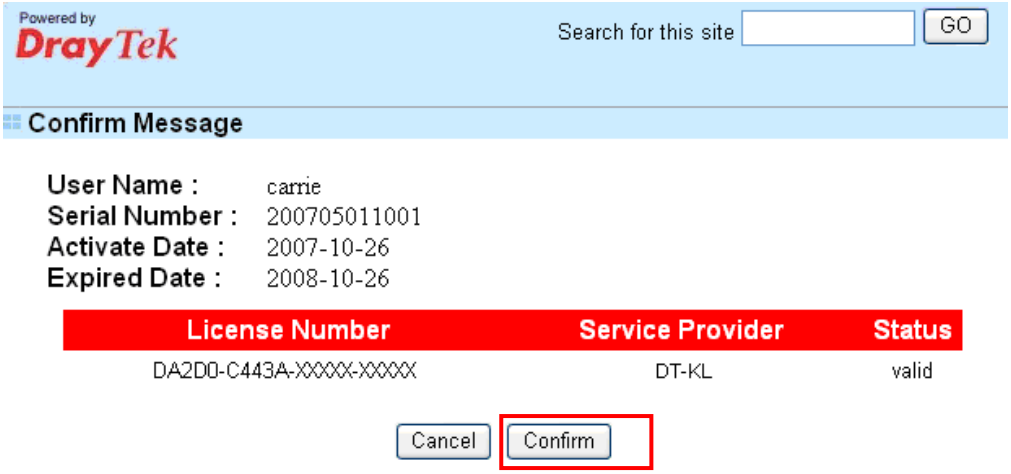
9. Check the box of "**I have read and accept the above Agreement**" and click **Next**.



10. When this page appears, click **Apply**.



11. Confirm Message window will appear for you to make a confirmation. Click **Confirm**.



12. The Service Activation screen will be shown as the following.

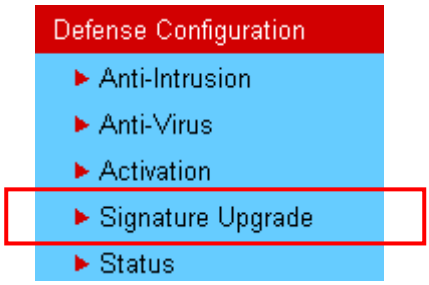
13. Click **Close**.

Return to **Defense Configuration>>Status** page of the router's web configurator. The start date and expire date for the license will be shown in this page.

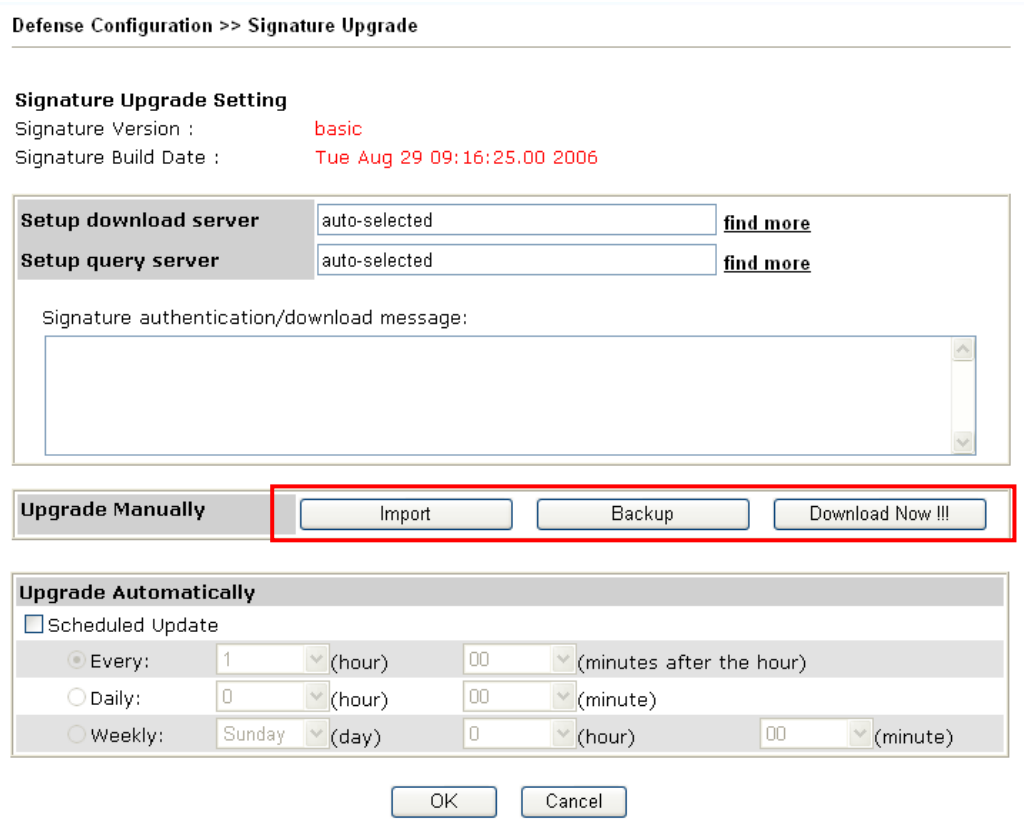
4.6 Backup and Upgrade Signature for Anti-Intrusion/Anti-Virus

You can get the most updated signature from DrayTek's server if the license key of anti-virus/anti-intrusion for the VigorPro 5510 is not expired. Before you upgrade the signature, please check the validation information either from WEB user interface of VigorPro 5510 or account information from www.vigorpro.com.

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. Do not type any word on the window and click **OK**.
2. From the router's web page, please open **Defense Configuration >>Signature Upgrade**. You will see the following web page.



3. On Signature Upgrade web page, locate Backup and Download Now!!!.



Time for Backup

Before changing other license, it is suggested for you to backup the original signature first. To backup current signature with the filename vigorpro.sig, click **Backup**.

Time for Download

After changing other license, it is suggested for you to download newly update signature for your router. To download newly update anti-intrusion and anti-virus from VigorPro website, please click **Download Now!!!**.

Time for Import

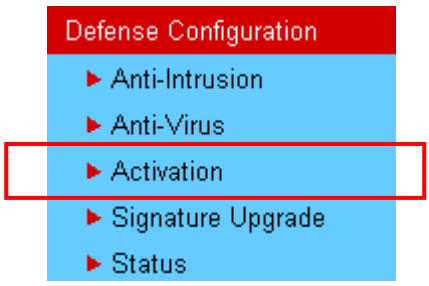
Backup files can be imported whenever you want. To use a saved signature information, please click **Import**.

In addition, users can specify certain time for executing the upgrade automatically by the router. Remember to check the **Schedule Update** box and click **OK** to activate the time settings.

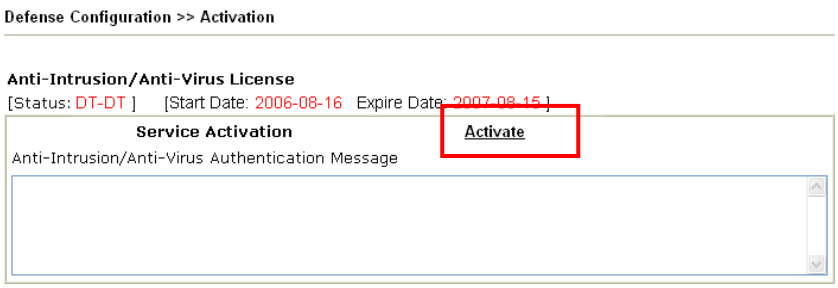
4.7 Switching between DT-DT and DT-KL

You can change anti-virus and anti-intrusion service between DT-DT and DT-KL service provider whenever you want. Simply follow the steps below:

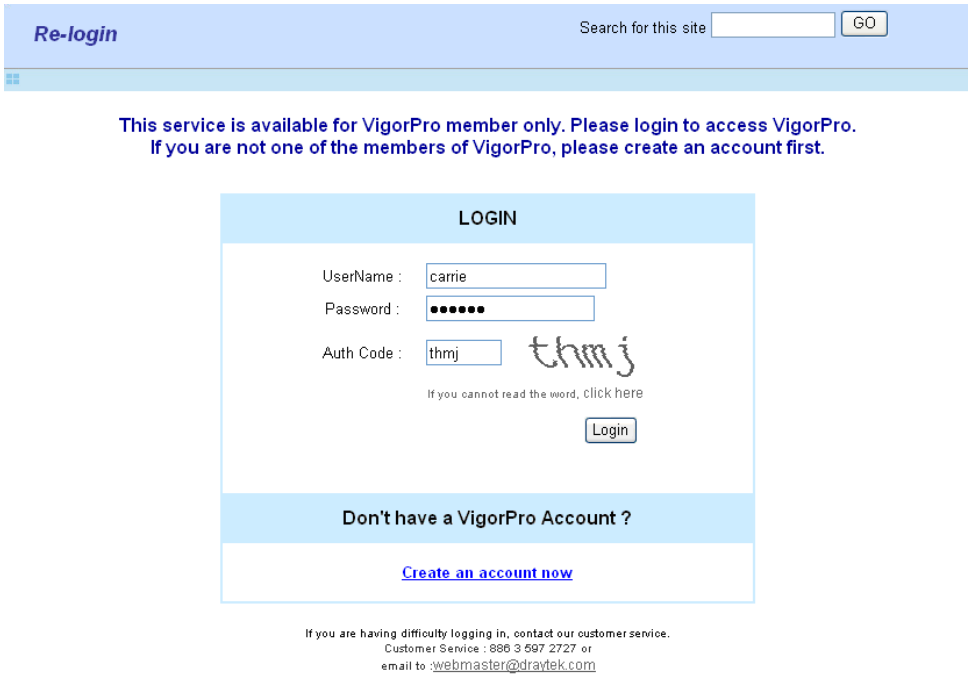
1. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for username and password. Do not type any word on the window and click **OK**.
2. From the router's web page, please open **Defense Configuration >>Activation**. You will see the following web page.



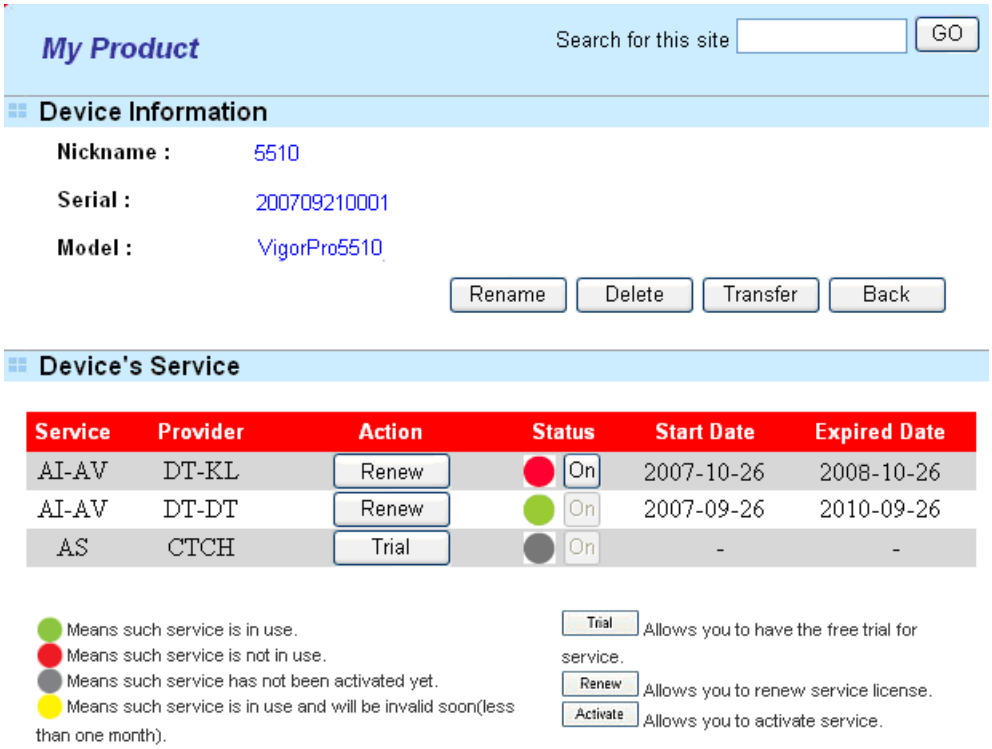
3. Click the **Activate** link from the **Defense Configuration >>Activation** web page. Remember that the license currently selected is DT-DT. Therefore, you can switch into DT-KL if you want.



4. A **Re-login** page will be shown on the screen. Please type new account and password that you created previously. And click **Login**.



5. The following page will be shown automatically. You will find there are two devices service added to your router. If you activated only one service before, it must be only one service displayed here. In this case, DT-DT and DT-KL services are activated on the VirgorPro website. However, DT-DT service is in use at present.



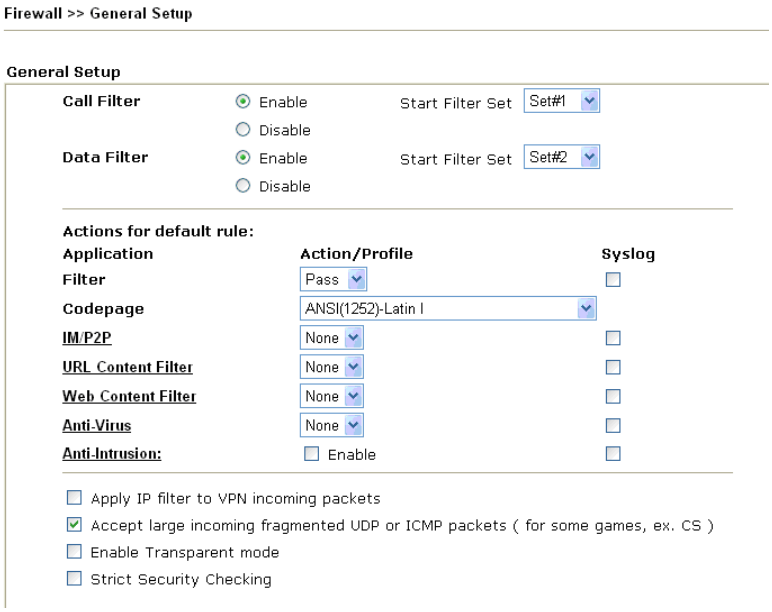
6. Click the **On** button on the line with DT-KL service to use that service. Then, the Status light for DT-DT service will be changed into red which means you can press on the **On** button for that one to use it for next time.

7. Now, you have successfully switched the service provider for your router.

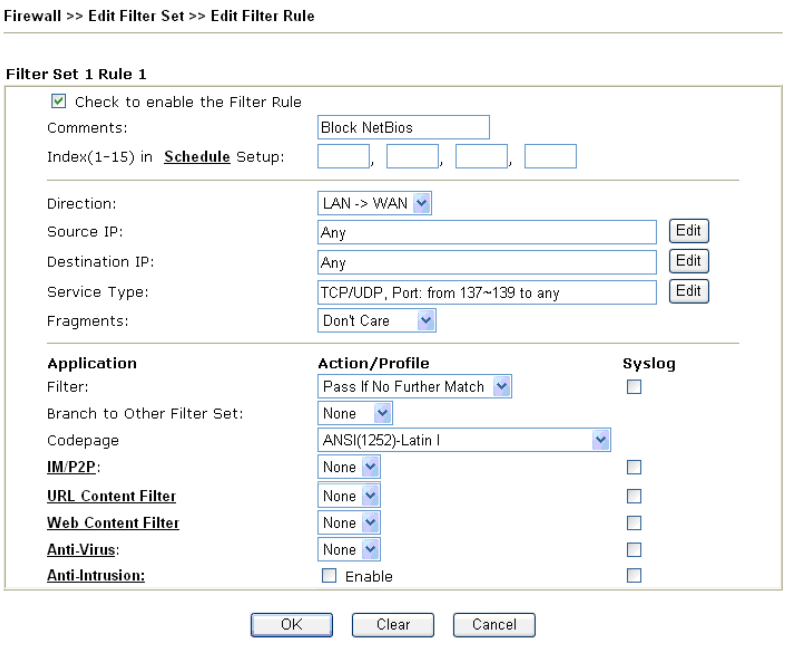
4.8 Enabling Anti-Virus/Anti-Intrusion

After applying an account, registering your account and router, you have to access into the web page of Vigor router to enable Anti-Virus/Anti-Intrusion functions. There are two ways to enable it.

A. For the default rule of firewall, please open **Firewall>>General Setup** page. Check the box of **Enable** for Anti-Intrusion and choose proper action (profile) from the drop down list of Anti-Virus. Next, click **OK** to finish the procedure of activation.



B. For specified filter rule (there are twelve filter sets in Firewall, and each set is allowed to set seven filter rules), please check the box of **Enable** for Anti-Intrusion and choose proper action (profile) from the drop down list of Anti-Virus. Next, click **OK** to finish the procedure of activation.

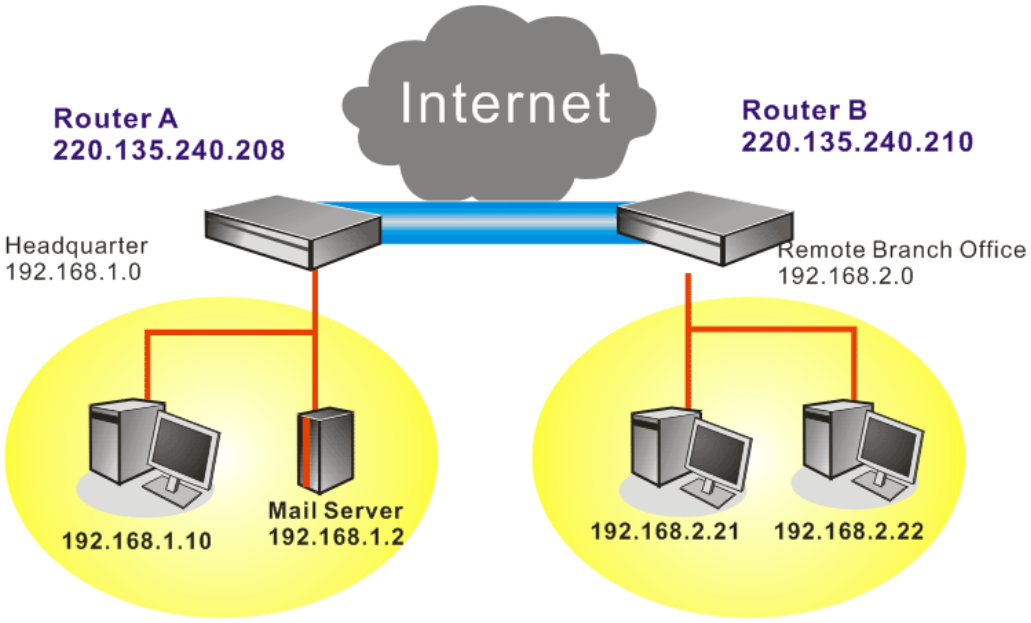


If you **did not** check the Anti-Intrusion box and choose a proper profile for Anti-Virus, you still **cannot use** the Anti-Intrusion/Anti-Virus function even if you finished all the relational profiles.

5 Application and Examples

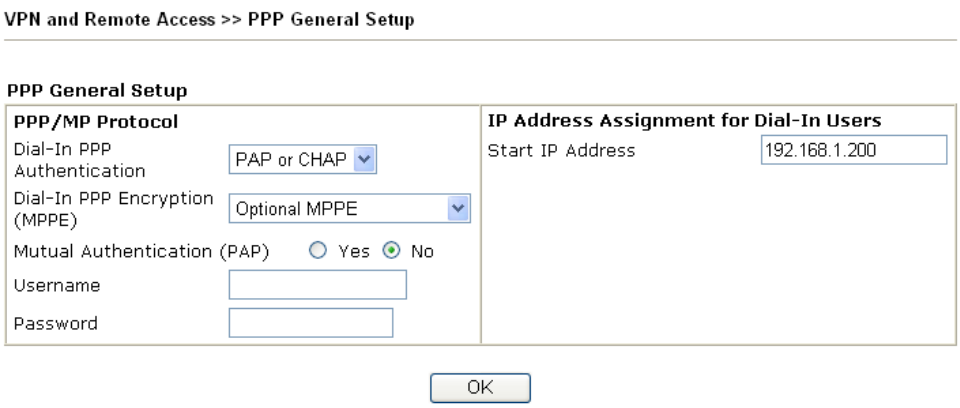
5.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter

The most common case is that you may want to connect to network securely, such as the remote branch office and headquarter. According to the network structure as shown in the below illustration, you may follow the steps to create a LAN-to-LAN profile. These two networks (LANs) should NOT have the same network address.

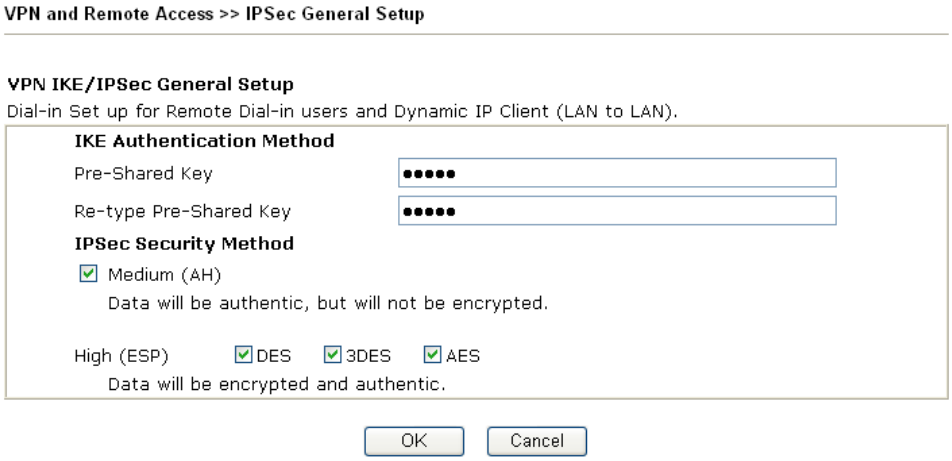


Settings in Router A in headquarter:

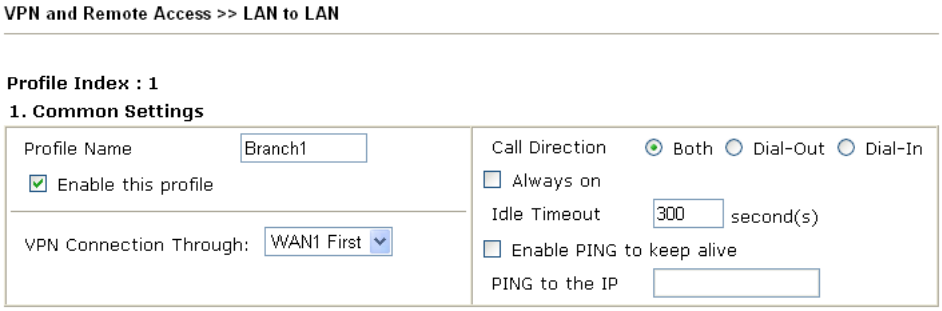
1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
2. Then,
   For using **PPP** based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.



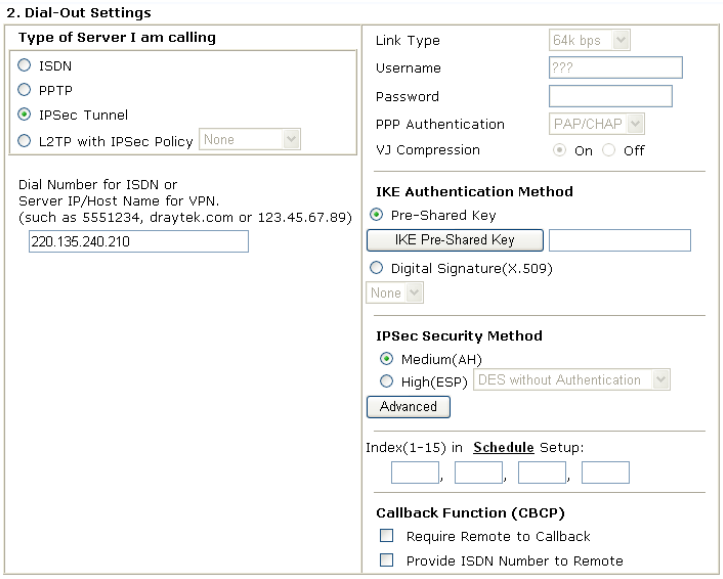
For using **IPSec**-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.



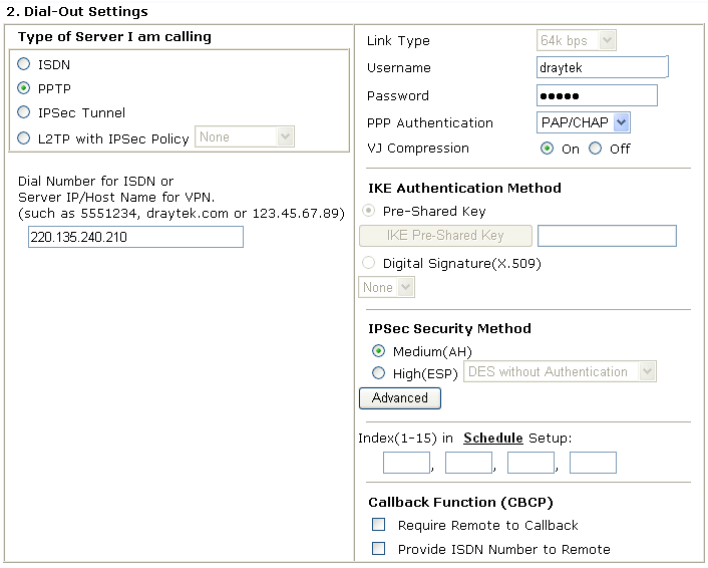
3. Go to **LAN-to-LAN**. Click on one index number to edit a profile.
4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.



5. Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.
   If an ***IPSec-based*** service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out connection.

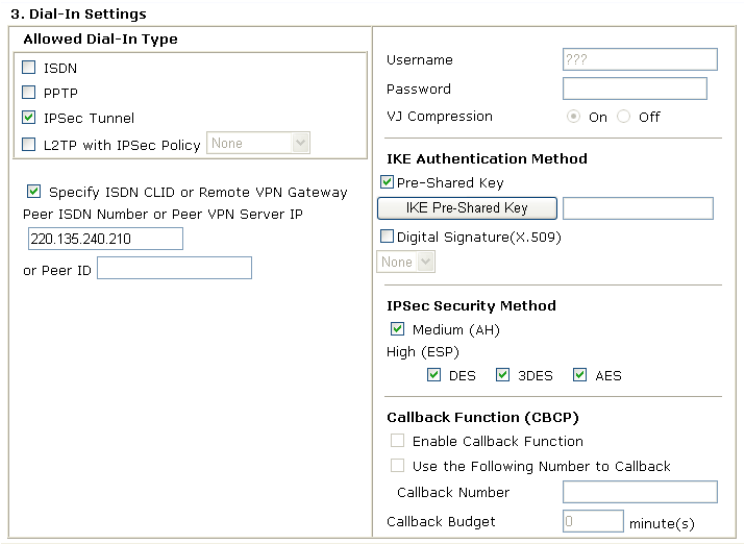


If a ***PPP-based service*** is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

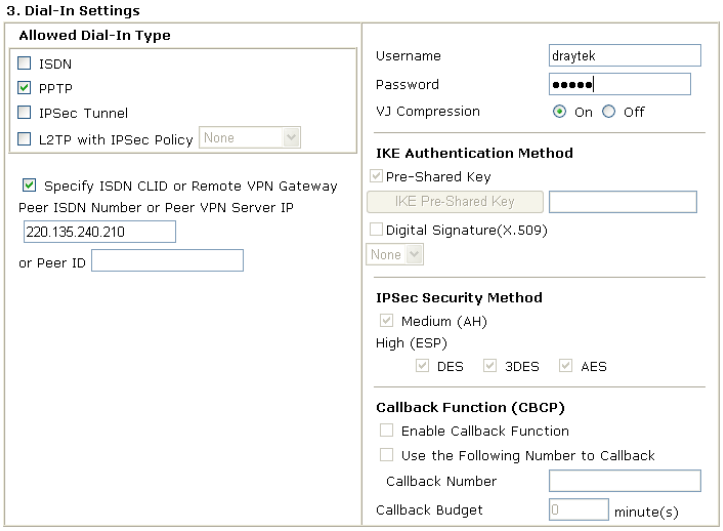


6. Set **Dial-In settings** to as shown below to allow Router B dial-in to build VPN connection.

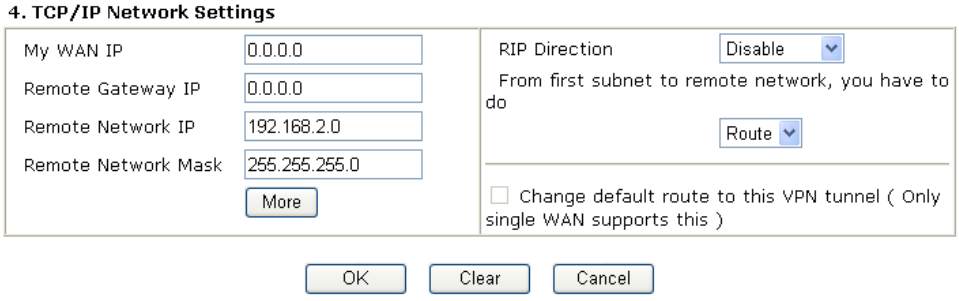
   If an ***IPSec-based*** service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.



If a ***PPP-based service*** is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.



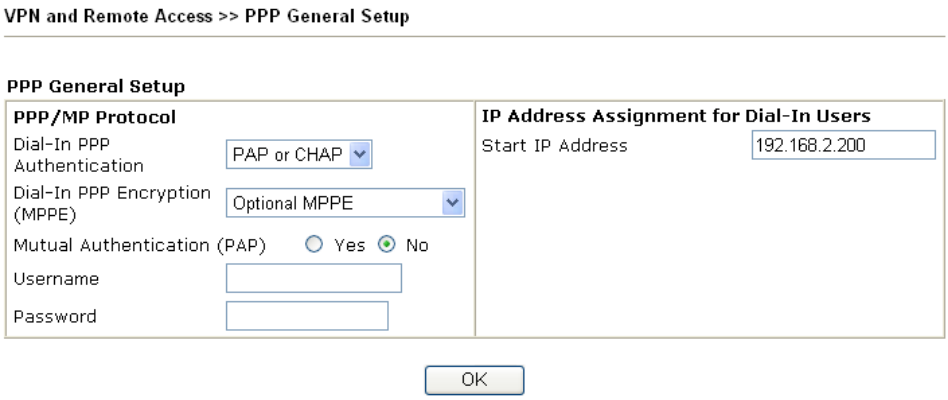
7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router A can direct the packets destined to the remote network to Router B via the VPN connection.



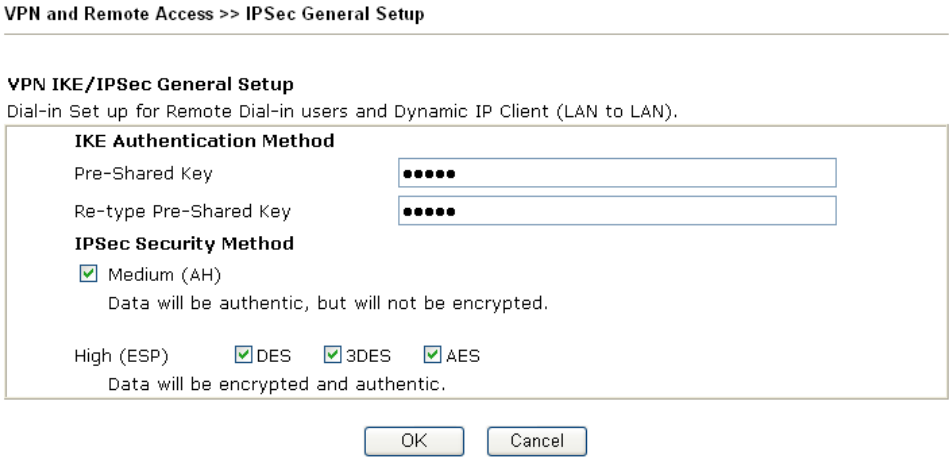
Settings in Router B in the remote office:

1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.

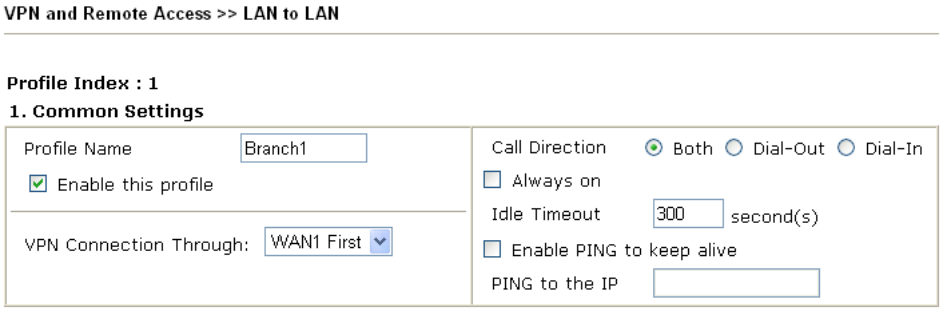
2. Then, for using **PPP based** services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.



For using **IPSec-based** service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.



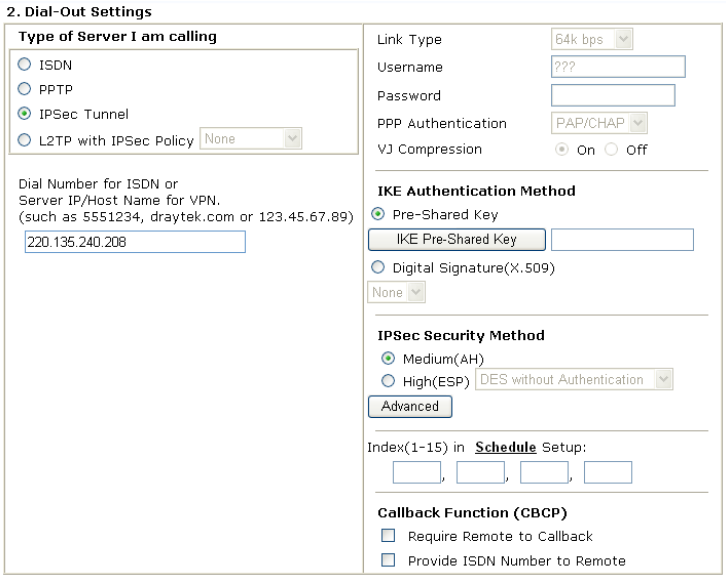
3. Go to **LAN-to-LAN**. Click on one index number to edit a profile.
4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.



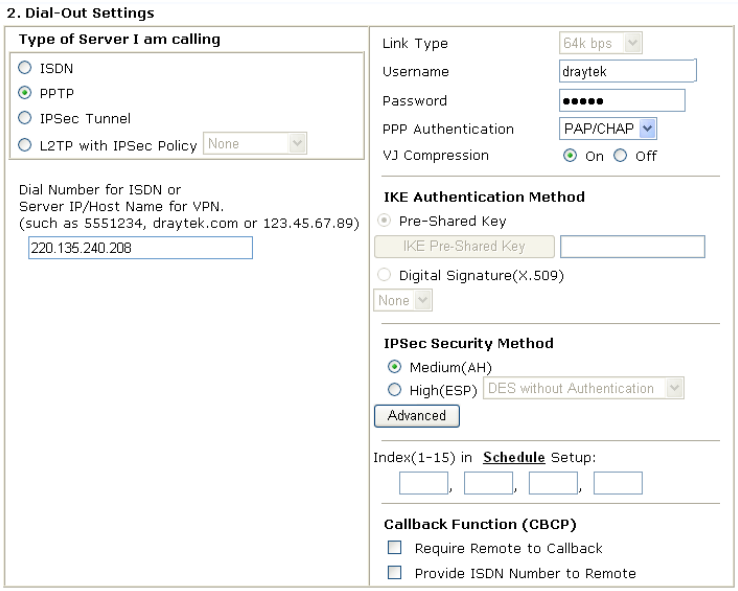
5. Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

If an ***IPSec-based*** service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out

connection.

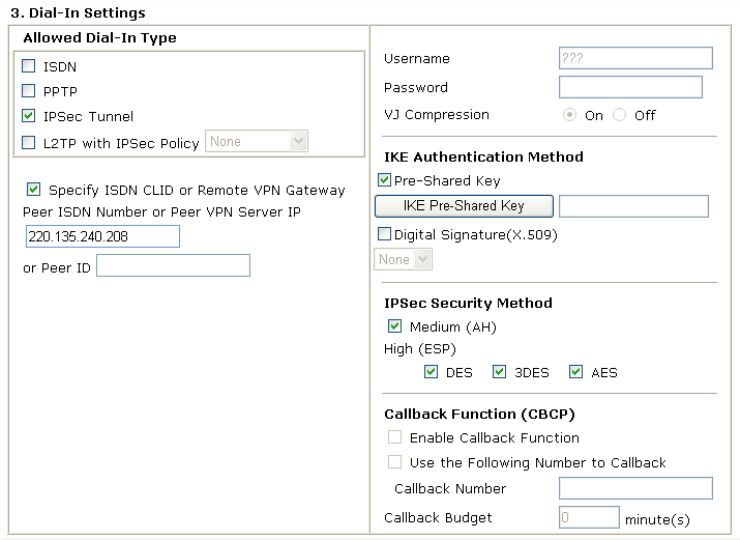


If a ***PPP-based*** service is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

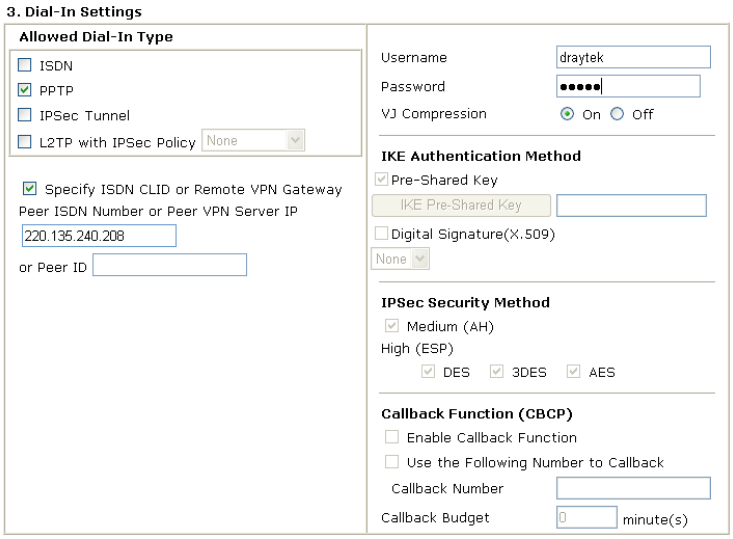


6. Set **Dial-In settings** to as shown below to allow Router A dial-in to build VPN connection.

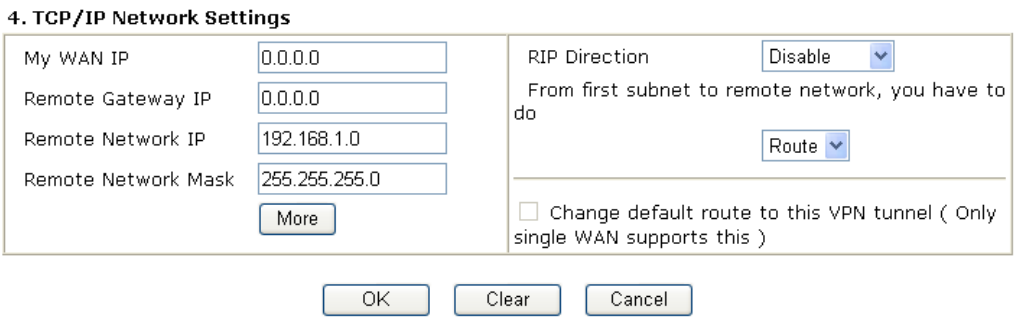
   If an ***IPSec-based*** service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.



If a ***PPP-based*** service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.

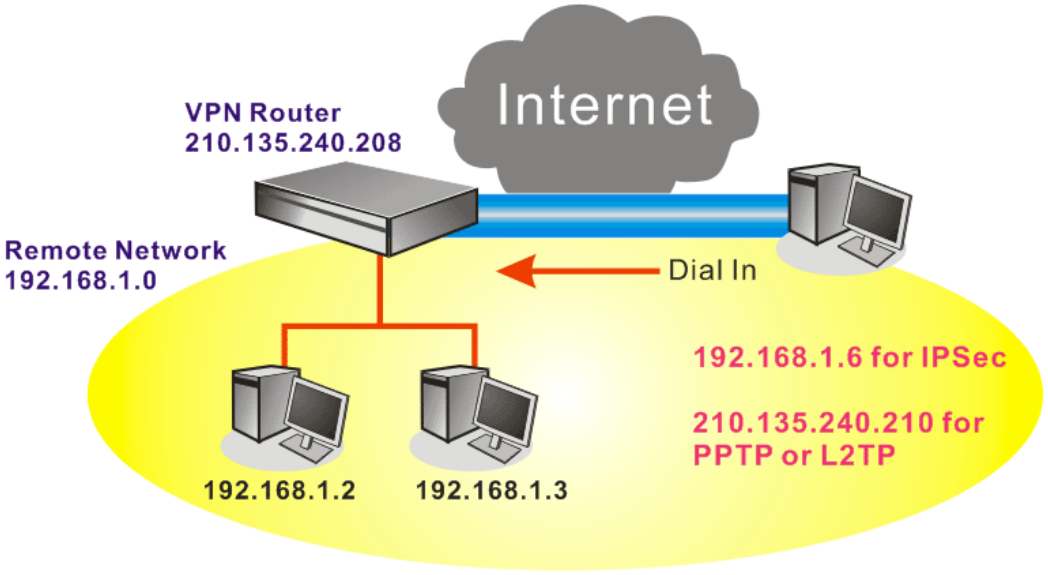


7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router B can direct the packets destined to the remote network to Router A via the VPN connection.



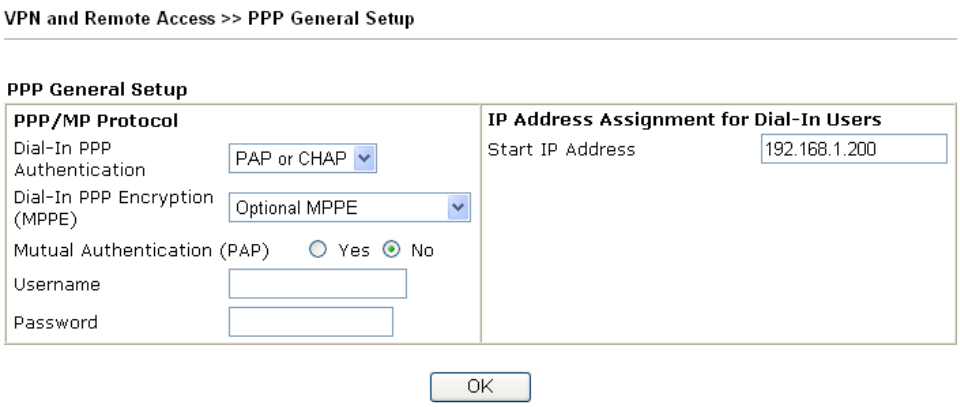
5.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter

The other common case is that you, as a teleworker, may want to connect to the enterprise network securely. According to the network structure as shown in the below illustration, you may follow the steps to create a Remote User Profile and install Smart VPN Client on the remote host.

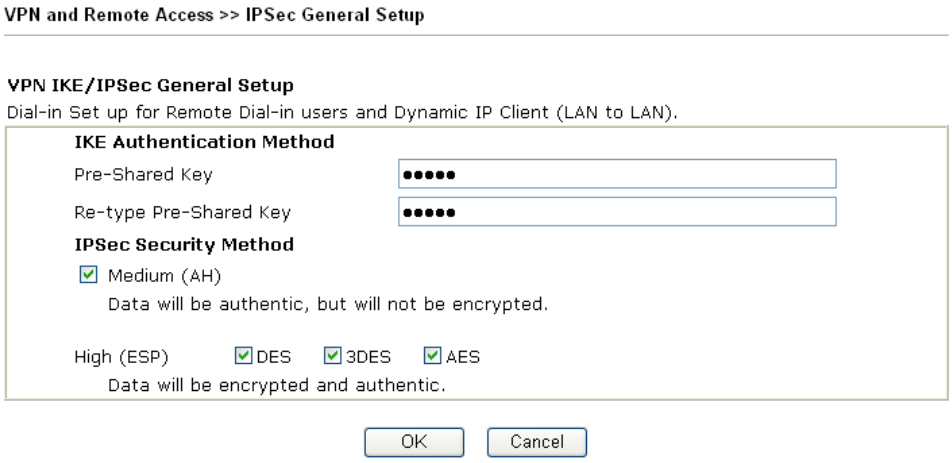


Settings in VPN Router in the enterprise office:

1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
2. Then, for using PPP based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.



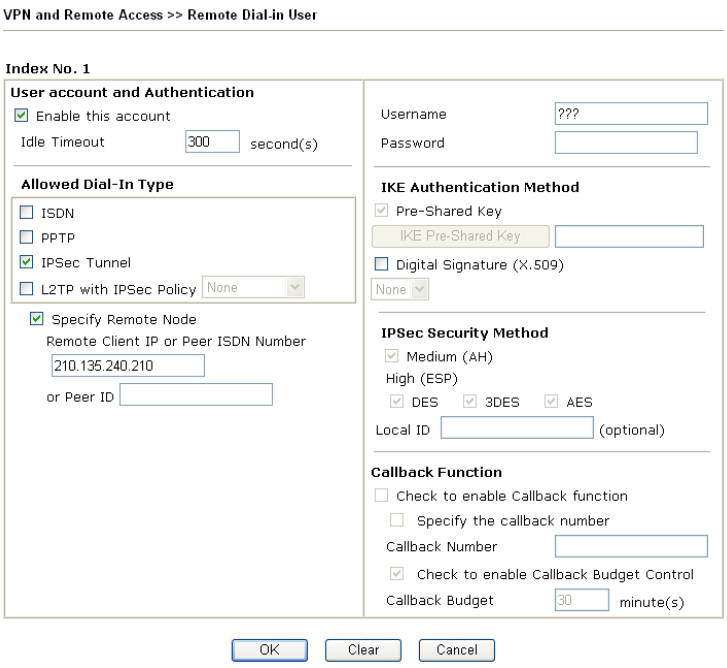
For using IPSec-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IKE/IPSec General Setup**, such as the pre-shared key that both parties have known.



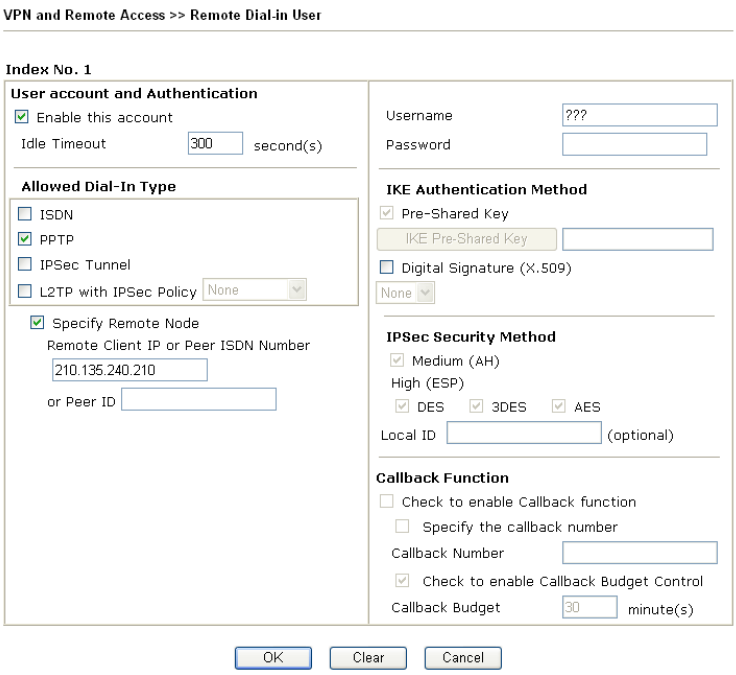
3. Go to **Remote Dial-In Users**. Click on one index number to edit a profile.

4. Set **Dial-In** settings to as shown below to allow the remote user dial-in to build VPN connection.

   If an ***IPSec*** service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.



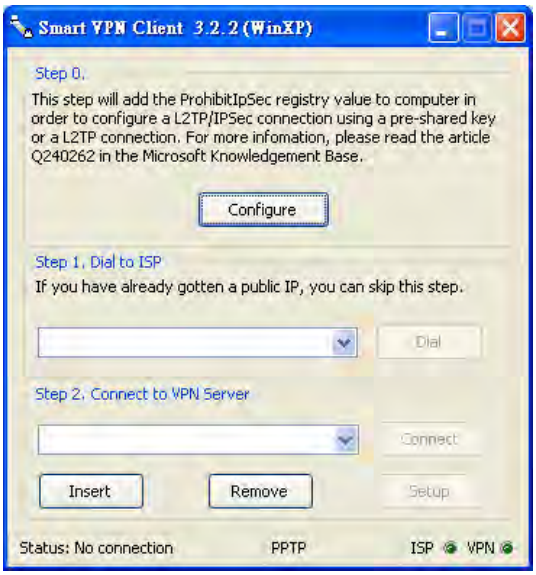
   If a ***PPTP*** service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.



Settings in the remote host:

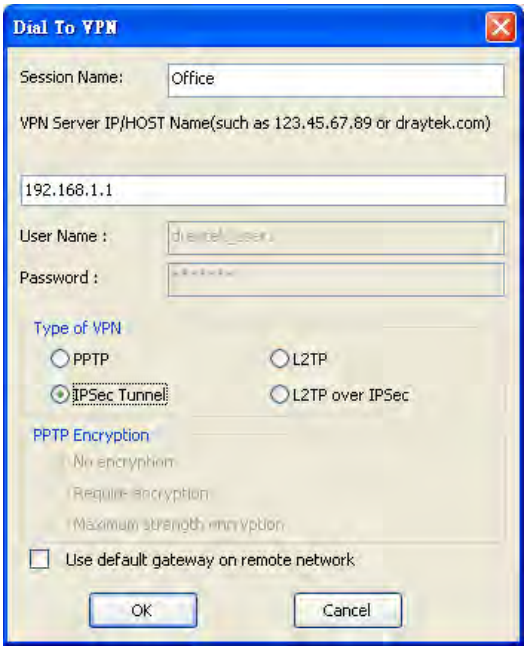
1. For Win98/ME, you may use "Dial-up Networking" to create the PPTP tunnel to Vigor router. For Win2000/XP, please use "Network and Dial-up connections" or “Smart VPN Client”, complimentary software to help you create PPTP, L2TP, and L2TP over IPSec tunnel. You can find it in CD-ROM in the package or go to www.draytek.com download center. Install as instructed.

2. After successful installation, for the first time user, you should click on the **Step 0. Configure** button. Reboot the host.

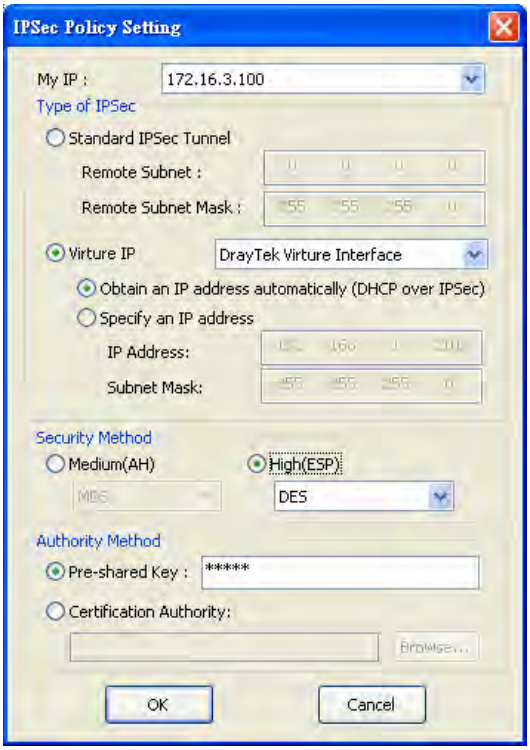


3. In **Step 2. Connect to VPN Server**, click **Insert** button to add a new entry.

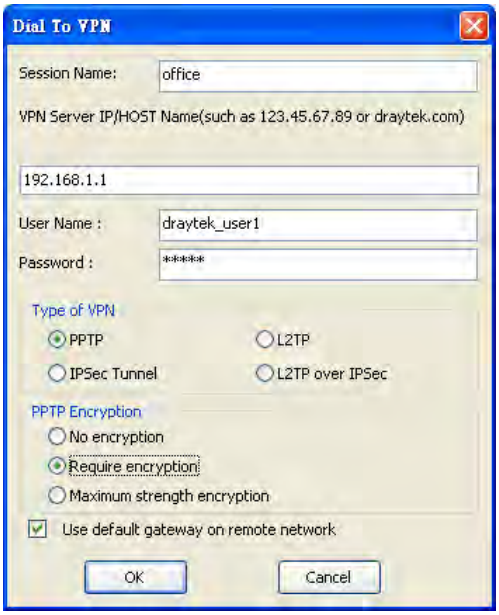
   If an IPSec-based service is selected as shown below,



You may further specify the method you use to get IP, the security method, and authentication method. If the Pre-Shared Key is selected, it should be consistent with the one set in VPN router.



If a PPP-based service is selected, you should further specify the remote VPN server IP address, Username, Password, and encryption method. The User Name and Password should be consistent with the one set up in the VPN router. To use default gateway on remote network means that all the packets of remote host will be directed to VPN server then forwarded to Internet. This will make the remote host seem to be working in the enterprise network.

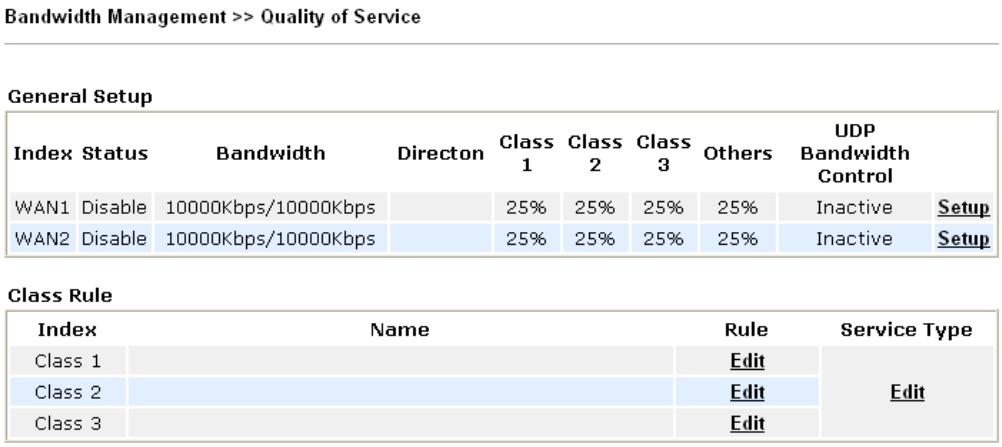


4. Click **Connect** button to build connection. When the connection is successful, you will find a green light on the right down corner.

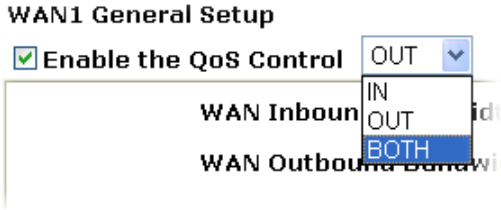
5.3 QoS Setting Example

Assume a teleworker sometimes works at home and takes care of children. When working time, he would use Vigor router at home to connect to the server in the headquarter office downtown via either HTTPS or VPN to check email and access internal database. Meanwhile, children may chat on Skype in the restroom.

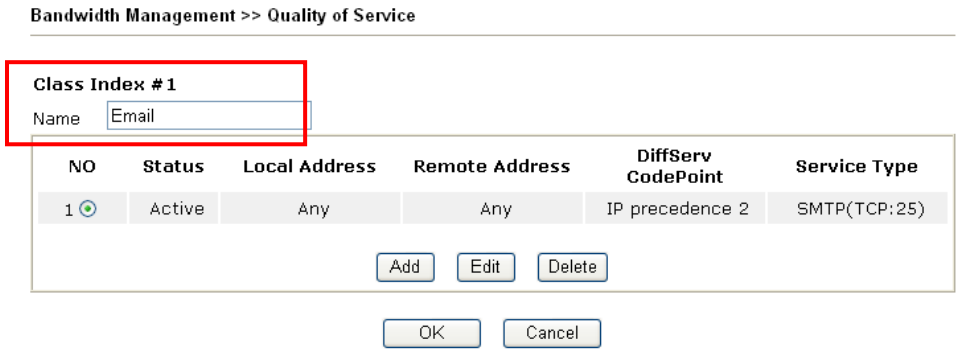
1. Go to **Bandwidth Management>>Quality of Service.**



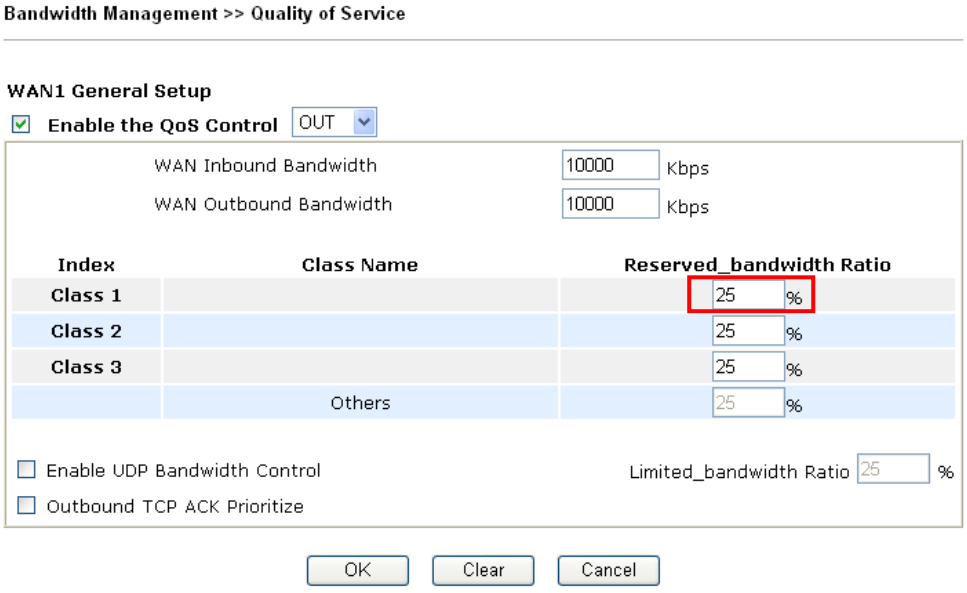
2. Click **Setup** link for WAN1. Make sure the QoS Control on the left corner is checked. And select **BOTH** as the **Direction**.



3. Return to previous page. Enter the Name of Index Class 1 by clicking **Edit** link. Type the name "**E-mail**" for Class 1.

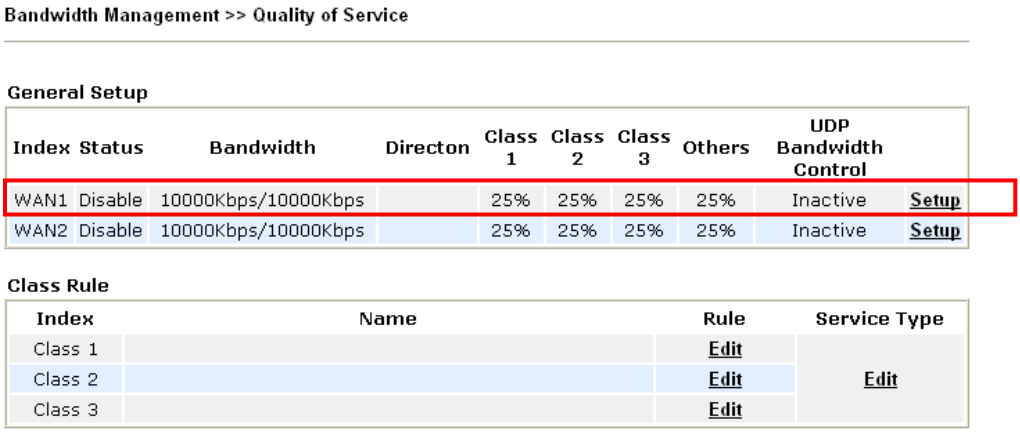


4. For this index, the user will set reserved bandwidth (e.g., 25%) for **Email** using protocol POP3 and SMTP.

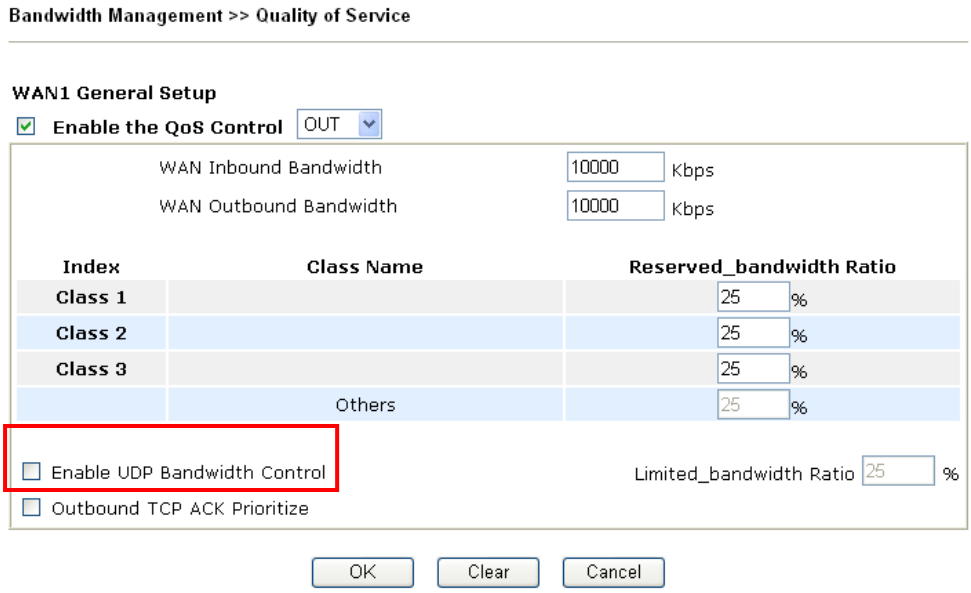


5. Return to previous page. Enter the Name of Index Class 2 by clicking **Edit** link. In this index, the user will set reserved bandwidth (e.g., 25%) for **HTTP**.

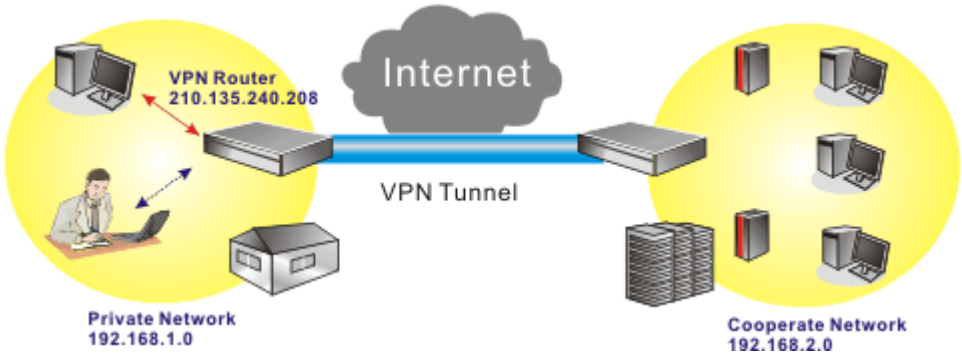
6. Click **Setup** link for WAN1.



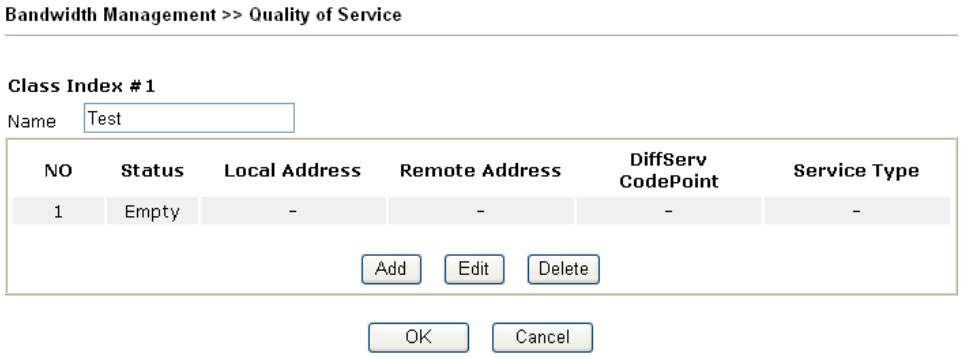
7. Check **Enable UDP Bandwidth Control** on the bottom to prevent enormous UDP traffic of VoIP influent other application, and click OK.



8. If the worker has connected to the headquarter using host to host VPN tunnel. (Please refer to Chapter 3 VPN for detail instruction), he may set up an index for it. Enter the Class Name of Index 3. In this index, he will set reserve bandwidth for 1 VPN tunnel.



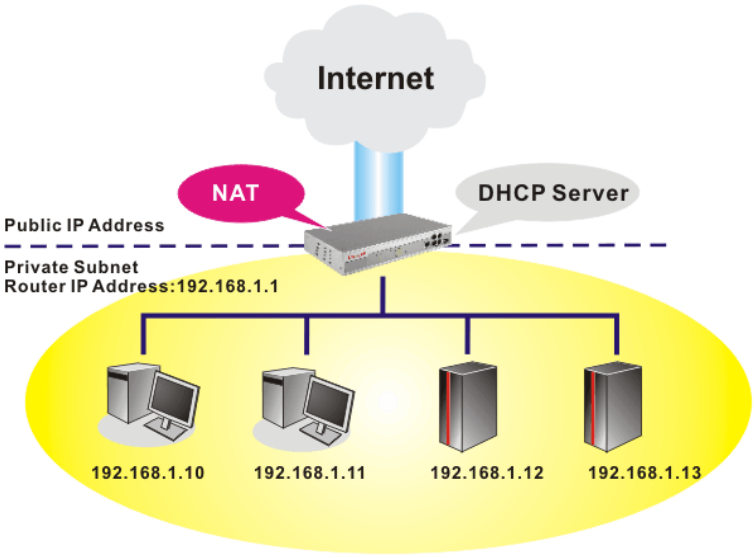
9. Click edit to open a new window.



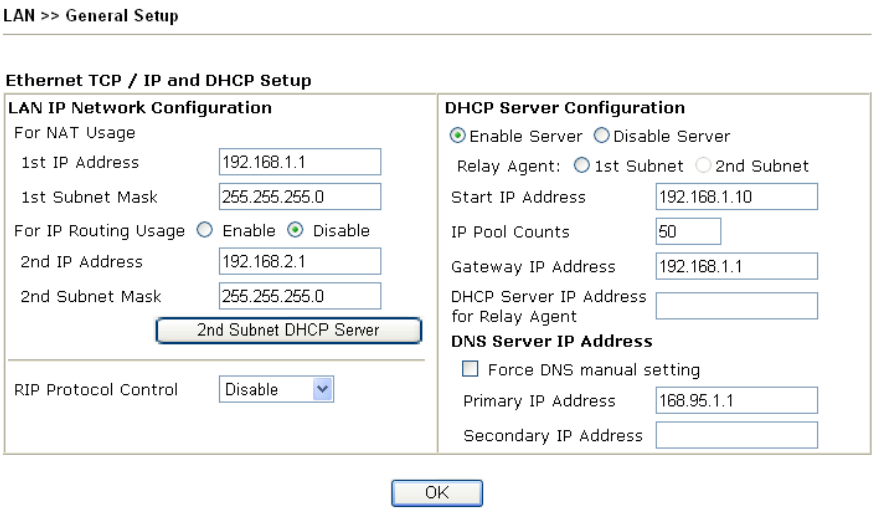
10. First, check the **ACT** box. Then click **Edit** of **Local Address** to set a worker's subnet address. Click **Edit** of **Remote Address** to set headquarter's subnet address. Leave other fields and click **OK**.

5.4 LAN – Created by Using NAT

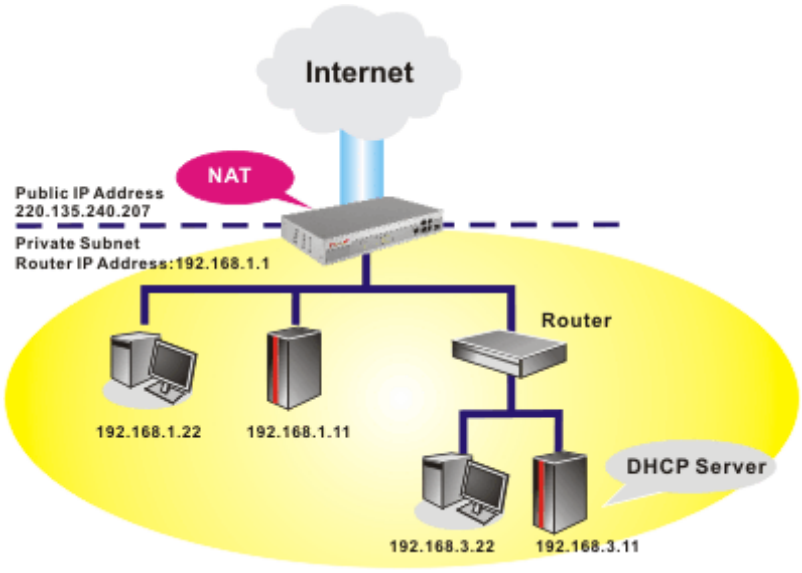
An example of default setting and the corresponding deployment are shown below. The default Vigor router private IP address/Subnet Mask is 192.168.1.1/255.255.255.0. The built-in DHCP server is enabled so it assigns every local NATed host an IP address of 192.168.1.x starting from 192.168.1.10.



You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.



To use another DHCP server in the network rather than the built-in one of Vigor Router, you have to change the settings as show below.



You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.

LAN >> General Setup

Ethernet TCP / IP and DHCP Setup

LAN IP Network Configuration

For NAT Usage

1st IP Address: 192.168.1.1

1st Subnet Mask: 255.255.255.0

For IP Routing Usage: Enable / Disable

2nd IP Address: 192.168.2.1

2nd Subnet Mask: 255.255.255.0

2nd Subnet DHCP Server

RIP Protocol Control: Disable

DHCP Server Configuration

Enable Server / Disable Server

Relay Agent: 1st Subnet / 2nd Subnet

Start IP Address: 192.168.1.10

IP Pool Counts: 50

Gateway IP Address: 192.168.1.1

DHCP Server IP Address for Relay Agent:

DNS Server IP Address

Force DNS manual setting

Primary IP Address: 168.95.1.1

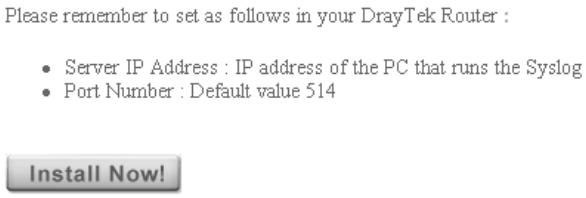
Secondary IP Address:

OK

5.5 Upgrade Firmware for Your Router

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools.

1. Insert CD of the router to your CD ROM.
2. From the webpage, please find out **Utility** menu and click it.
3. On the webpage of Utility, click **Install Now!** (under Syslog description) to install the corresponding program.

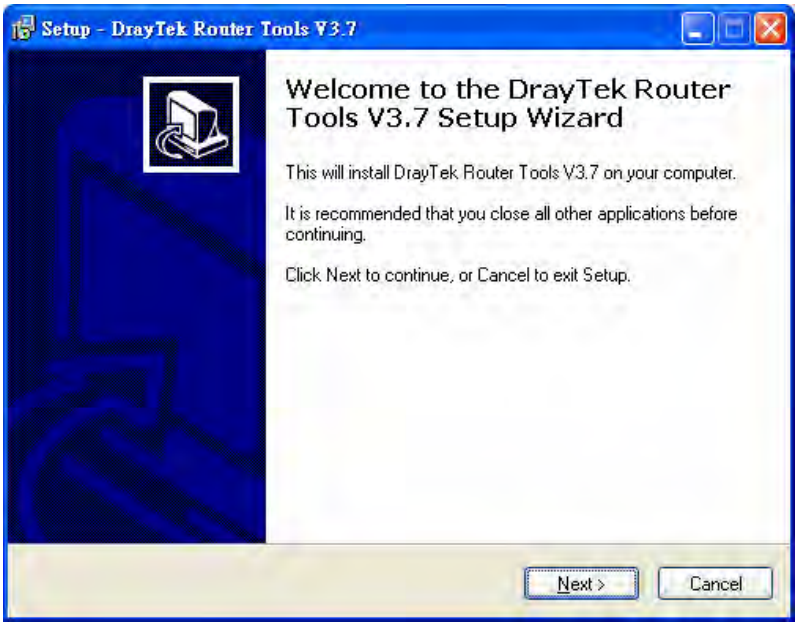


4. The file **RTSxxx.exe** will be asked to copy onto your computer. Remember the place of storing the execution file.
5. Go to **www.draytek.com** to find out the newly update firmware for your router.
6. Access into **Support Center** >> **Downloads**. Find out the model name of the router and click the firmware link. The Tools of Vigor router will display as shown below.

Tools Name	Released Date	Version	OS	Support Model	Download
Router Tools	28/03/2007	3.7	MS-Windows	All Model	zip
Smart VPN Client	18/08/2006	3.2.6	MS-Windows	All Model	zip
Smart VPN Client	21/06/2007	3.2.6	MS-Vista	All Model	zip
LPR	27/06/2005	1.0	MS-Windows	For Print Function	zip
VTA	15/09/2005	2.8	Windows2000/XP	For ISDN Model	zip
DialPlan	26/01/2006	2.5_lite	MS-Windows	For VoIP Model	zip

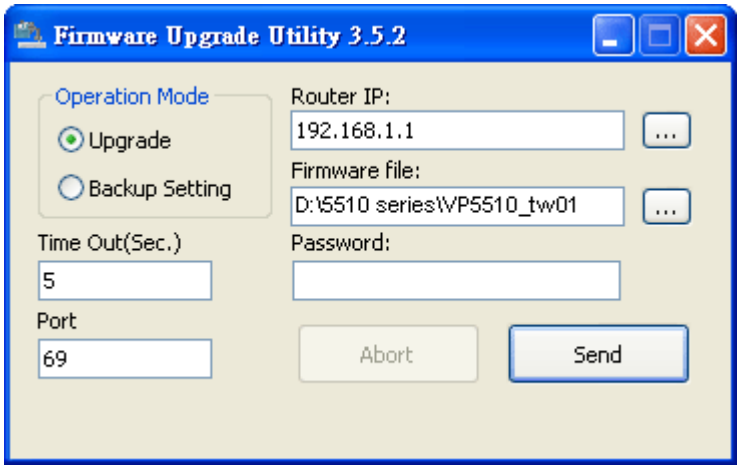
7. Choose the one that matches with your operating system and click the corresponding link to download correct firmware (zip file).
8. Next, decompress the zip file.

9. Double click on the icon of router tool. The setup wizard will appear.

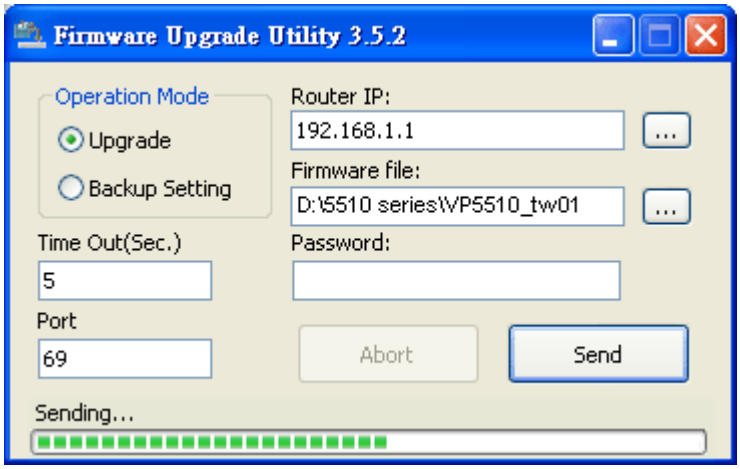


10. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.
11. From the **Start** menu, open **Programs** and choose **Router Tools XXX** >> **Firmware Upgrade Utility**.

12. Type in your router IP, usually **192.168.1.1**.
13. Click the button to the right side of Firmware file typing box. Locate the files that you download from the company web sites. You will find out two files with different extension names, **xxxx.all** (keep the old custom settings) and **xxxx.rst** (reset all the custom settings to default settings). Choose any one of them that you need.

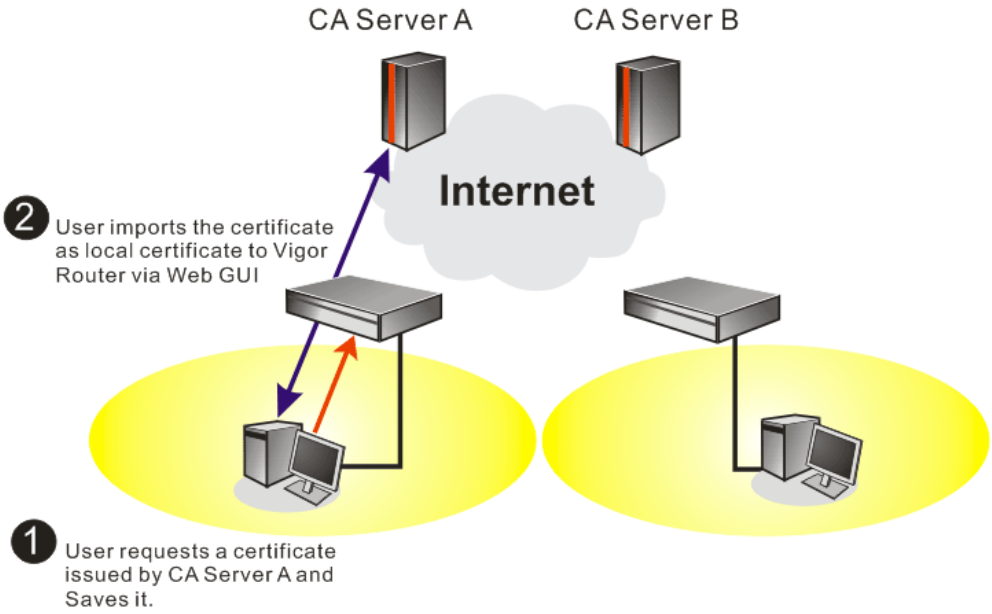


14. Click **Send**.

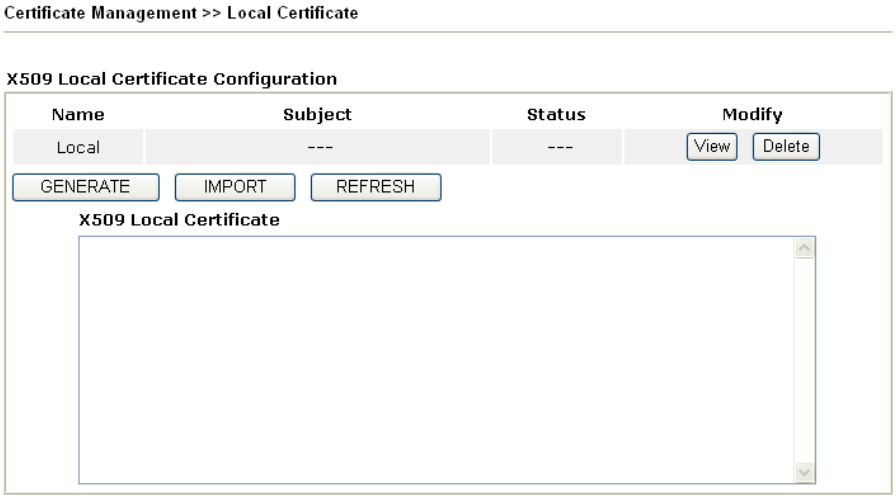


15. Now the firmware update is finished.

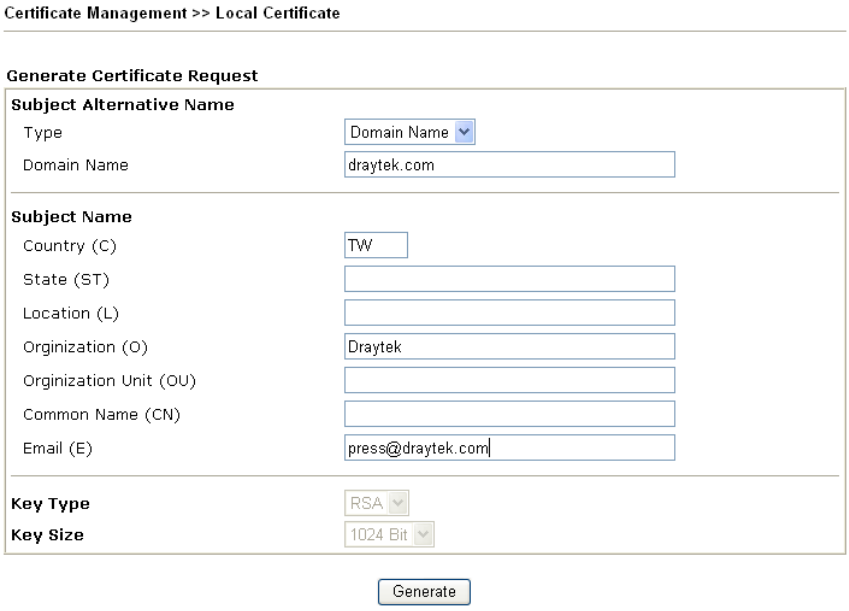
5.6 Request a certificate from a CA server on Windows CA Server



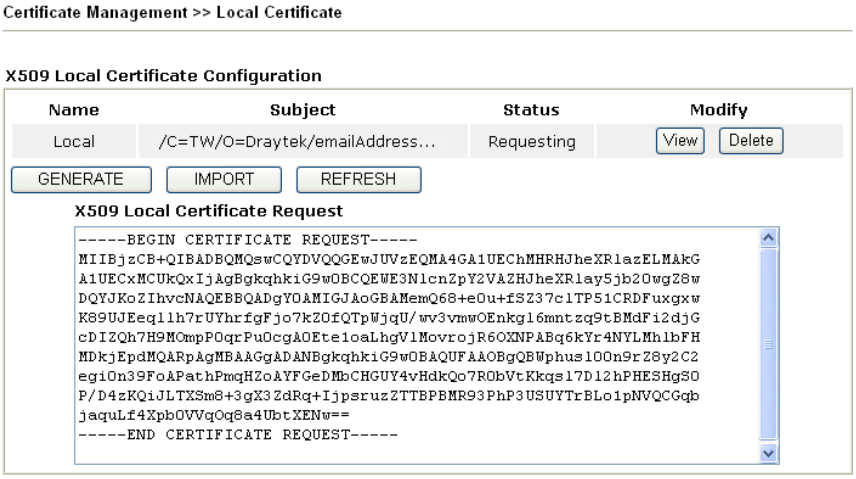
1. Go to **Certificate Management** and choose **Local Certificate**.



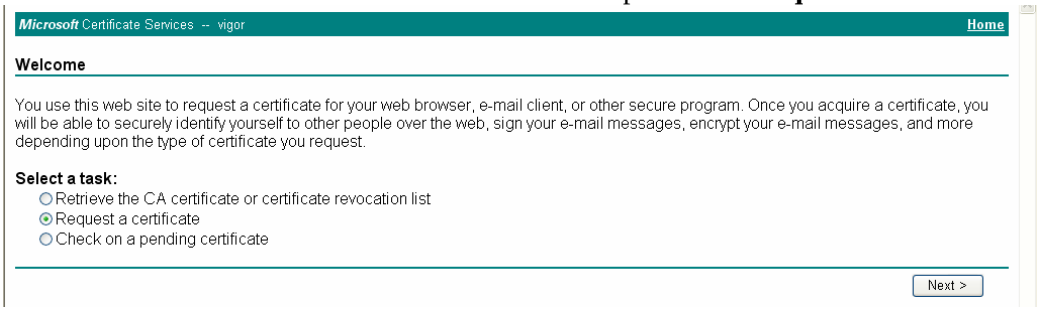
2. You can click **GENERATE** button to start to edit a certificate request. Enter the information in the certificate request.



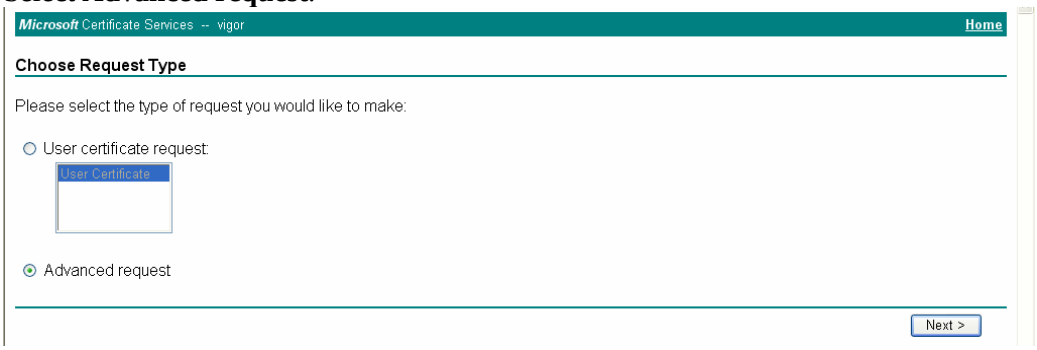
3. Copy and save the X509 Local Certificate Requet as a text file and save it for later use.



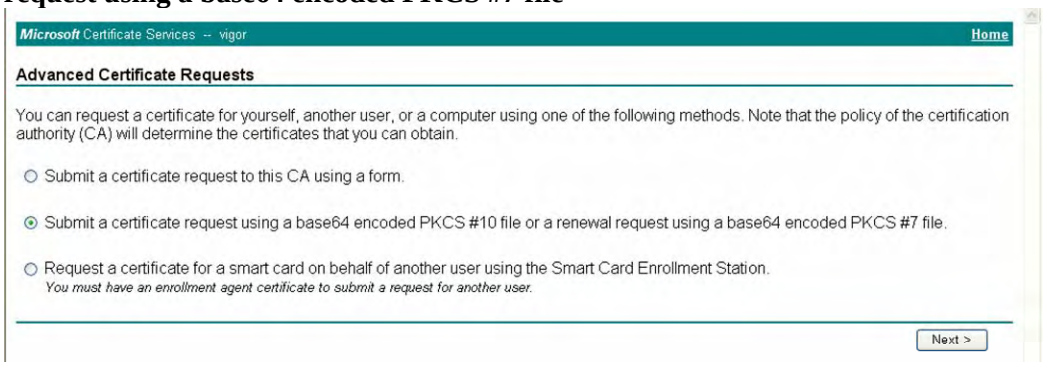
4. Connect to CA server via web browser. Follow the instruction to submit the request. Below we take a Windows 2000 CA server for example. Select **Request a Certificate**.



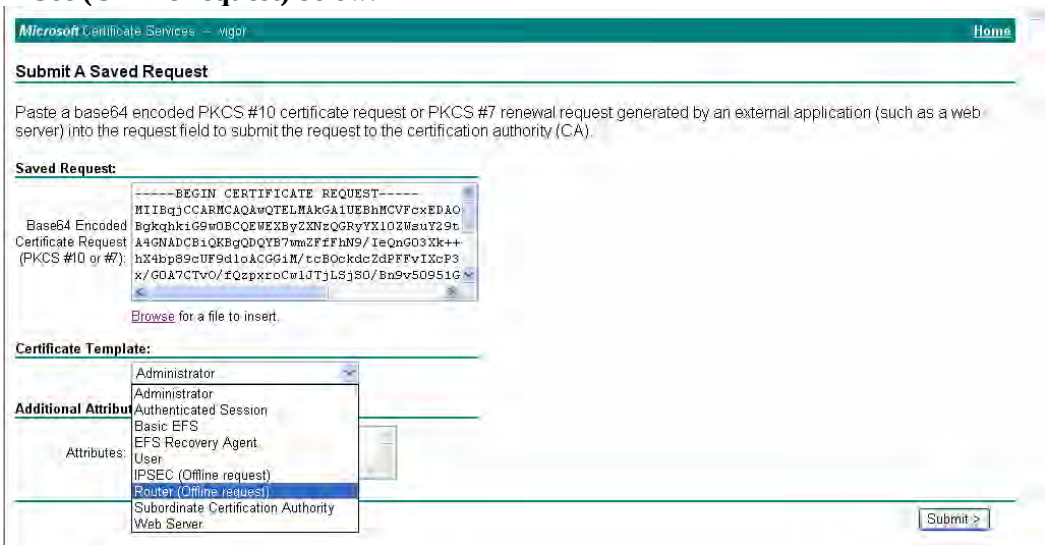
Select **Advanced request**.



Select **Submit a certificate request a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file**



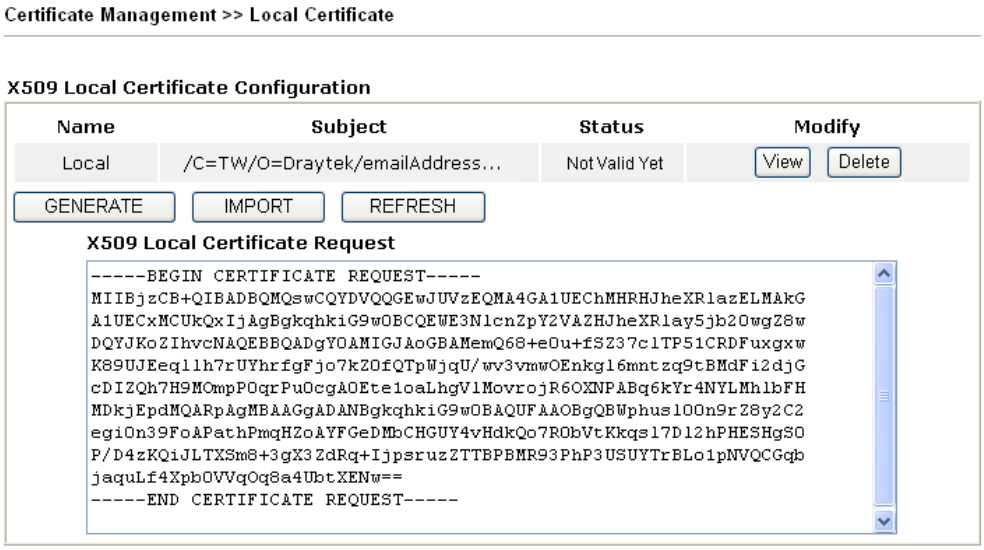
Import the X509 Local Certificate Request text file. Select **Router (Offline request)** or **IPSec (Offline request)** below.



Then you have done the request and the server now issues you a certificate. Select **Base 64 encoded** certificate and **Download CA certificate**. Now you should get a certificate (.cer file) and save it.

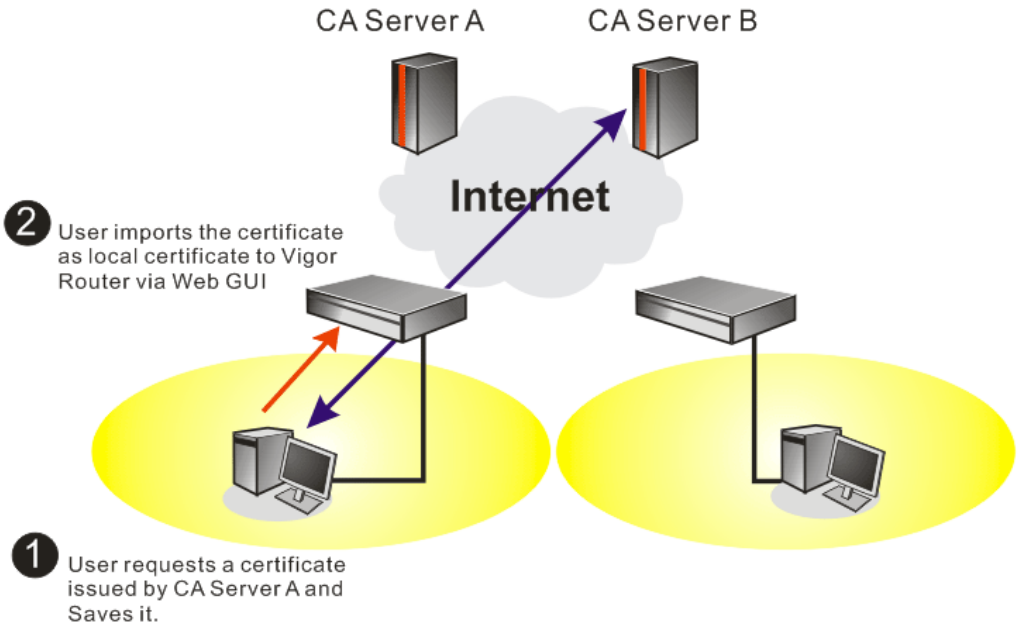
5. Back to Vigor router, go to **Local Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh

and you will find the below window showing “------BEGINE CERTIFICATE------.....”

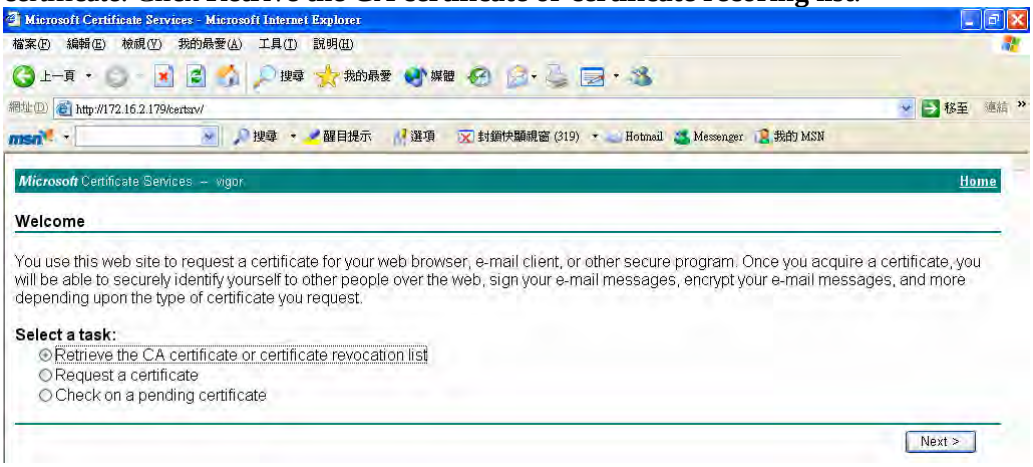


6. You may review the detail information of the certificate by clicking **View** button.

5.7 Request a CA Certificate and Set as Trusted on Windows CA Server

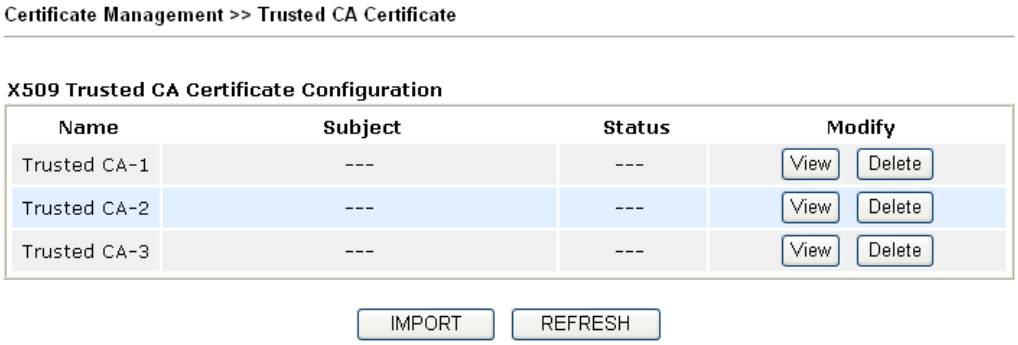


1. Use web browser connecting to the CA server that you would like to retrieve its CA certificate. Click **Retrive the CA certificate or certificate recoring list**.

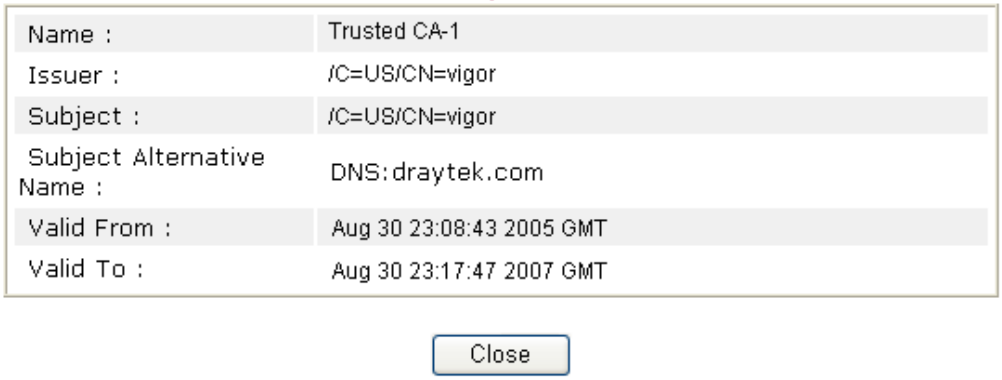


2. In **Choose file to download**, click CA Certificate **Current** and **Base 64 encoded,** and **Download CA certificate** to save the .cer. file.

3. Back to Vigor router, go to **Trusted CA Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below illustration.



4. You may review the detail information of the certificate by clicking **View** button.



Note: Before setting certificate configuration, please go to **System Maintenance** >> **Time and Date** to reset current time of the router first.

This page is left blank.

6 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.

6.1 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 "**2.1 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 **"2.1 Hardware Installation"** to execute the hardware installation again. And then, try again.

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

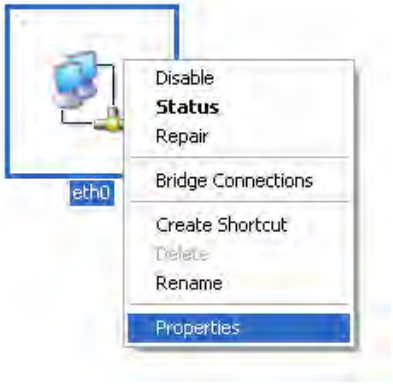
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

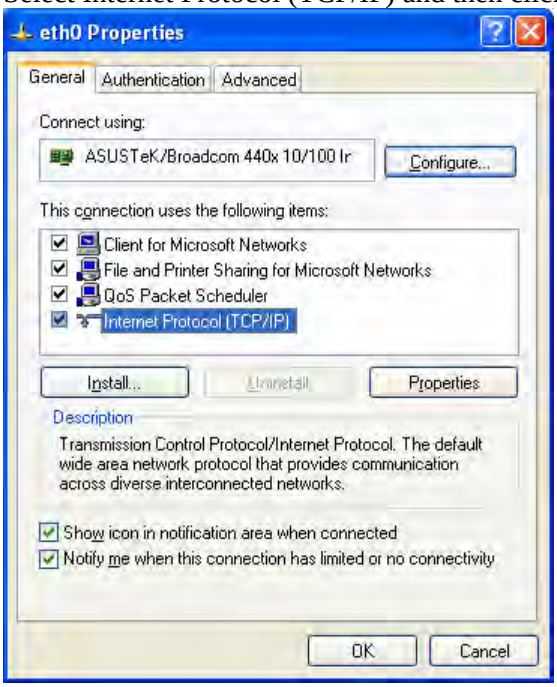
The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

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

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



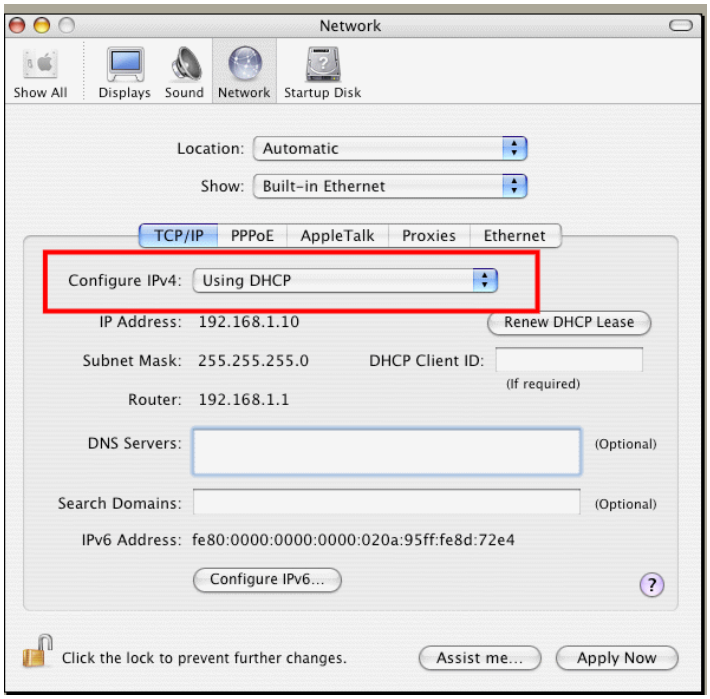
3. Select Internet Protocol (TCP/IP) and then click Properties.



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

For MacOs

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



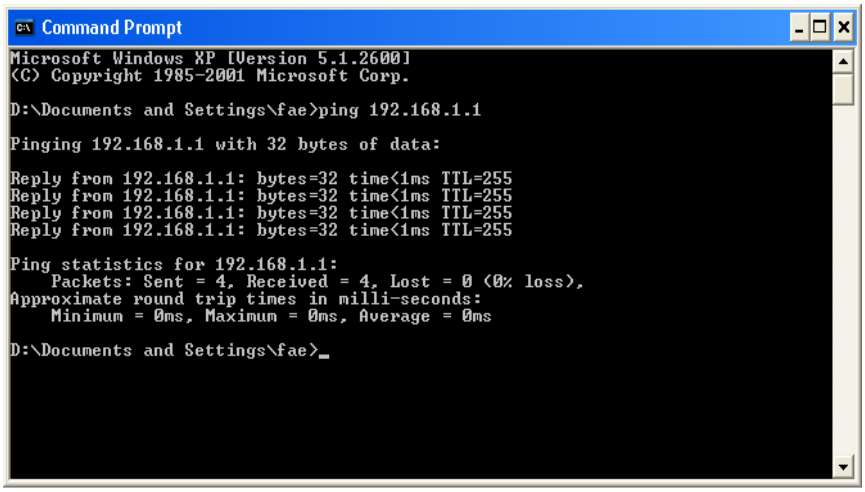
6.3 Pinging the Router from Your Computer

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

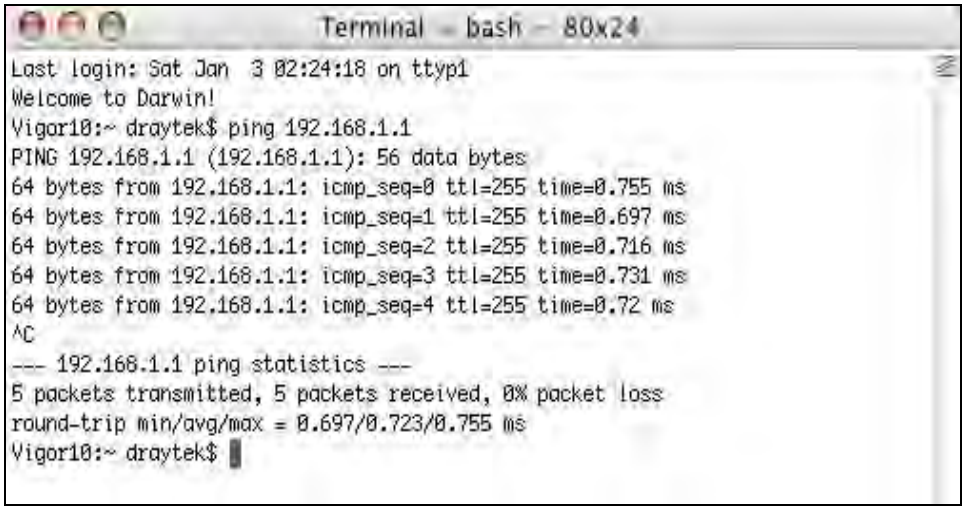
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP). The DOS command dialog will appear.



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

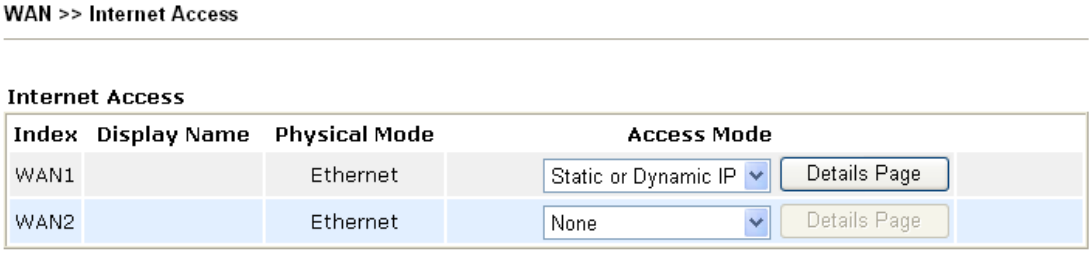
For MacOs (Terminal)

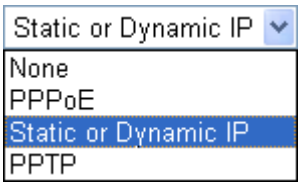
1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. It the link is OK, the line of **"64 bytes from 192.168.1.1: icmp_seq=0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



6.4 Checking If the ISP Settings are OK or Not

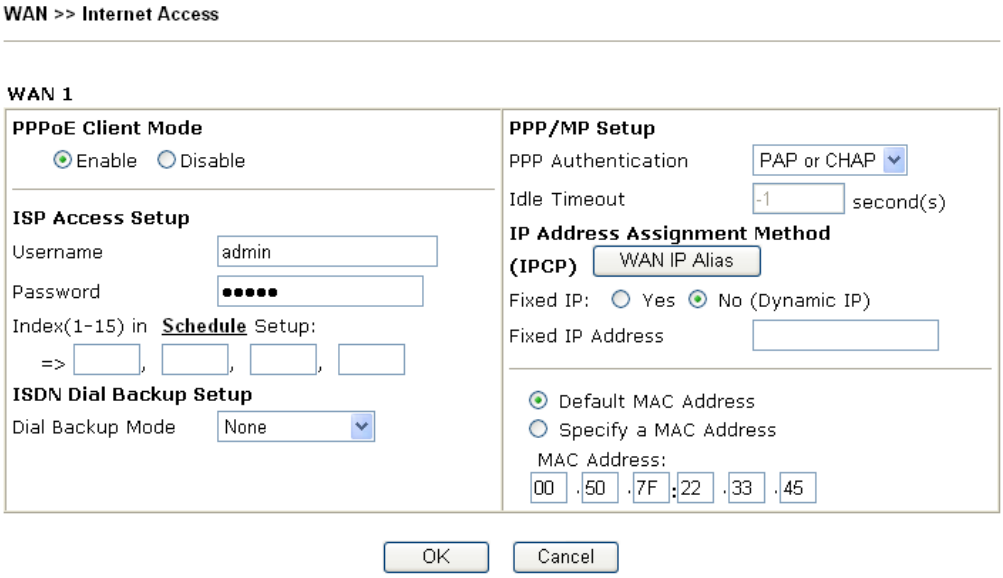
Click **WAN>> Internet Access** and then check whether the ISP settings are set correctly. Click **Details Page** of WAN1/WAN2 to review the settings that you configured previously.





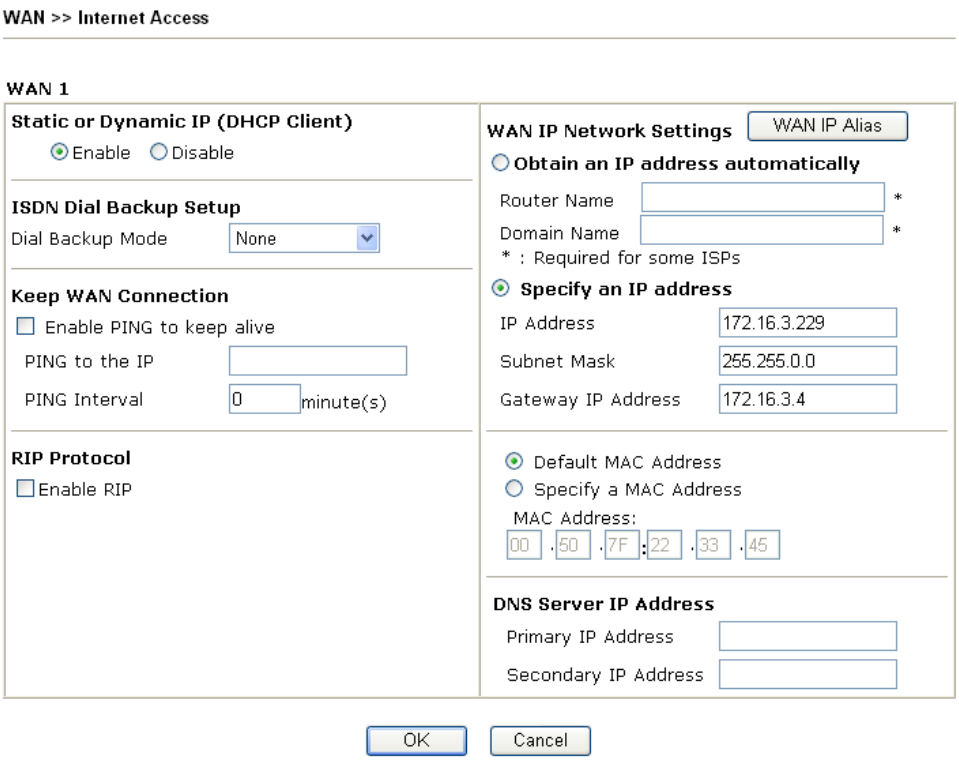
For PPPoE Users

1. Check if the **Enable** option is selected.
2. Check if **Username** and **Password** are entered with correct values that you **got from** your **ISP**.



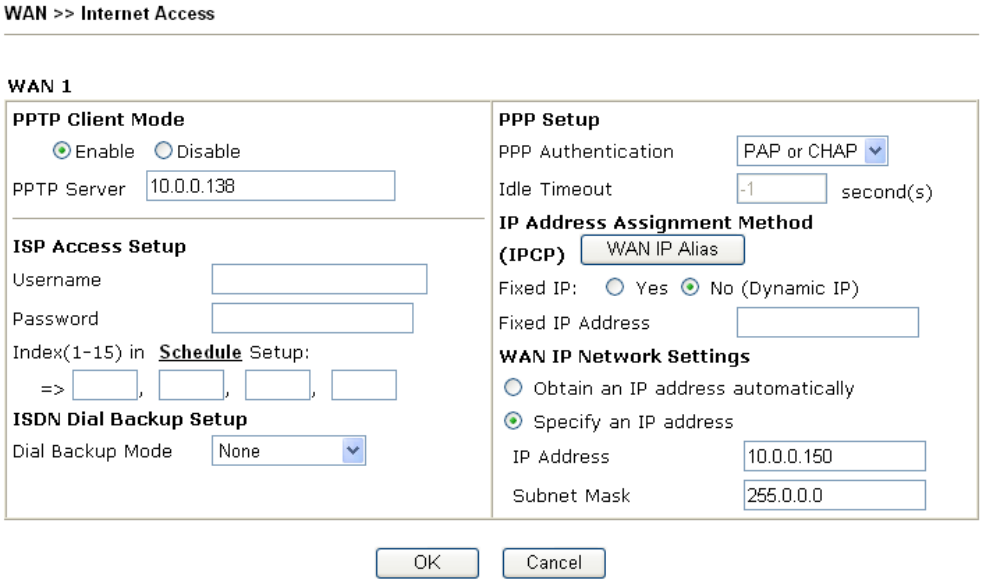
For Static/Dynamic IP Users

1. Check if the **Enable** option is selected.
2. Check if **IP address, Subnet Mask** and **Gateway** are entered with correct values that you **got from** your **ISP**.



For PPTP Users

1. Check if the **Enable** option for **PPTP** Link is selected.



2. Check if **PPTP Server, Username, Password** and **WAN IP address** are set correctly (must identify with the values from your ISP).

6.5 Backing to Factory Default Setting If Necessary

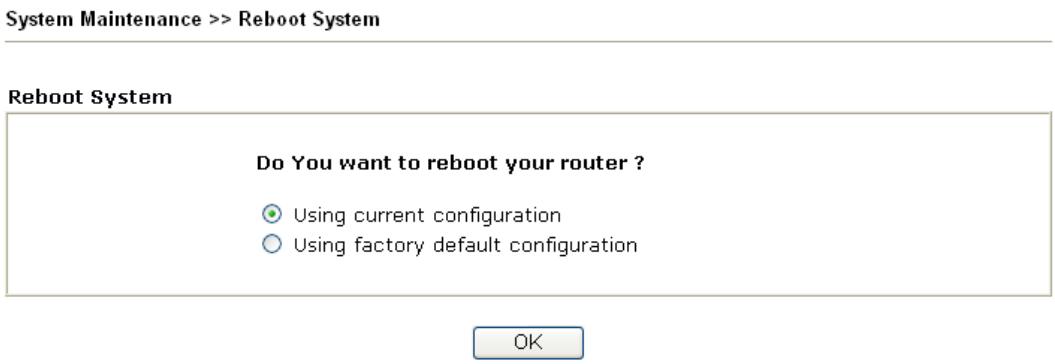
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

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. The password of factory default is null.

Software Reset

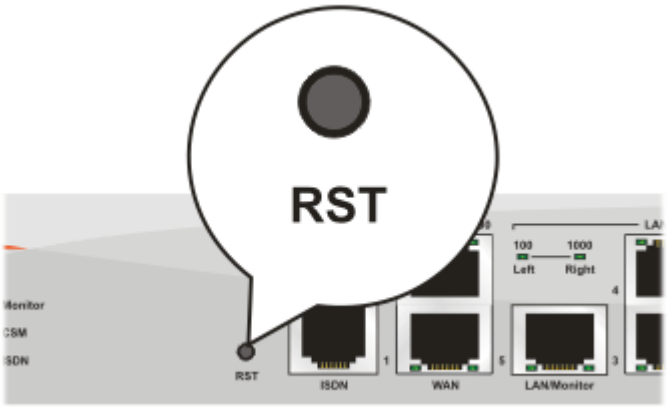
You can reset the router to factory default via Web page.

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 **RST** 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.

6.6 Contacting Your Dealer

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