DrayTek

Vigor 3100 Series Router
User's Guide

Version: 1.1

Date: 2007/01/08

Safety Instructions and Approval

Safety Instructions

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

Warranty

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

Be a Registered Owner

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

Firmware & Tools Updates

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

http://www.draytek.com

European Community Declarations

Manufacturer: DrayTek Corp.
Address: No. 26, Fu Shing Road, HuKou County, HsinChu Industrial Park, Hsin-Chu, Taiwan 303
Product: Vigor3100 Series G.SHDSL Routers

DrayTek Corp. declares that Vigor3100 series of routers are 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 B and EN55024/Class B.

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

The ***Vigor3100G*** is designed for the WLAN 2.4GHz network throughout EC region, Switzerland, and the restrictions of France.

Regulatory Information

Federal Communication Commission Interference Statement

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

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

Table of Contents

1 Preface

Targeting requirement for residential, SOHO (Small Office and Home Office) and business users, the Vigor3100 series are G.SHDSL enabled integrated access device. G.SHDSL is going to be a prevailing standard for business and residential SDSL (Symmetrical DSL) in the rapidly growing worldwide marketplace. Vigor3100/G provides data upto 2.3Mbps through one single pair; Vigor3120 offers data upto 4.6Mbps through two pairs.

The Vigor3100G models are embedded 802.11g compliant wireless module which provides wireless LAN access with line rate as much as 108Mbps with Super G ™. The Vigor3100G models feature WPA2 (802.11i), wireless LAN isolation, and WDS (Wireless Distribution System).

A Virtual Private Network (VPN) is an extension of a private network that encompasses links across shared or public networks like an Intranet. A VPN enables you to send data between two computers across a shared public Internet network in a manner that emulates the properties of a point-to-point private link. The DrayTek Vigor3100 series VPN router supports Internet-industry standards technology to provide customers with open, interoperable VPN solutions such as X.509, DHCP over Internet Protocol Security (IPSec) up to 32 tunnels, and Point-to-Point Tunneling Protocol (PPTP).

1.1 Panel Description

1.1.1 Vigor3100

Front Panel

LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running properly.
VPN		On	The VPN tunnel is launched.
QoS		On	The QoS function is active.
PRN		On	The USB interface printer is ready.
DSL		On	The G.SHDSL line is connected
LAN (1, 2, 3, 4)	LNK	Blinking	It means that Ethernet packets are transmitting.
	100	On	It means that a normal 100Mbps connection is through its corresponding port.
		Off	It means that a normal 10Mbps connection is through its corresponding port.
	FDX	On	It means a full duplex connection.
		Off	It means a half duplex connection.
		Blinking	It means that a packet collision happens.

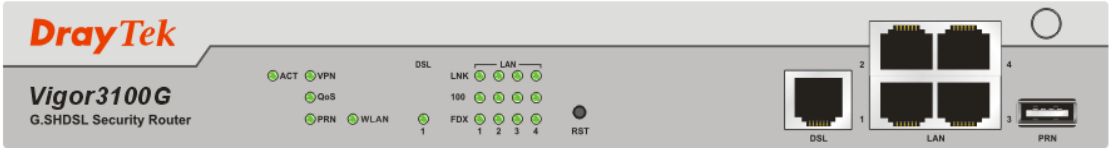
Interface	Description
RST (Factory Reset)	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
DSL	Connect the G.SHDSL line to access the Internet.
LAN (1,2,3,4)	Connect to the local networked devices.
PRN	Connect to the USB printer.

Rear Panel

Interface	Description
	Connecter for a power cord with 100-240 VAC (inlet).
	Power Switch. “1” is ON; “0” is OFF.

1.1.2 Vigor3100G

Front Panel



LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running properly.
VPN		On	The VPN tunnel is launched.
QoS		On	The QoS function is active.
PRN		On	The USB interface printer is ready.
WLAN		On	The wireless LAN function is enabled.
		Blinking	Wireless traffic goes through.
DSL		On	The G.SHDSL line is connected.
LAN (1, 2, 3, 4)	LNK	Blinking	It means that Ethernet packets are transmitting.
	100	On	It means that a normal 100Mbps connection is through its corresponding port.
		Off	It means that a normal 10Mbps connection is through its corresponding port.
	FDX	On	It means a full duplex connection.
		Off	It means a half duplex connection.
		Blinking	It means that a packet collision happens.

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.
DSL	Connect the G.SHDSL line to access the Internet.
LAN (1,2,3,4)	Connect to the local networked devices.
PRN	Connect to the USB printer.

Rear Panel

Interface	Description
	Connecter for a power cord with 100-240 VAC (inlet).
	Power Switch. “1” is ON; “0” is OFF.

1.1.3 Vigor3120

Front Panel

LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running properly.
VPN		On	The VPN tunnel is launched.
QoS		On	The QoS function is active.
PRN		On	The USB interface printer is ready.
DSL		On	The G.SHDSL line is connected.
LAN (1, 2, 3, 4)	LNK	Blinking	It means that Ethernet packets are transmitting.
	100	On	It means that a normal 100Mbps connection is through its corresponding port.
		Off	It means that a normal 10Mbps connection is through its corresponding port.
	FDX	On	It means a full duplex connection.
		Off	It means a half duplex connection.
		Blinking	It means that a packet collision happens.

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.
DSL(1/2)	Connecter for remote networked devices.
LAN (1-4)	Connecter for local networked devices.
PRN	USB interface for printer.

Rear Panel

Interface	Description
	Connecter for a power cord with 100-240 VAC (inlet).
	Power Switch. “1” is ON; “0” is OFF.

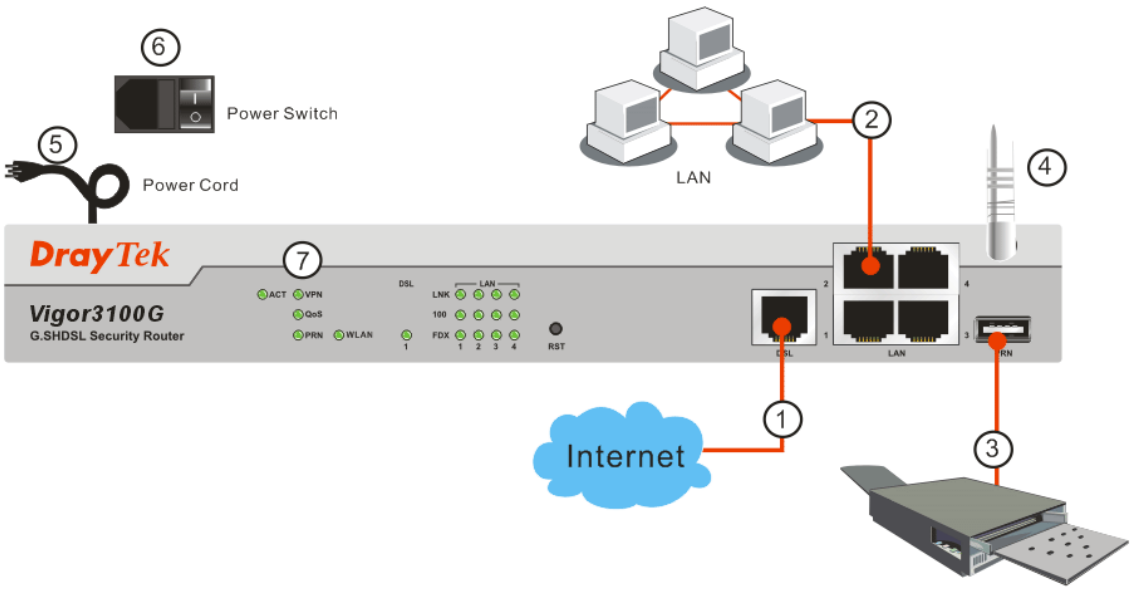
1.2 Hardware Installation

1.2.1 For Vigor3100 and Vigor3100G

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

1. Connect the DSL port of the router to the wall outlet with a RJ-11 to RJ-45 (or RJ-45 to RJ-45) cable. For Vigor3120, please refer to 2.2.1
2. Connect one port of 4-port switch to your computer with a RJ-45 cable.
3. Connect the printer to the router with the USB cable and connect the power cord. If you do not have a printer for using, skip this step.
4. Connect detachable antennas to the router for Vigor3100G.
5. Connect one end of the power cord to the power port of the router. Connect the other end to the wall outlet of electricity.
6. Power on the router.
7. Check the **ACT** and **DSL**, **LAN** LEDs to assure network connections.

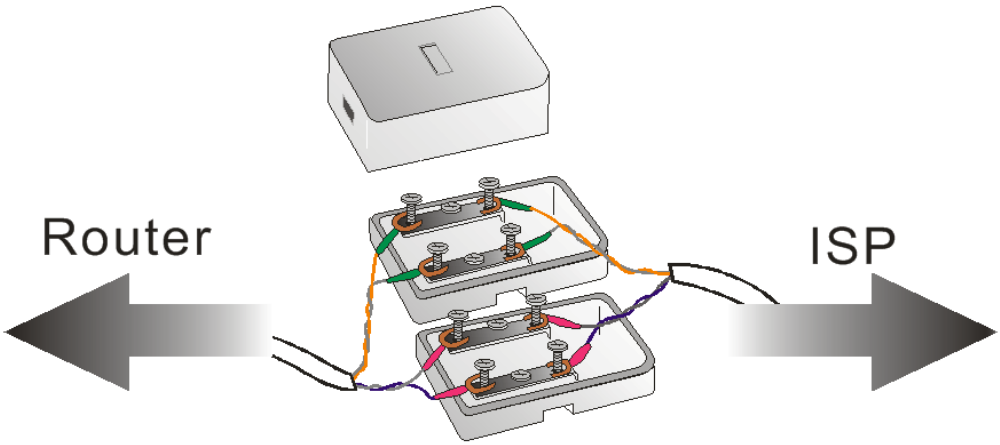
(For the detailed information of LED status, please refer to section 1.1.)



1.2.2 Hardware Installation for Vigor3120

Vigor3120 provides Flat Module Cable (RJ-45, 4x4) for bonding bandwidth for data transmission. Please apply two-pair of circuit from your ISP first for hardware connection.

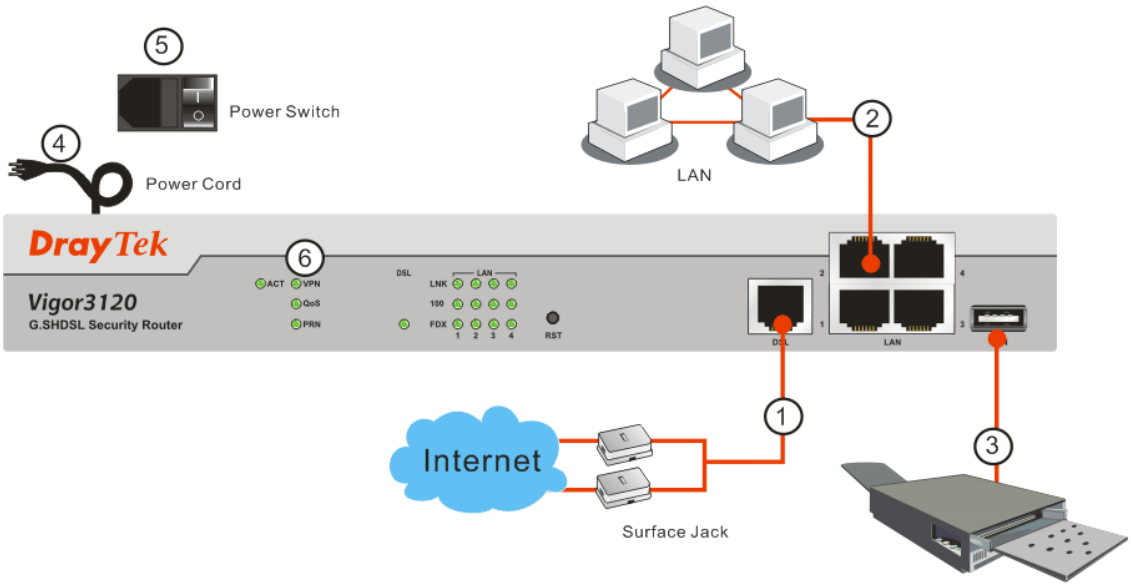
Then, open the cover of surface jack and use a screw driver to loosen the screws inside the surface jack. Notice that lines wrapped with same color tape mean one pair. Please connect them to one surface jack (that will be used to connect to DSL connector of the router). Use the same way to connect another pair of lines to another surface jack (that will be used to connect to ISP).



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

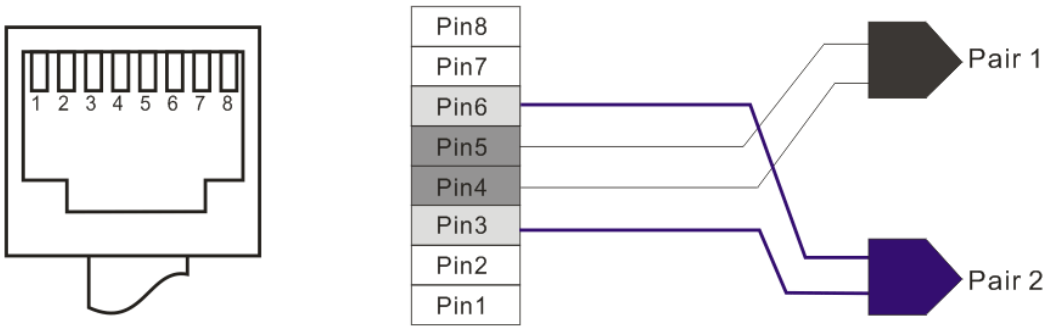
1. Connect the DSL port of the router to the wall outlet with a Flat Module Cable (RJ-45, 4x4).
2. Connect one port of 4-port switch to your computer with a RJ-45 cable.
3. Connect the printer to the router with the USB cable and connect the power cord. If you do not have a printer for using, skip this step.
4. Connect one end of the power cord to the power port of the router. Connect the other end to the wall outlet of electricity.
5. Power on the router.
6. Check the **ACT** and **DSL**, **LAN** LEDs to assure network connections.

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



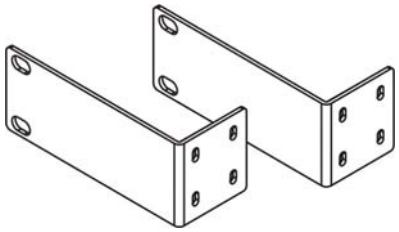
1.2.3 Pin Definition for Flat Module Cable

Below shows the pin definition of flat module cable. One pair is composed by Pin4 and Pin5. The other pair is composed by Pin3 and Pin6.

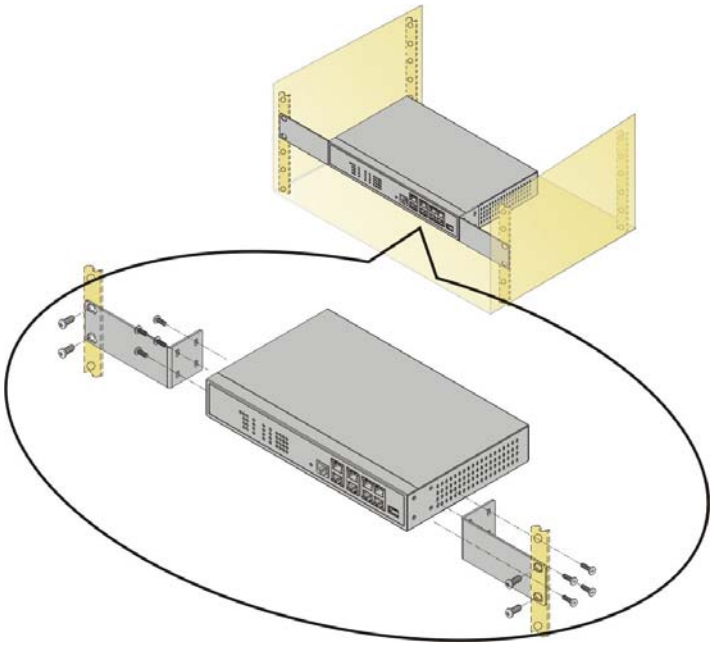


1.3 Rack Mount Instruction

The Vigor3100 series can be mounted on a rack by using standard brackets in a 19-inch rack or optional larger brackets on 23-inch rack (not included). The bracket for the racks are shown below.



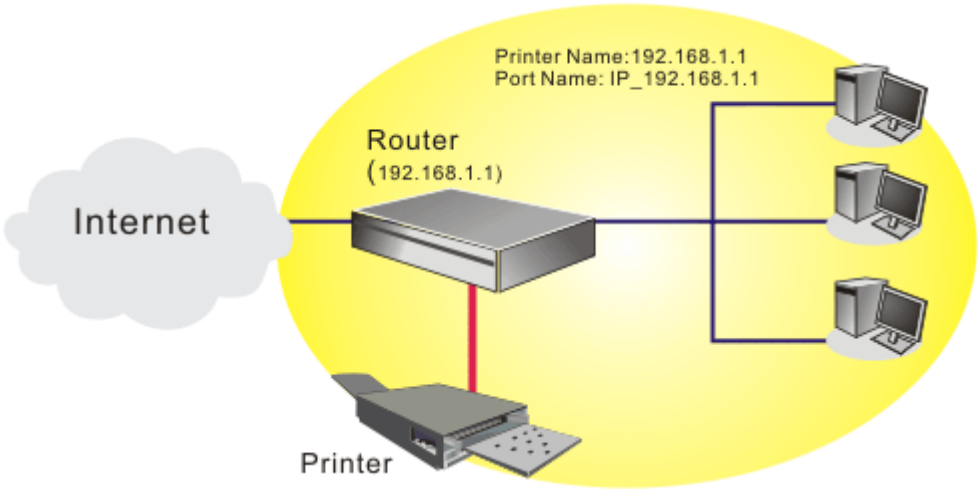
Use brackets to set the Vigor router on the rack as shown below.



After the bracket installation, the Vigor router chassis can be installed in a rack by using four screws for each side of the rack.

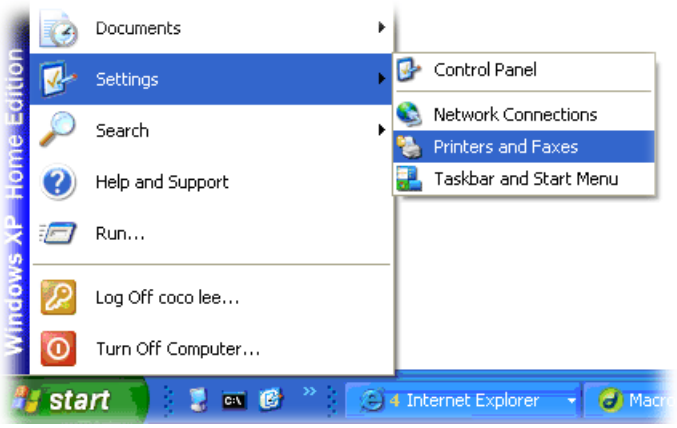
1.4 Printer Installation

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.

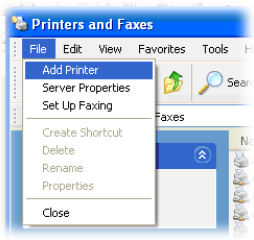


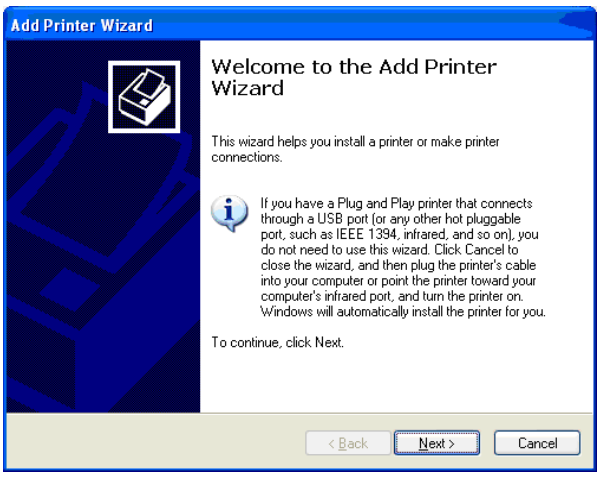
Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

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

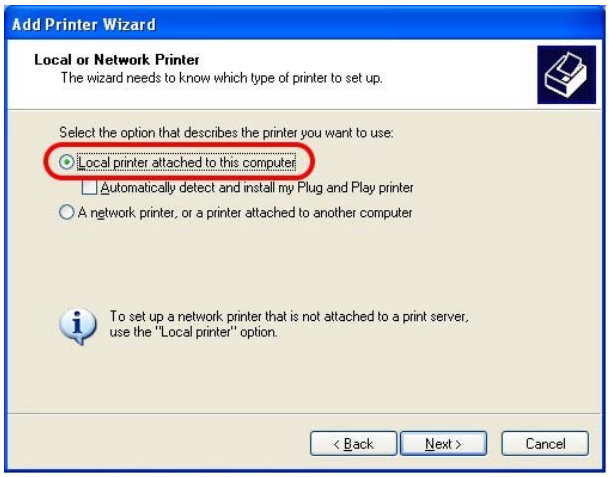


3. Open **File->Add a New Computer**. A welcome dialog will appear. Please click **Next**.

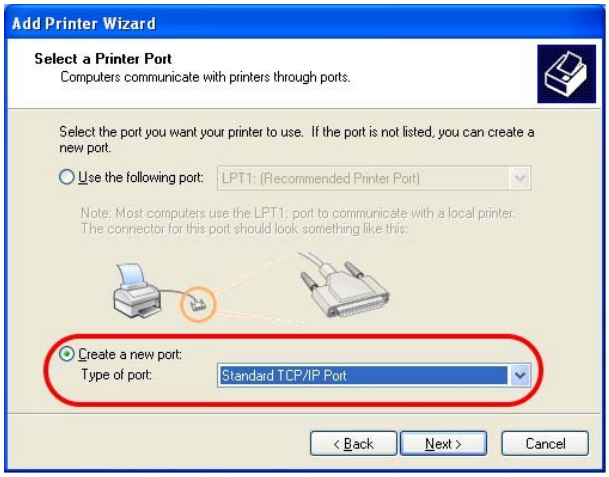




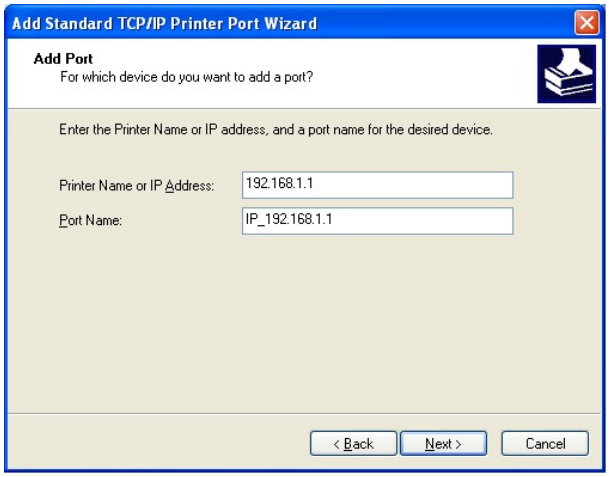
4. Click Local printer attached to this computer and click Next.



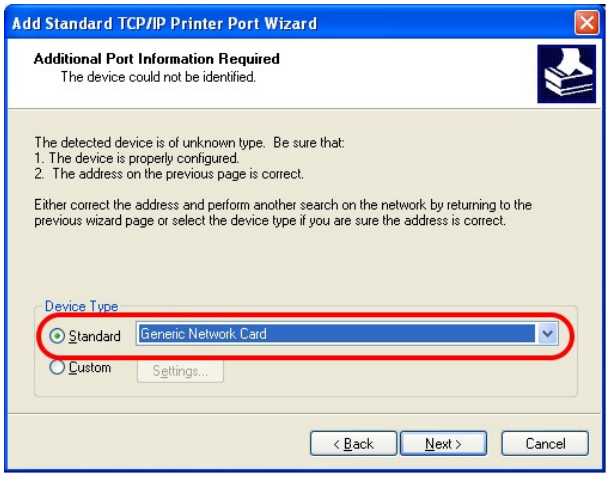
5. In this dialog, choose **Create a new port Type of port** and use the drop down list to select **Standard TCP/IP Port**. Click **Next**.



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**.

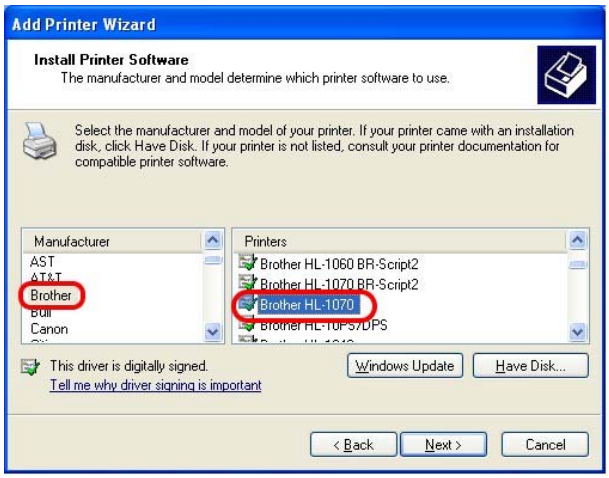


7. Click Standard and choose Generic Network Card.

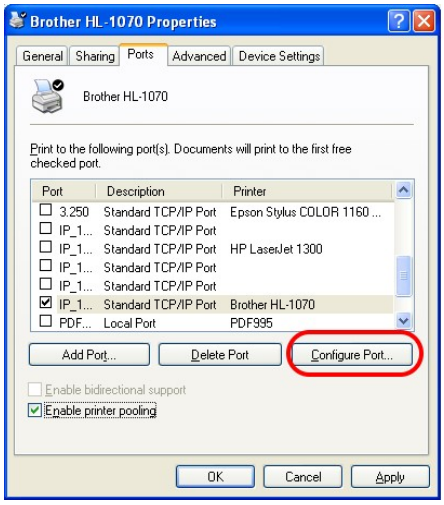


8. Then, in the following dialog, click **Finish**.

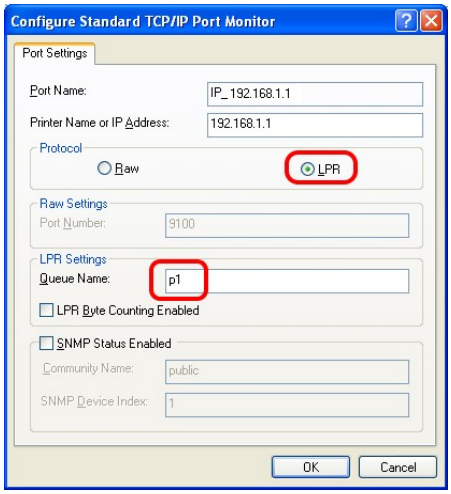
9. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



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.

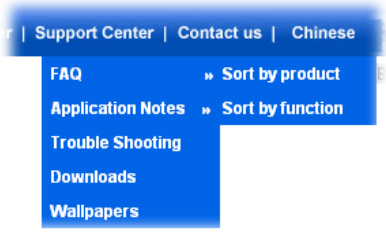


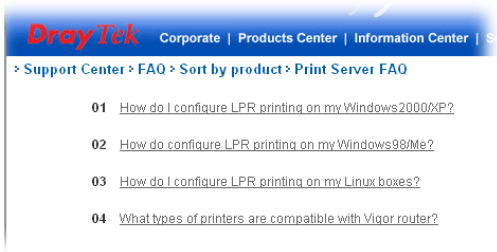
11. Select "**LPR**" on Protocol, type **p1** (number 1) as Queue Name. Then click **OK**. Next please refer to the red rectangle for choosing the correct protocol and UPR name.



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.

---

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

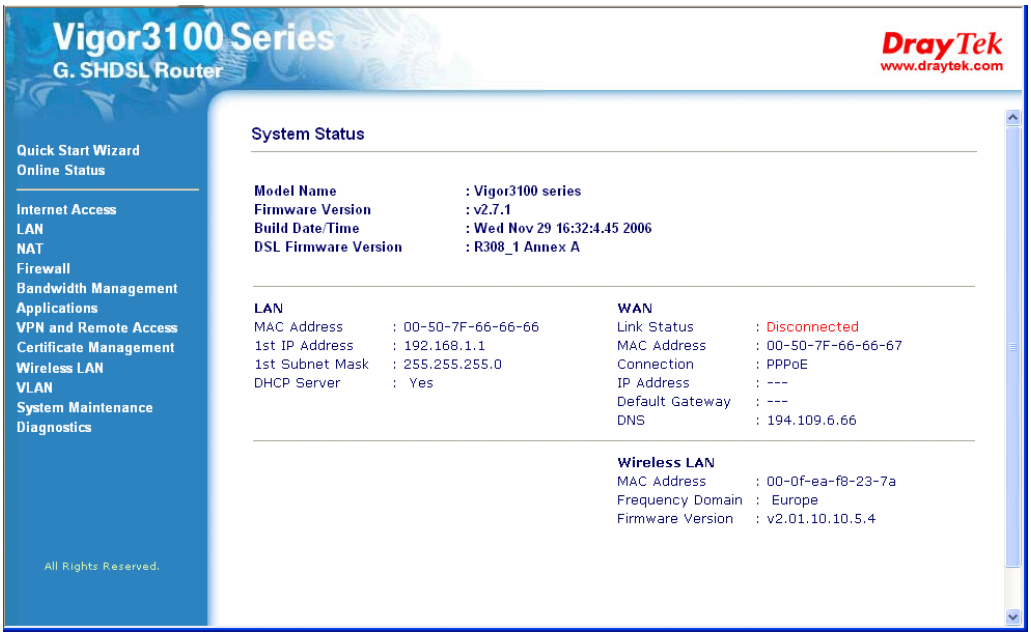
To change the password for this device, you have to access into the web browse with default password first.

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 **Confirm Password**. Then click **OK** to continue.

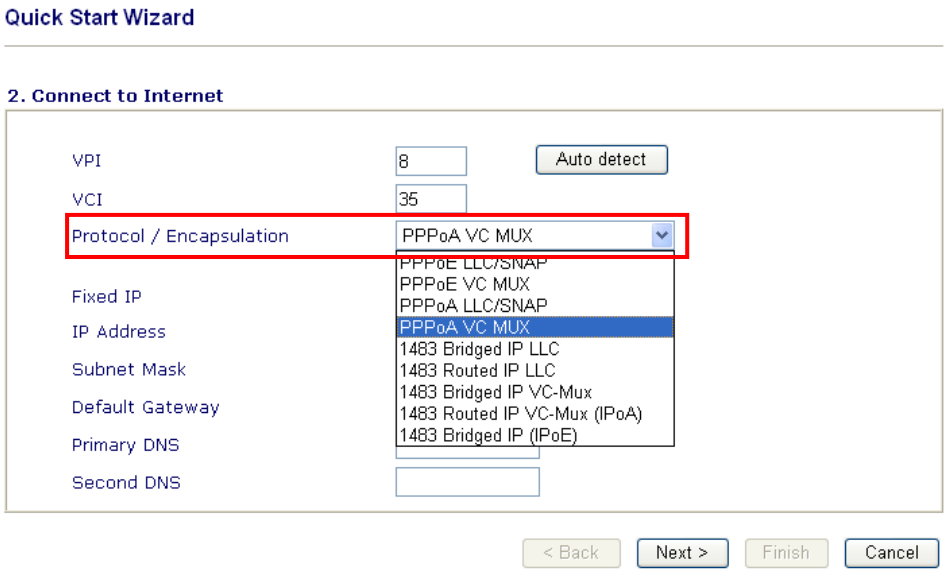
6. Now, the password has been changed. Next time, use the new password to access the Web Configurator for this router.

2.2 Quick Start Wizard

If your Vigor router can be under an environment with high speed NAT, the configuration provide here can help you to deploy and use the router quickly. There are two phases of quick setup, one is protocol/encapsulation configuration; and the other is LAN configuration.

2.2.1 Adjusting Protocol/Encapsulation

In the **Quick Start Wizard**, you can configure the router to access the Internet with different protocols/modes such as **PPPoE**, **PPPoA, Bridged IP, or Routed IP**. The router supports the Ethernet WAN interface for Internet access.



Now, you have to select an appropriate WAN connection type for connecting to the Internet through this router according to the settings that your ISP provided.

VPI	Stands for **Virtual Path Identifier**. It is an 8-bit header inside each ATM cell that indicates where the cell should be routed. The ATM, is a method of sending data in small packets of fixed sizes. It is used for transferring data to client computers.
VCI	Stands for **Virtual Channel Identifier.** It is a 16-bit field inside ATM cell's header that indicates the cell's next destination as it travels through the network. A virtual channel is a logical connection between two end devices on the network.
Protocol/Encapsulation	Select an IP mode for this WAN interface. There are several available modes for Internet access such as **PPPoE**, **PPPoA, Bridged IP** and **Routed IP**.
Fixed IP	Click **Yes** to specify a fixed IP for the router. Otherwise, click **No (Dynamic IP)** to allow the router choosing a dynamic IP. If you choose **No**, the following IP Address, Subnet Mask and Default Gateway will not be changed.
IP Address	Assign a private IP address for the protocol that you select.
Subnet Mask	Assign a subnet mask value for the protocol of **Routed IP** and **Bridged IP**.
Default Gateway	Assign a private IP address to the gateway for the protocol of **Routed IP** and **Bridged IP**.

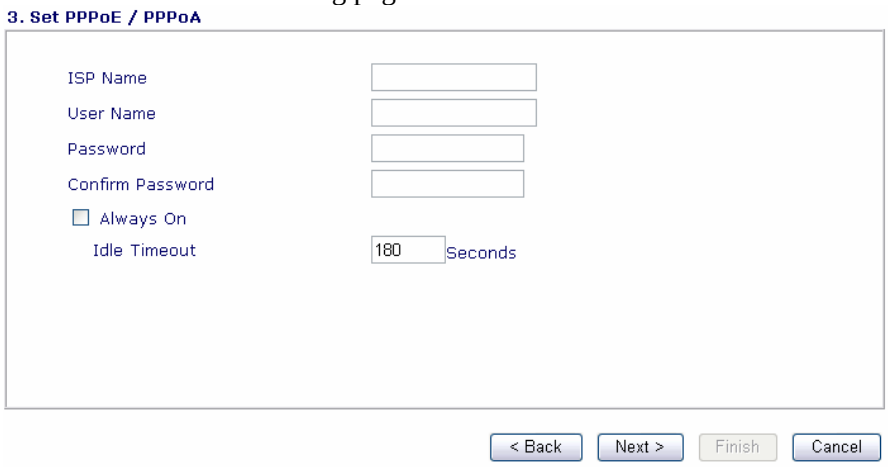
Primary DNS	Assign a private IP address to the primary DNS.
Second DNS	Assign a private IP address to the secondary DNS.

2.2.2 PPPoE/PPPoA

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. And the PPPoA stands for Point-to-Point Protocol over ATM. PPPoA uses the PPP dial-up protocol with ATM as the transport.

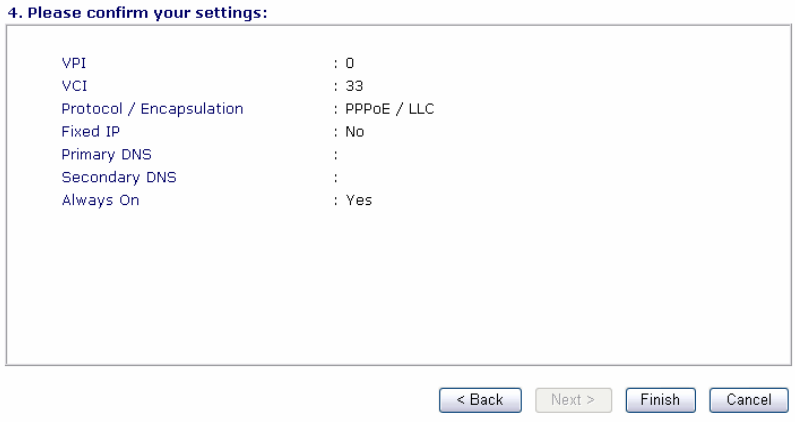
PPPoE or PPPoA is used for most of DSL modem users. All local users can share one PPPoE or PPPoA connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.

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

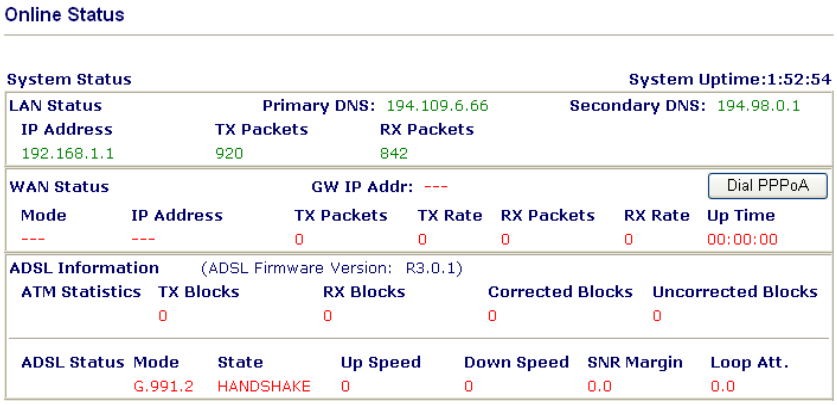


ISP Name	Assign a specific name for ISP requirement.
User Name	Assign a specific valid user name provided by the ISP.
Password	Assign a valid password provided by the ISP.
Confirm Password	Retype the password.
Always On	Check this box to allow the router connecting to Internet forever.
Idle Timeout	Type in the value (unit is second) as the idle timeout of the connection.

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

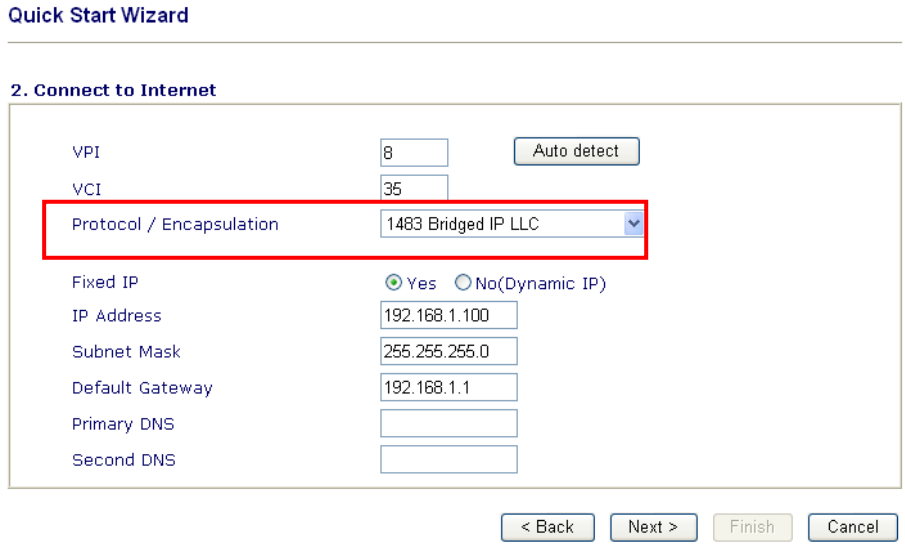


Click **Finish.** The online status of this protocol will be shown as below.

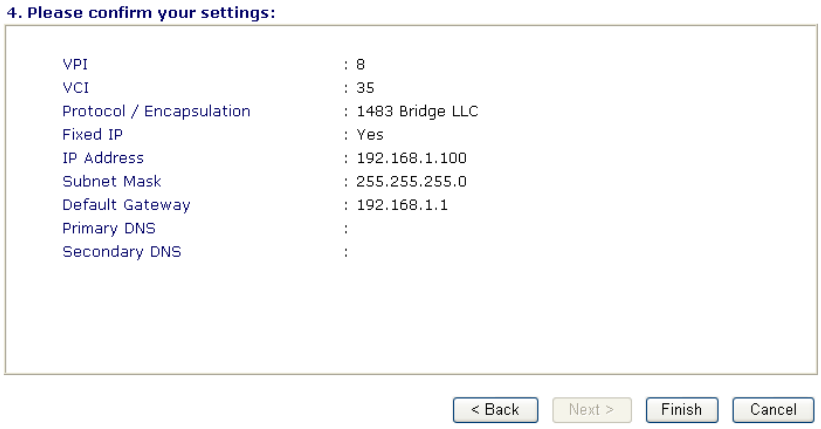


2.2.3 Bridged IP

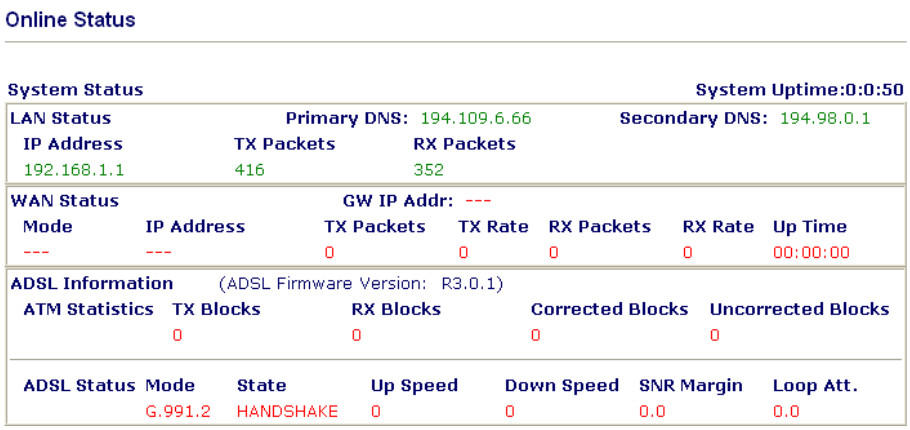
Click **1483 Bridged IP** as the protocol. Type in all the information that your ISP provides for this protocol.



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

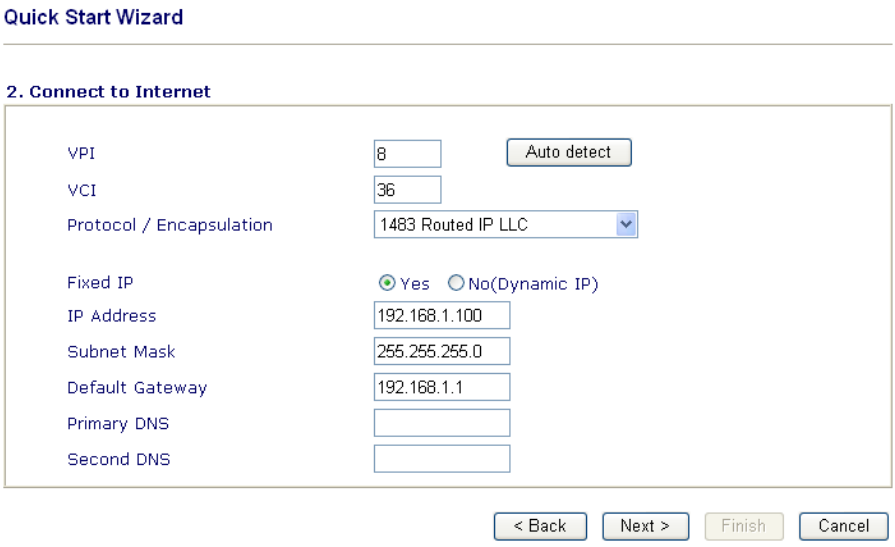


Click **Finish.** The online status of this protocol will be shown as below.

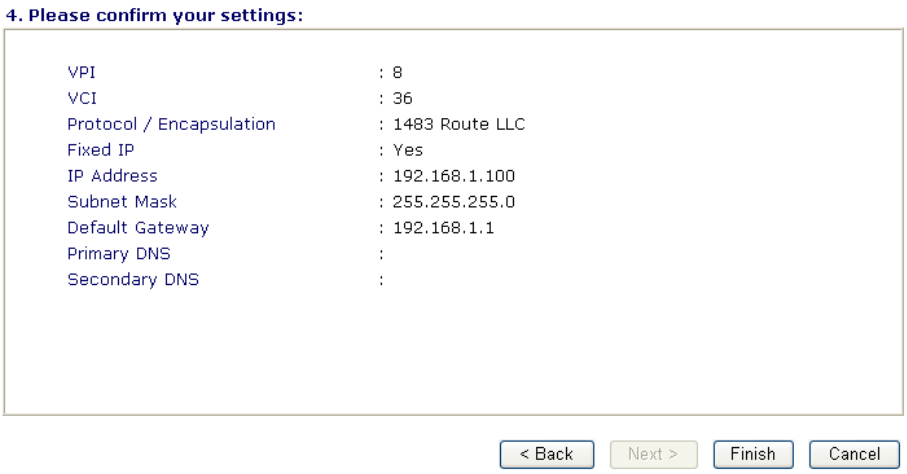


2.2.4 Routed IP

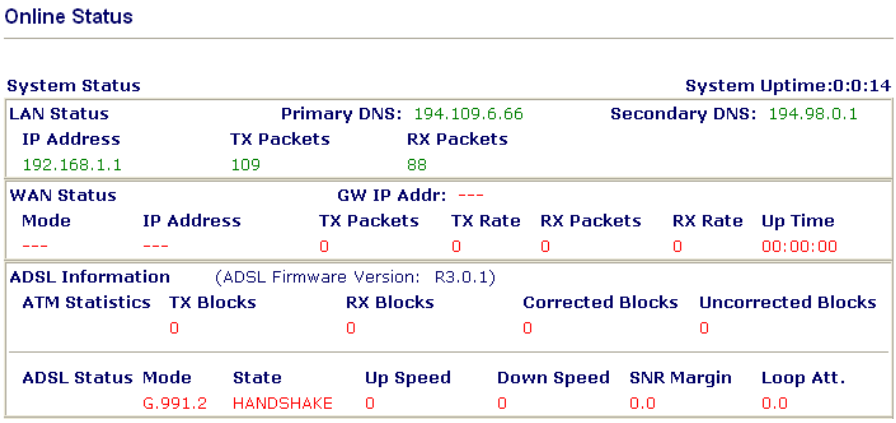
Click **1483 Routed IP** as the protocol. Type in all the information that your ISP provides for this protocol.



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



Click **Finish.** The online status of this protocol will be shown as below.



2.3 Selecting Correct Annex Type

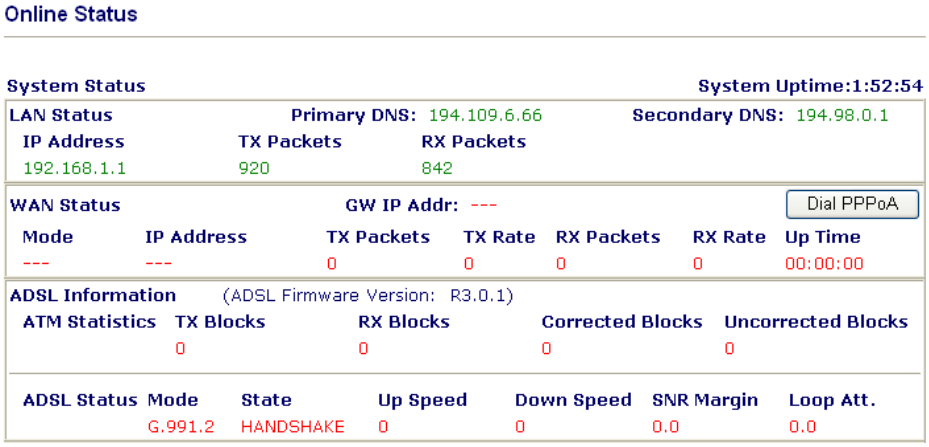
After finishing **Quick Start Wizard**, please go to **Internet Access** and choose **DSL Settings** for choosing correct annex type for your router.

Use the drop down list of **Annex Type** for choosing A or B according to the annex type of your router. If you do not choose the correct one, you will not access into Internet. This is very important.

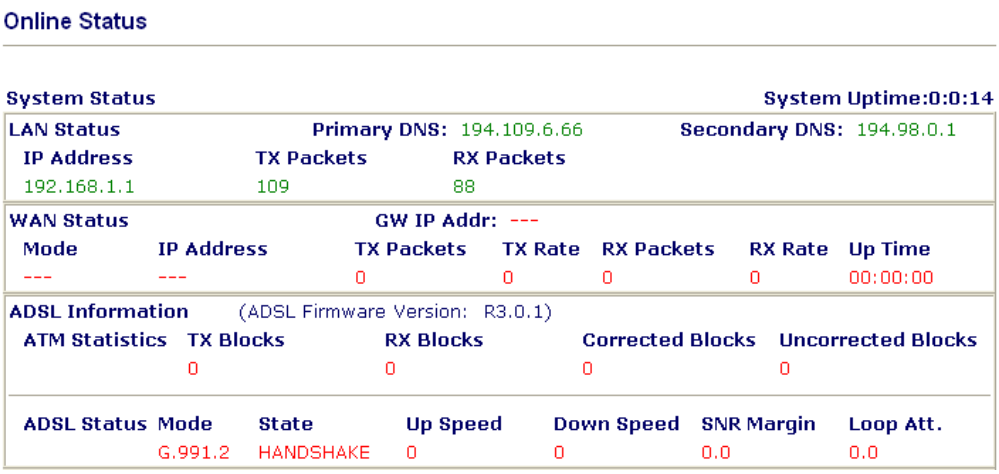
2.4 Online Status

Now, check the online status for your router. 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** or **PPPoA** as the protocol, you will find out a button of **Dial PPPoE** or **Dial PPPoE** in the Online Status web page.

Online status for PPPoA



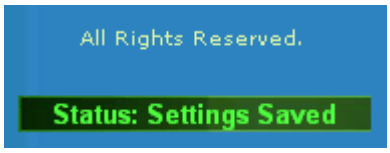
Online status for Routed IP



Primary DNS	Displays the assigned IP address of the primary DNS.
Secondary DNS	Displays the assigned IP address of the secondary DNS.
IP Address (in LAN)	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.
GW IP Addr:	Displays the assigned IP address of the default gateway.
IP Address (in WAN)	Displays the IP address of the WAN interface.
TX Rate	Displays the speed of transmitted packets at the WAN interface.
RX Rate	Displays the speed of received packets at the WAN interface.
Up Time	Displays the total system uptime of the interface.
ADSL Information	Displays the firmware version of this router.

2.5 Saving Configuration

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



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

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

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 Internet Access

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: 18

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

To acquire a public IP address from your ISP for Vigor router as a customer premises equipment, there are three common protocols: Point to Point Protocol over Ethernet (**PPPoE), PPPoA and MPoA**. **Multi-PVC** is provided for more advanced setup of the above.

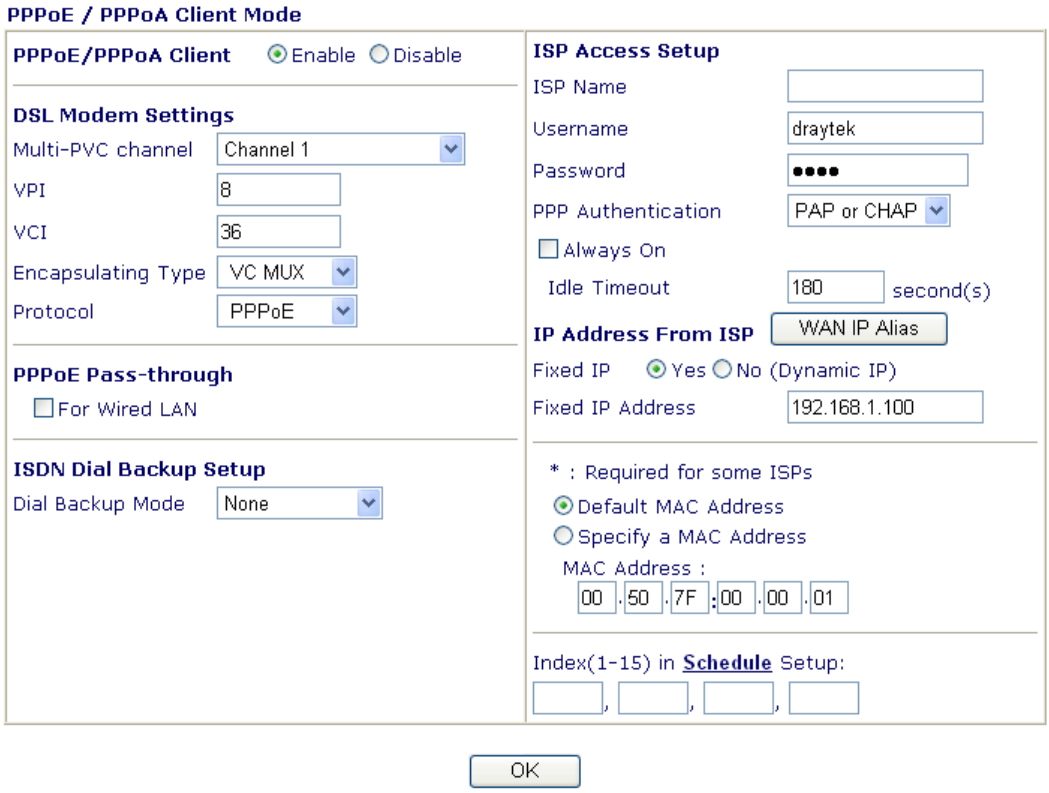
In ADSL deployment, the PPP (Point to Point)-style authentication and authorization is required for bridging customer premises equipment (CPE). Point to Point Protocol over Ethernet (PPPoE) connects a network of hosts via an access device to a remote access concentrator or aggregation concentrator. This 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.

3.1.2 PPPoE/PPPoA

PPPoA, included in RFC1483, can be operated in either Logical Link Control-Subnetwork Access Protocol or VC-Mux mode. As a CPE device, Vigor router encapsulates the PPP session based for transport across the ADSL loop and your ISP's Digital Subscriber Line Access Pultiplexer (SDLAM).

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



PPPoE/PPPoA 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.

DSL Modem Settings Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP.
Multi-PVC channel – The selections displayed here are determined by the page of **Internet Access** – **Multi PVCs**. **Select M-PVCs Channel** means no selection will be chosen.
VPI - Type in the value provided by ISP.
VCI - Type in the value provided by ISP.
Encapsulating Type - Drop down the list to choose the type provided by ISP.
Protocol - Drop down the list to choose the one provided by ISP.
If you have already used **Quick Start Wizard** to set the protocol, then it is not necessary for you to change any settings in this group.

PPPoE Pass-through

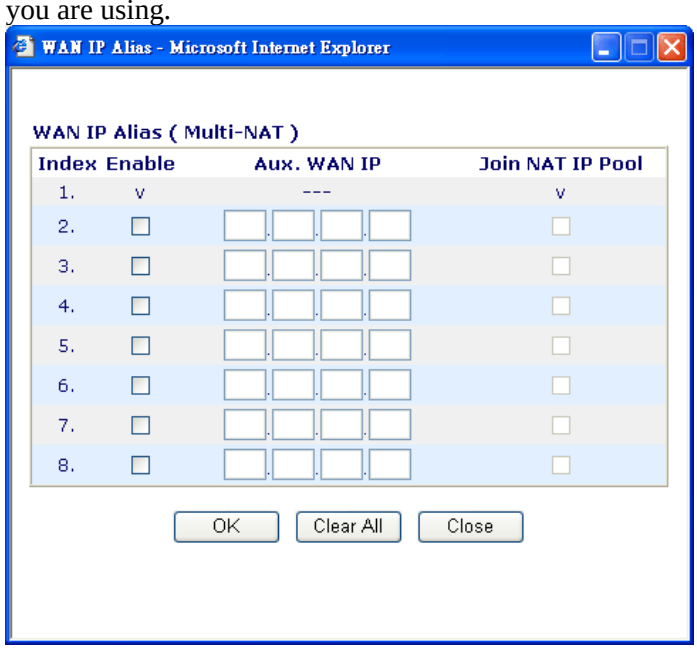
The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router.
For Wired LAN – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet.

ISP Access Setup

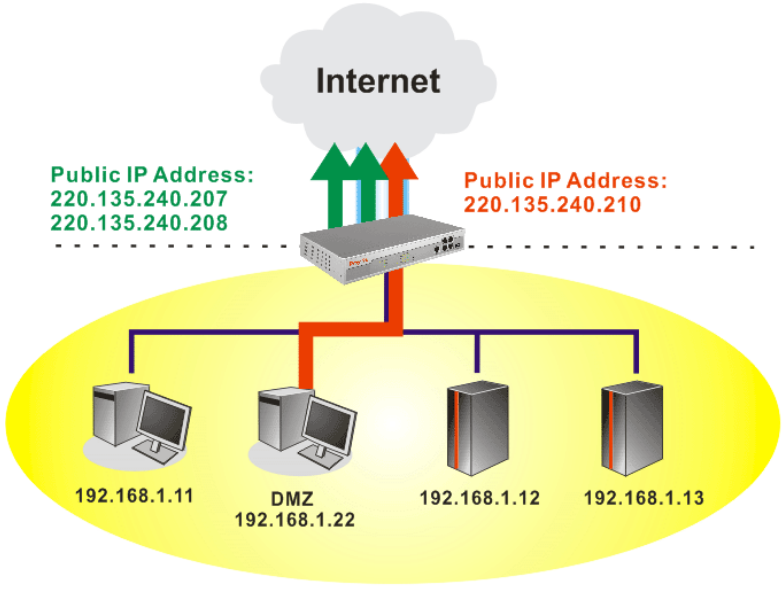
Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check **Always On**.
ISP Name – Type in the ISP Name provided by ISP in this field.
Username – Type in the username provided by ISP in this field.
Password – Type in the password provided by ISP in this field.
PPP Authentication – Select **PAP only** or **PAP or CHAP** for PPP.
Always On – Check this box if you want the router keeping connecting to Internet forever.
Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action.

IP Address From ISP

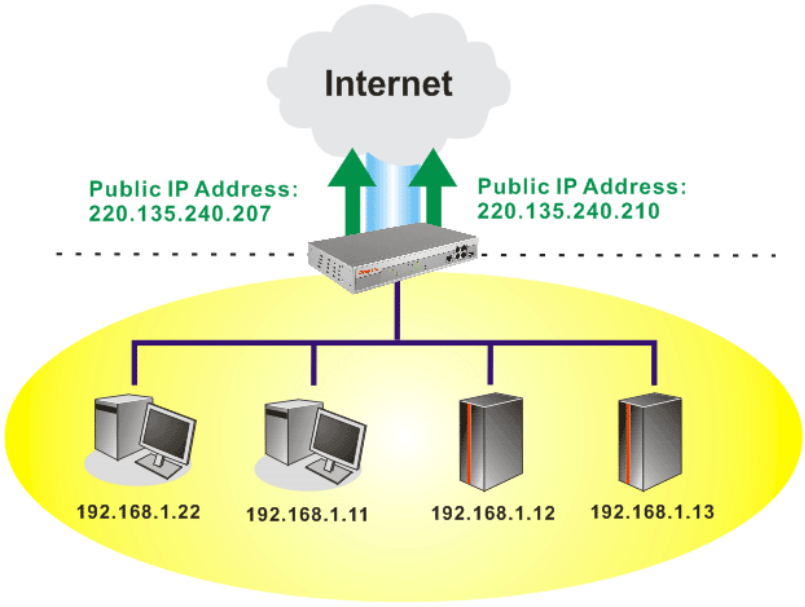
Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want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



By checking the checkbox **Join NAT IP Pool**, data from NAT hosts will be round-robin forwarded on a session basis.



If you do not check **Join NAT IP Pool**, you can still use these public IP addresses for other purpose, such as DMZ host, Open Ports.



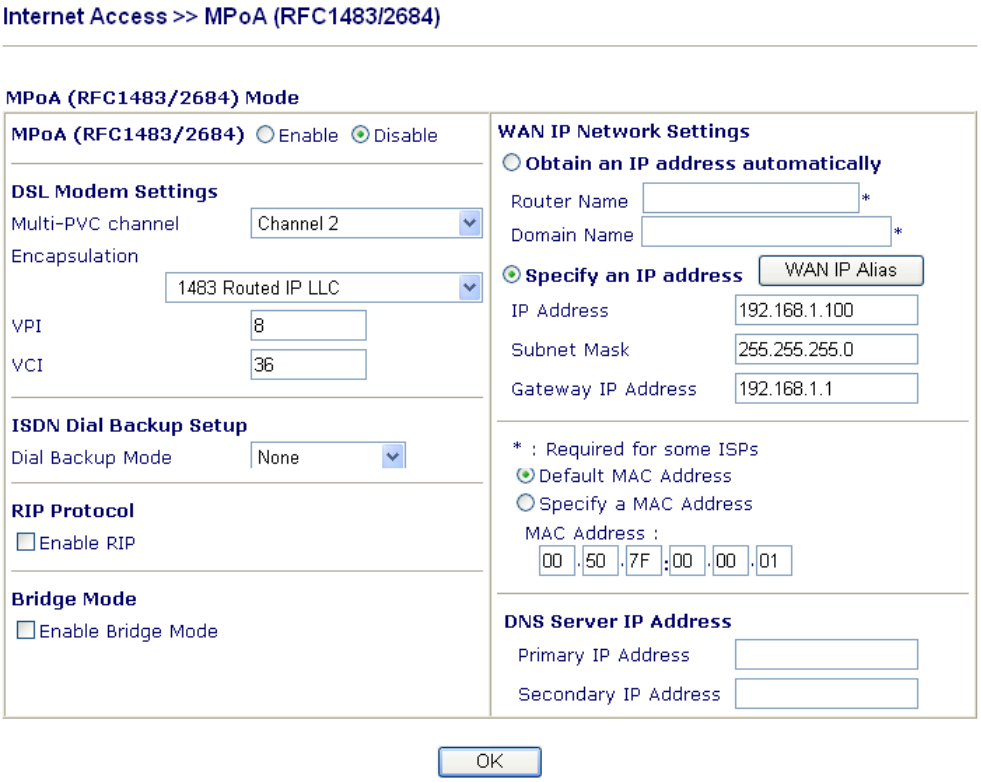
Default MAC Address	Type in MAC address for the router. You can use **Default MAC Address** or specify another MAC address for your necessity. MAC Address – Type in the MAC address for the router manually.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All 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.

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

3.1.3 MPoA

MPoA is a specification that enables ATM services to be integrated with existing LANs, which use either Ethernet, token-ring or TCP/IP protocols. The goal of MPoA is to allow different LANs to send packets to each other via an ATM backbone.

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



MPoA(RFC1483/2684) 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.

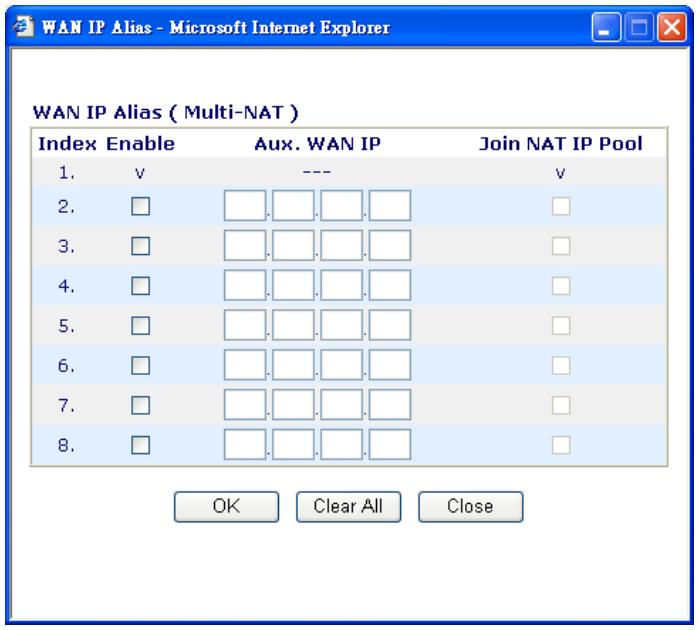
DSL Modem Settings Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP.
Multi-PVC channel - The selections displayed here are determined by the page of **Internet Access** – **Multi PVCs**. **Select M-PVCs Channel** means no selection will be chosen.
Encapsulating Type - Drop down the list to choose the type provided by ISP.
VPI - Type in the value provided by ISP.
VCI - Type in the value provided by ISP.

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

Bridge Mode If you choose **Bridged IP** as the protocol, you can check this box to invoke the function.

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

Obtain an IP address automatically – Click this button to obtain the IP address automatically.
Router Name – Type in the router name provided by ISP.
Domain Name – Type in the domain name that you have assigned.
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.



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

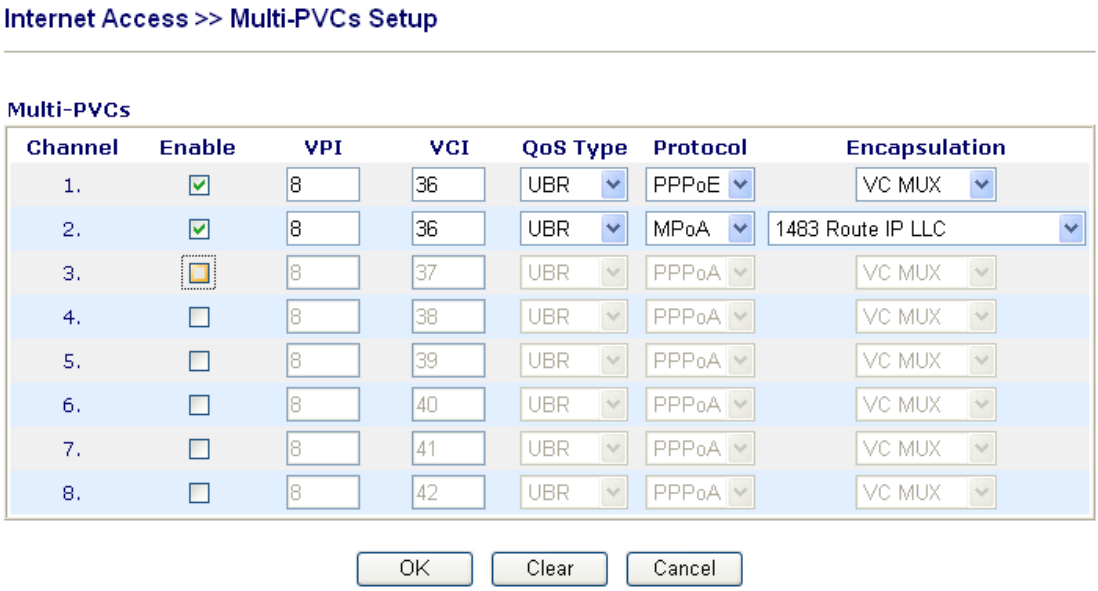
Default MAC Address — Type in MAC address for the router. You can use **Default MAC Address** or specify another MAC address for your necessity.
MAC Address – Type in the MAC address for the router manually.

DNS Server IP Address — Type in the primary IP address for the router. If necessary, type in secondary IP address for necessity in the future.

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

3.1.4 Multi-PVCs

This router allows you to create multi-PVCs for different data transferring for using. Simply go to **Internet Access** and select **Multi-PVC Setup** page.

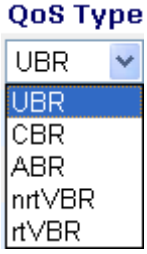


Enable Type in the primary IP address for the router. If necessary, type

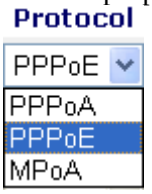
VPI Type in the value provided by your ISP.

VCI Type in the value provided by your ISP.

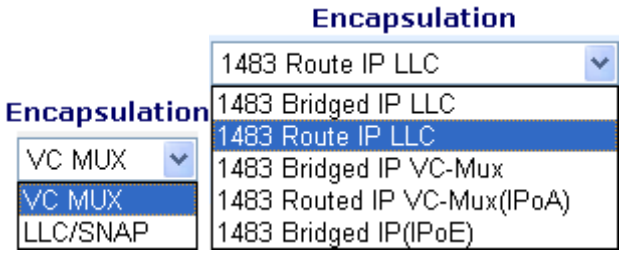
QoS Type Select a proper QoS type for the channel.



Protocol Select a proper protocol for this channel.



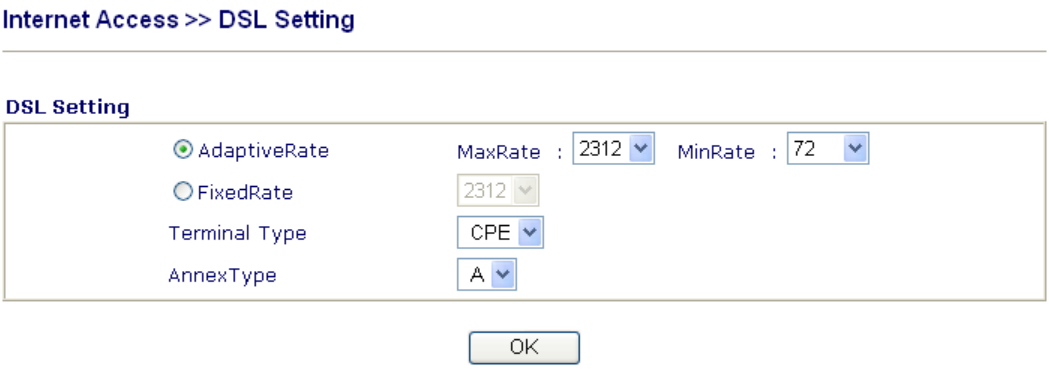
Encapsulation Choose a proper type for this channel. The types will be different according to the protocol setting that you choose.



3.1.5 DSL Settings

DSL is one technology that dramatically increases the digital capacity of ordinary telephone lines (the local loops) into the home or office. The speed of DSL is based on the distance between the customer and telco central office.

Below shows settings for Vigor3100 and Vigor3100G.

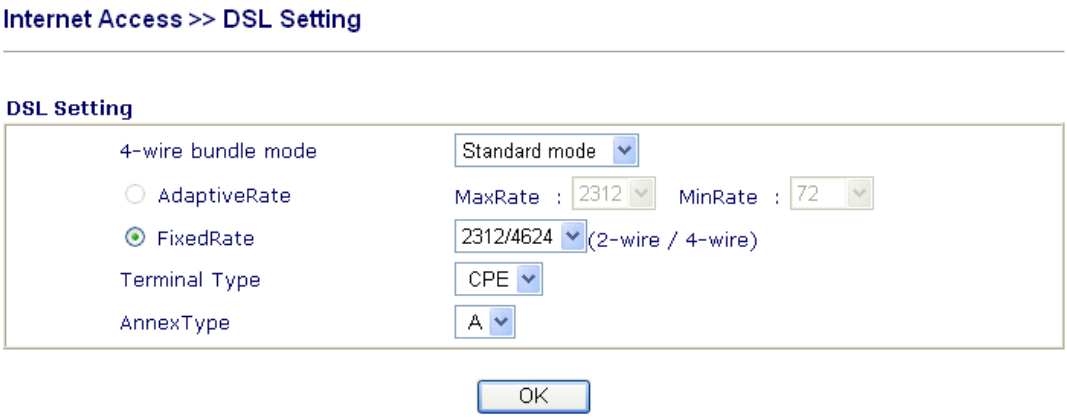


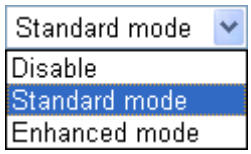
AdaptiveRate Set the connection rate for the network.

MaxRate Select the maximum rate for this setting. Use the drop down list to select the one that suits your router. The default value is 2312.

MinRate	Select the minimum rate for this setting. Use the drop down list to select the one that suits your router. The default value is 72.
FixedRate	If you select this one, only the fixed value is useful.
Terminal Type	Determine the role of this device as a CPE or CO.
Annex Type	Choose the correct annex type (A or B) for your router.

Vigor3120 offers different DSL settings with Vigor 3100 and Vigor3100G due to its feature of 4-wire bundle mode.



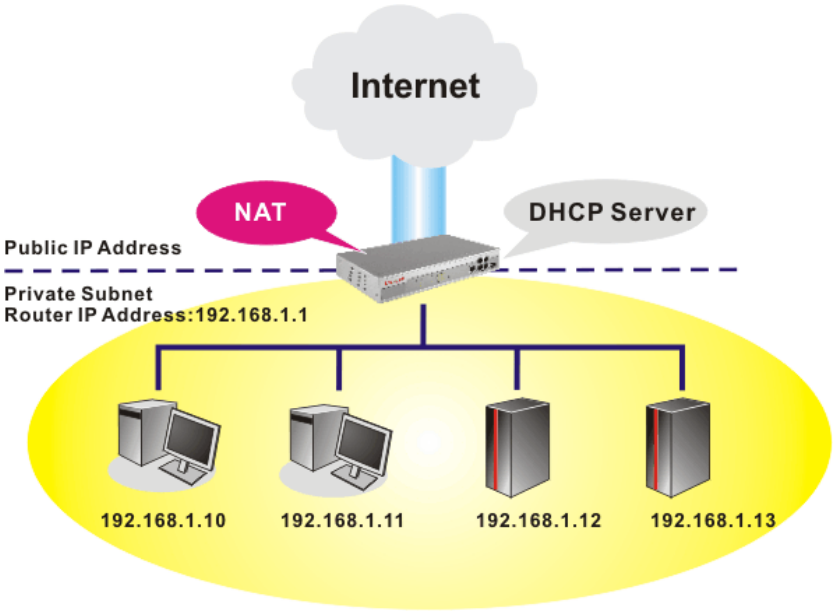
4-wire bundle mode	To have wider bandwidth in network transmission, please choose proper mode in this field. Basically, you can just select the proper one according to the mode that your ISP provides. And you can set FixedRate setting only if you select **Standard mode** or **Enhanced mode** here.  Enhanced mode allows network connection via 2-wire instead if connection via 4-wire fails.
FixedRate	If you select **Standard mode** or **Enhanced mode** on 4-wire bundle mode, only the fixed rate is available for line speed. Please use the drop down list to choose the one that you subscribe.
Terminal Type	Determine the role of this device as a CPE or CO.
Annex Type	Choose the correct annex type (A or B) for your router.

3.2 LAN

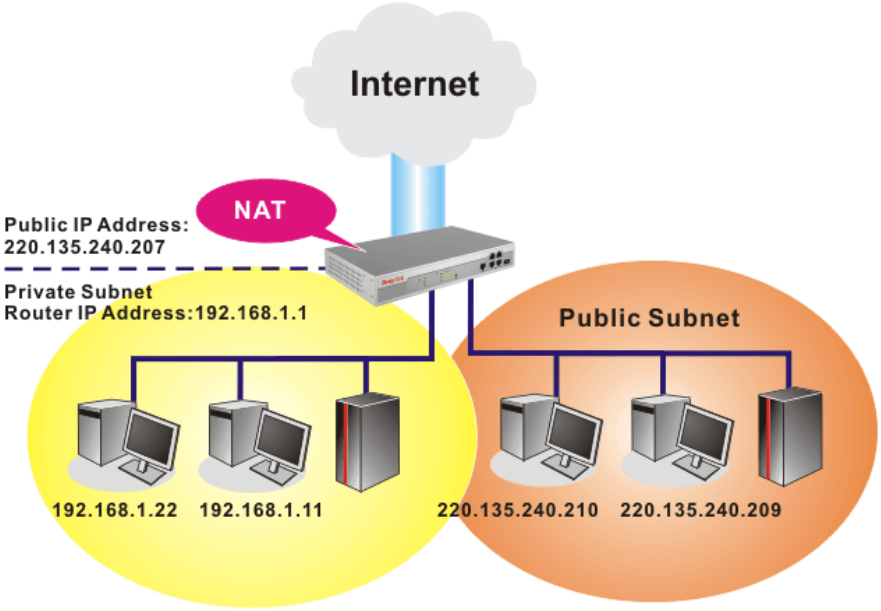
Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

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)

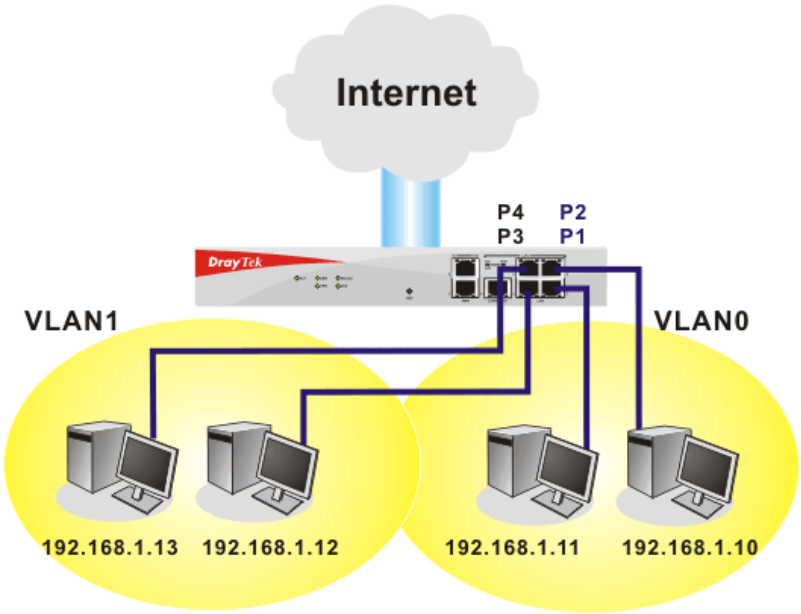
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

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

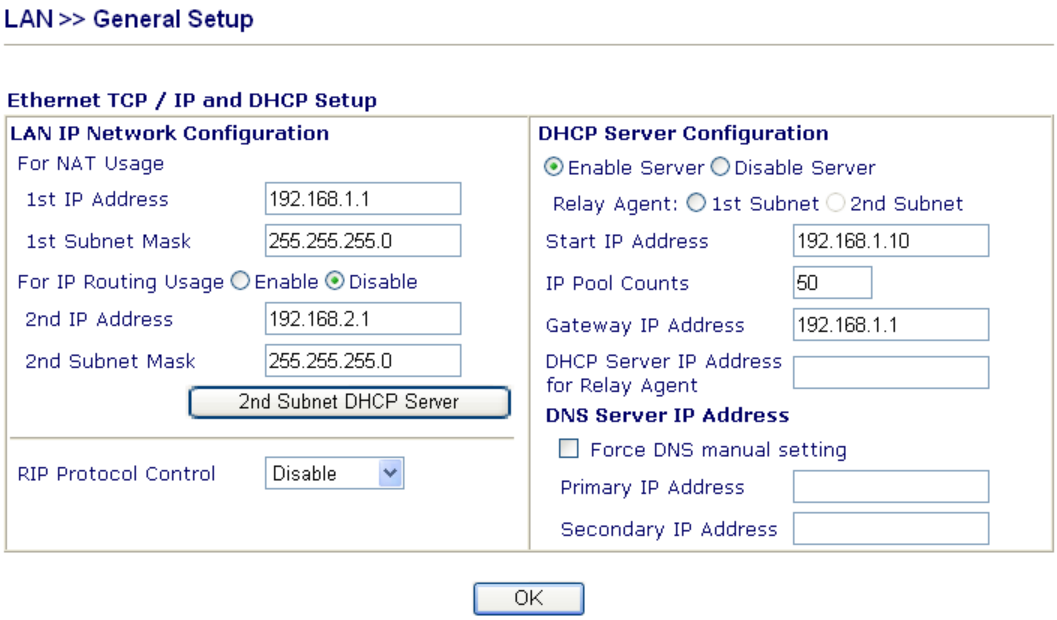
You can group local hosts by physical ports and create up to 4 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.



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).

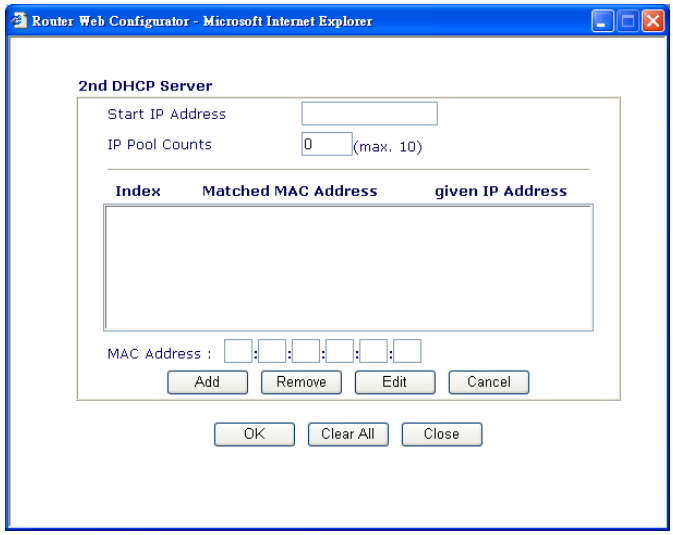
1st Subnet Mask Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)

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.

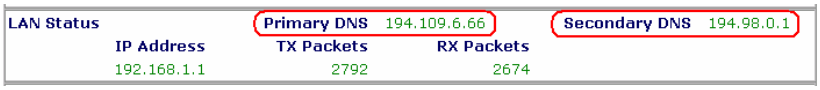
If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
Enable Server - Let the router assign IP address to every host in the LAN.
Disable Server – Let you manually assign IP address 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 -
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:



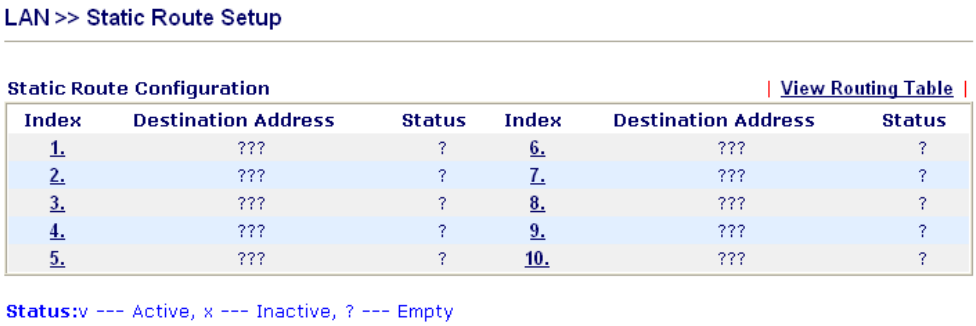
If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.

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.

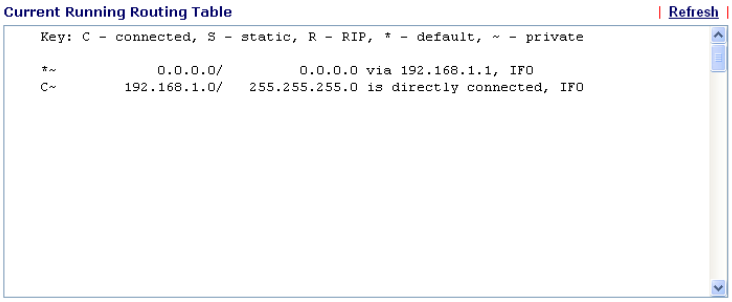
There are two common scenarios of LAN settings that stated in Chapter 4. For the configuration examples, please refer to that chapter to get more information for your necessity.

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 setup 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.

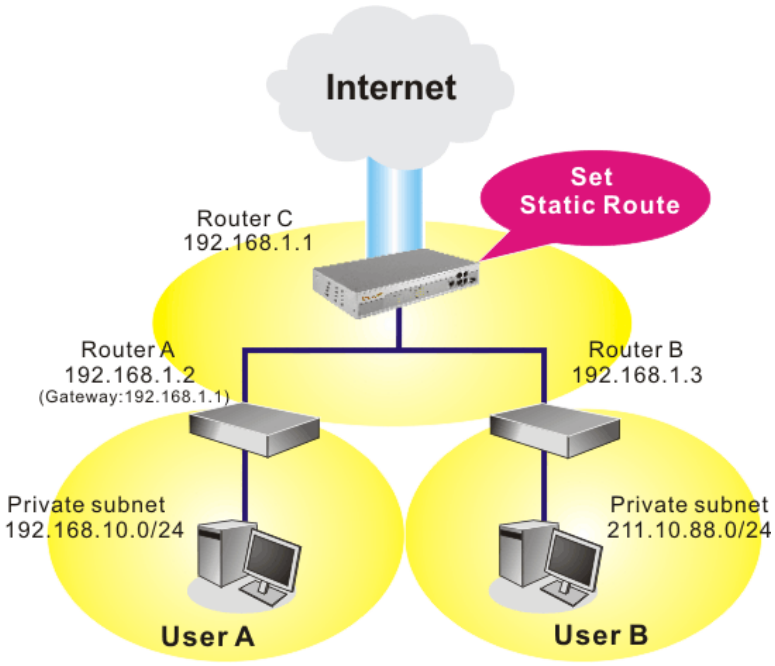


Add Static Routers to Private and Public Networks

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.

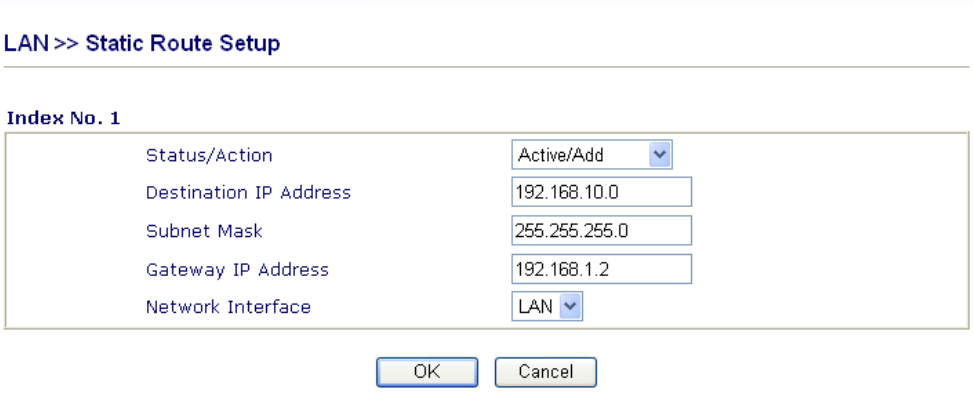


1. Go to **LAN** page and click **General Setup**, select 1st Subnet as the **RIP Protocol Control.** Then click the **OK** button.

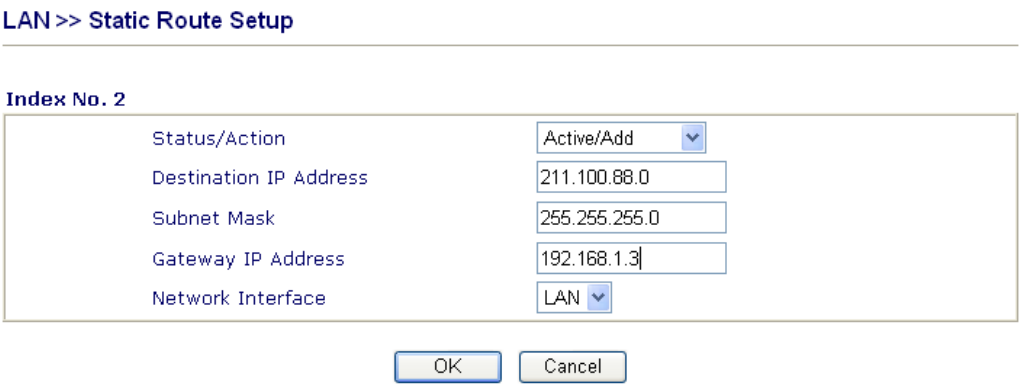
Note: There are two reasons that we have to apply RIP Protocol Control on 1st Subnet. The first is that the LAN interface can exchange RIP packets with the neighboring routers via the 1st subnet (192.168.1.0/24). The second is that those hosts on the internal private subnets (ex. 192.168.10.0/24) can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

---

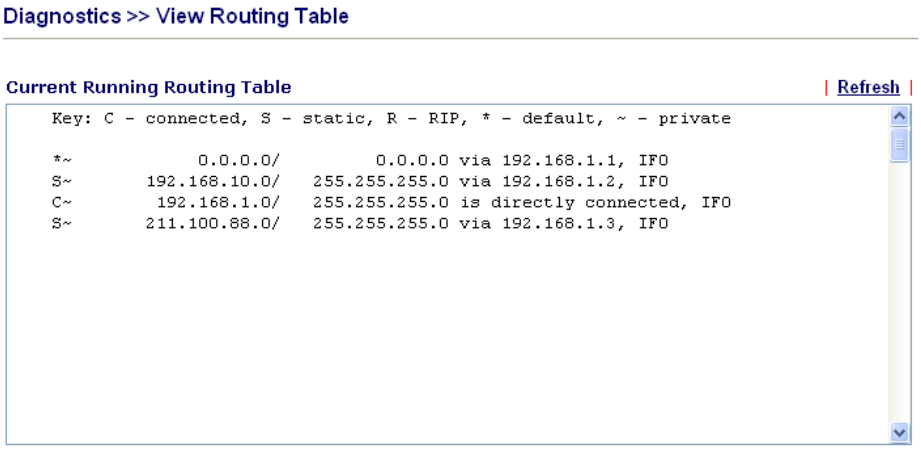
2. Click the **LAN - Static Route** and click on the **Index Number 1.** Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click **OK**.



3. 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.

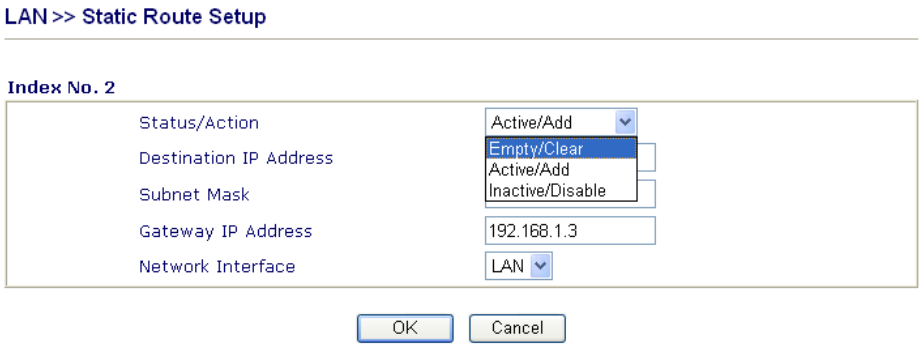


4. Go to **Diagnostics** and choose **Routing Table** to verify current routing table.



Disable Static Route

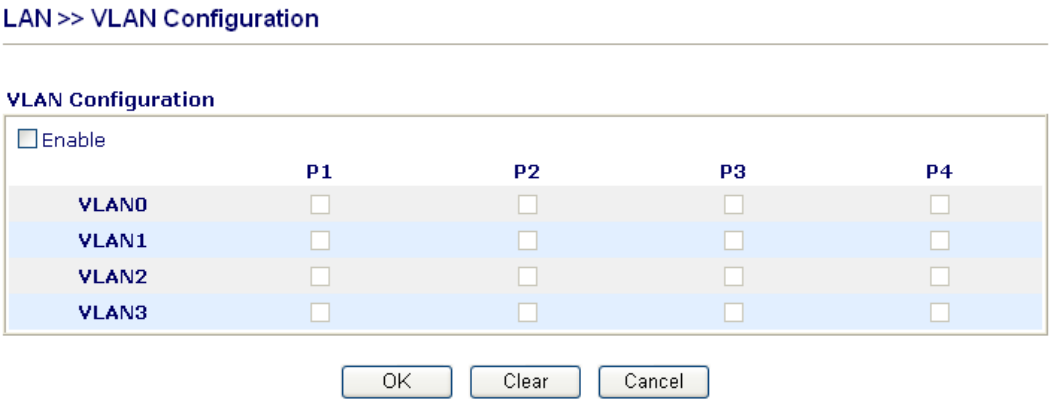
1. Click the **Index Number** that you want to disable from the **Static Route Configuration** page.
2. Select **Inactive/Disable** from the drop-down menu, and then click the **OK** button to disable the route.



3.2.4 VLAN

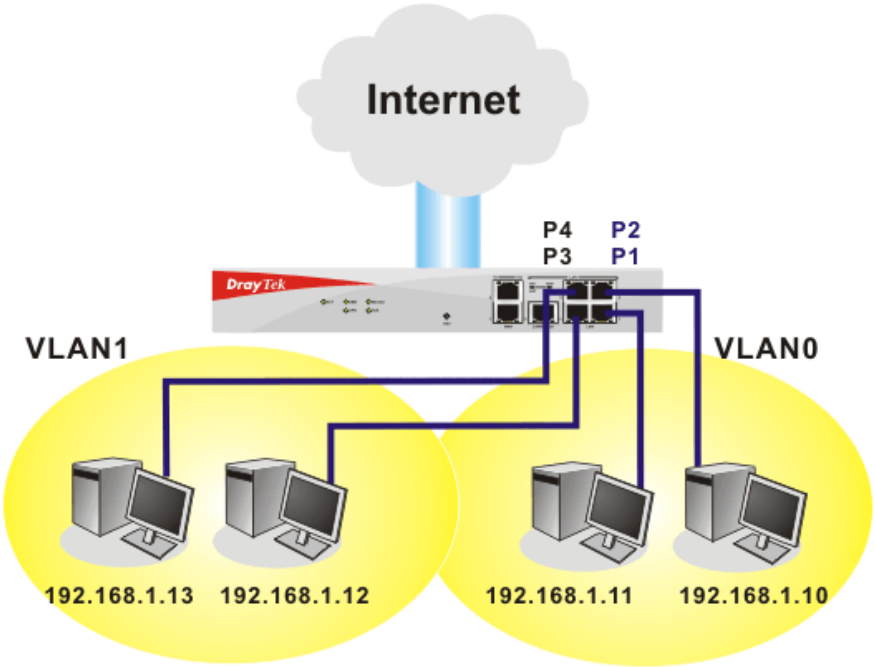
Note: This menu is available for **Vigor3100** and **Vigor3120** model. For Vigor3100G, please refer to 3.10.

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.

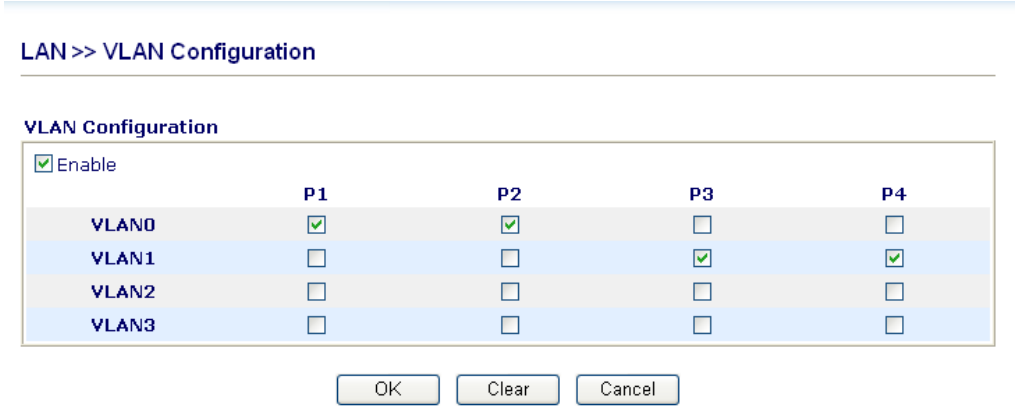


To add or remove a VLAN, please refer to the following example.

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.

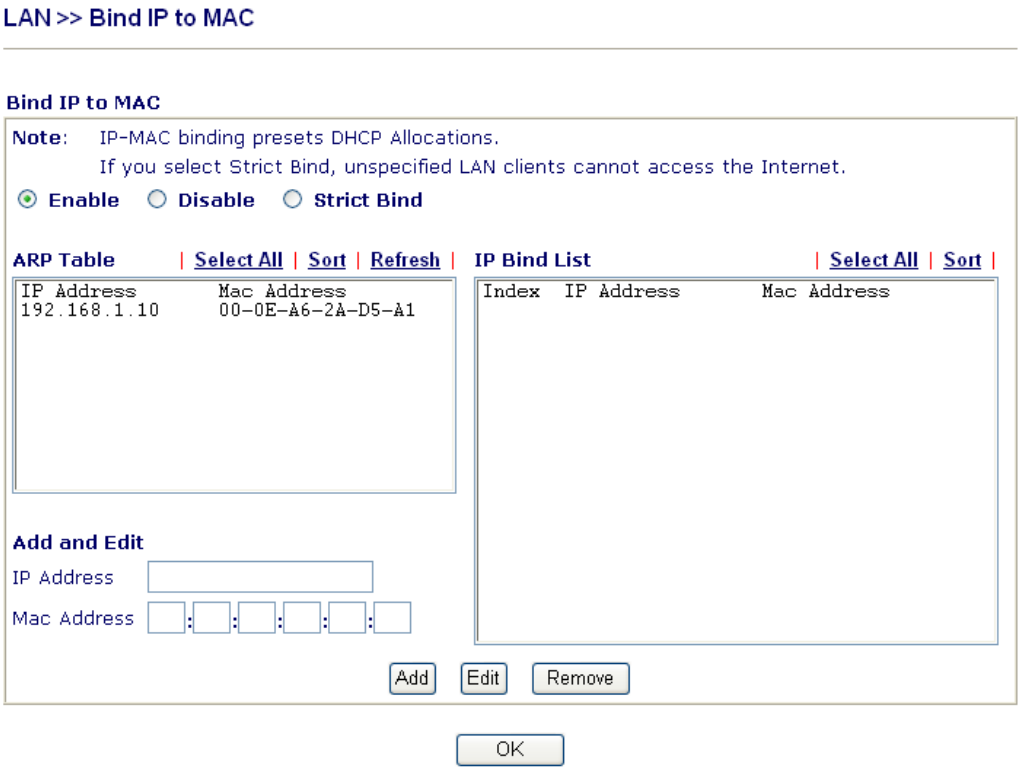


3. To remove VLAN, uncheck the needed box and click **OK** to save the results.

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.
Remove	You can remove any item listed in **IP Bind List**. Simply click and select the one, and click **Remove**. 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.

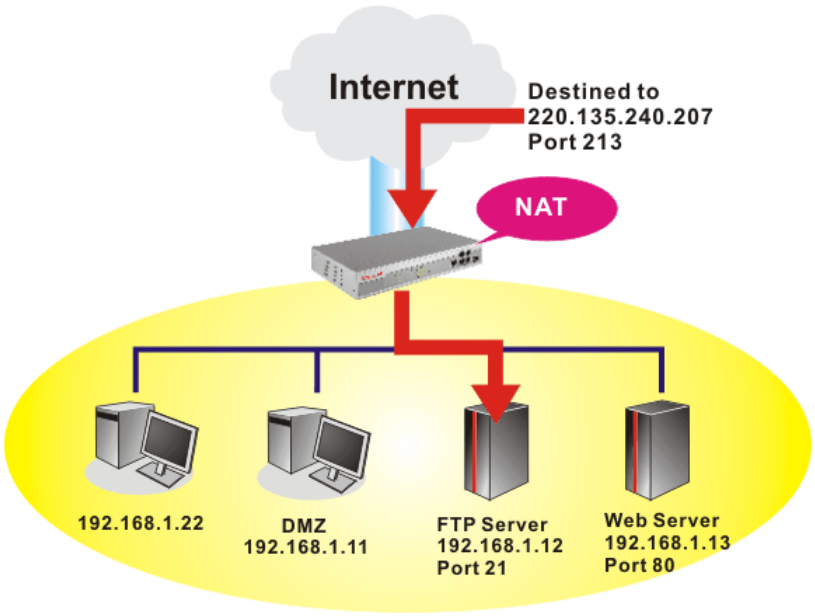
The benefit of the NAT includes:

- **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.

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. The server users inside the LAN can not access public IP address of the server. The correct route is to access the server using the local private IP address of the server, or you should set up an alias in a Windows hosts file. Please only redirect the ports you know you have to forward rather than forward all ports. Otherwise, you will compromise the firewall-type security initially deployed by the NAT facility.

To use this function, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 10 port-mapping entries for the internal hosts.

NAT >> Configure Port Redirection Table

Port Redirection Table

Index	Service Name	Protocol	WAN IP	Public Port	Private IP	Private Port	Active
1		---	3.WAN IP Alias[2]	0		0	☐
2		---	3.WAN IP Alias[2]	0		0	☐
3		---	3.WAN IP Alias[2]	0		0	☐
4		---	3.WAN IP Alias[2]	0		0	☐
5		---	1.All 2.WAN IP Alias[1]---	0		0	☐
6		---	3.WAN IP Alias[2]	0		0	☐
7		---	4.WAN IP Alias[3] 5.WAN IP Alias[4]	0		0	☐
8		---	6.WAN IP Alias[5] 7.WAN IP Alias[6]	0		0	☐
9		---	8.WAN IP Alias[7] 9.WAN IP Alias[8]	0		0	☐
10		---	3.WAN IP Alias[2]	0		0	☐

OK

Service Name Enter the description of the specific network service.

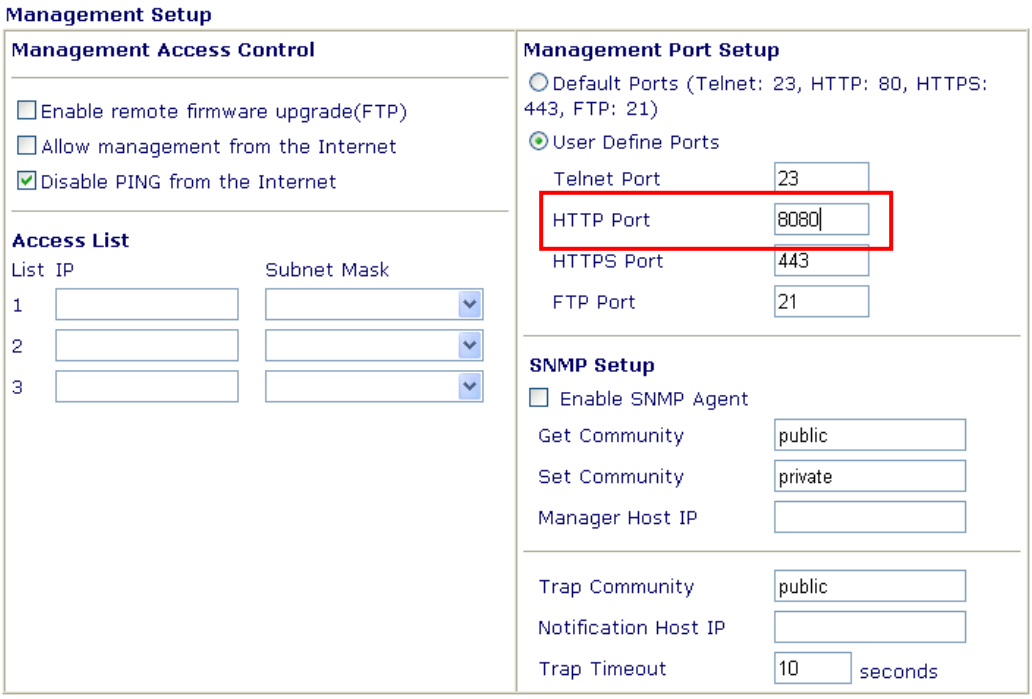
Protocol Select the transport layer protocol (TCP or UDP).

WAN IP Select one of the WAN IP selections for port redirection. Only the selected WAN IP with incoming data will be redirected to the specified IP. If you choose **All**, all incoming traffic through any

	WAN IP will be transferred to the IP address specified in this web page.
Public Port	Specify which port can be redirected to the specified **Private IP and Port** of the internal host.
Private IP	Specify the private IP address of the internal host providing the service.
Private Port	Specify the private port number of the service offered by the internal host.
Active	Check this box to activate the port-mapping entry you have defined.

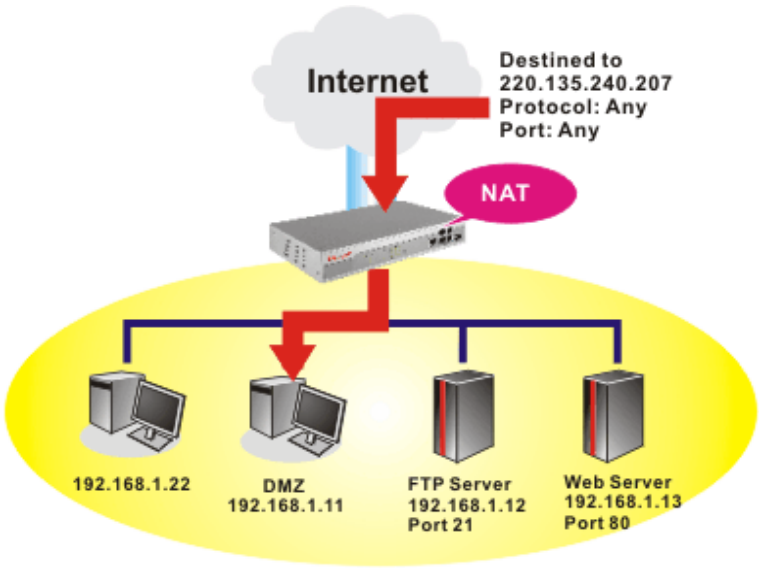
Note that the router has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the router's in order to avoid confliction.

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**. 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.



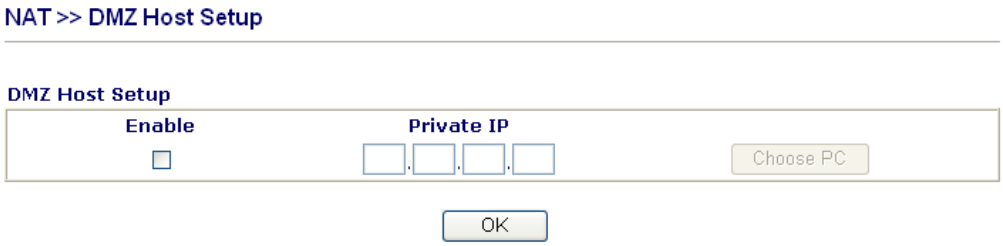
3.3.2 DMZ Host

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 map 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.



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.

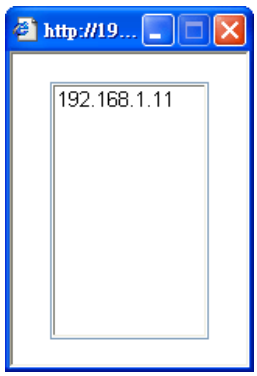
Click **DMZ Host** to open the following page:



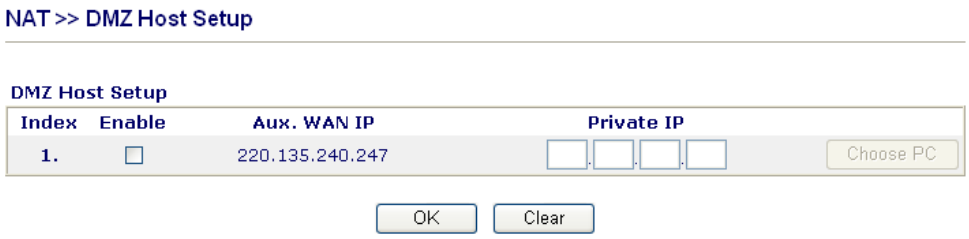
Enable Check to enable the DMZ Host function.

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.



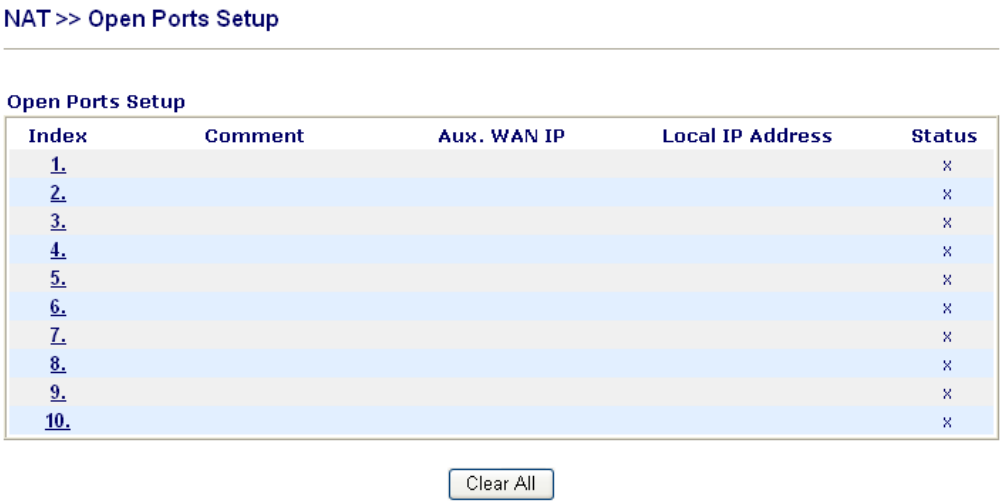
If you previously have set up **WAN Alias** in **Internet Access>>PPPoE/PPPoA** or **Internet Access>>MPoA,** you will find them in **Aux. WAN IP list** for your selection.



3.3.3 Open Ports

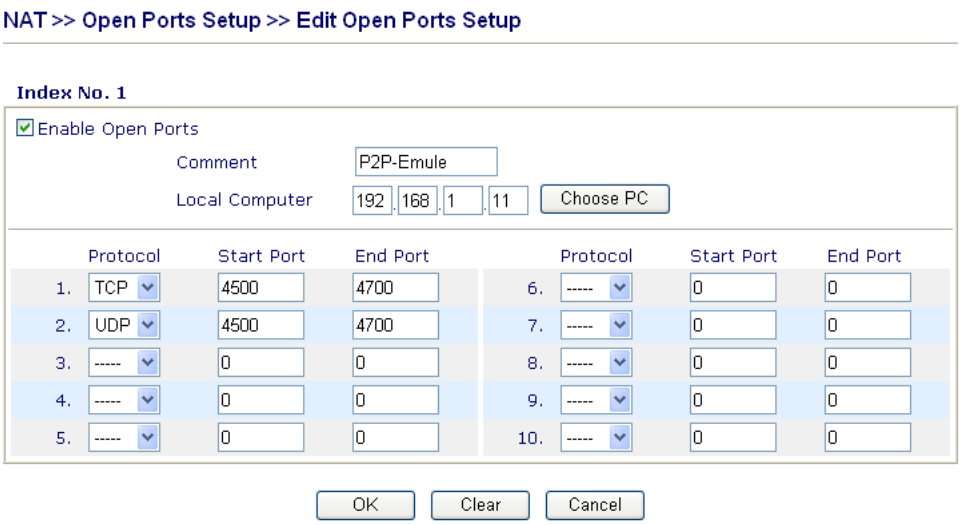
Open Ports allows you to open a range of ports for the traffic of special applications. Common application of Open Ports includes P2P application (e.g., BT, KaZaA, Gnutella, WinMX, eMule and others), Internet Camera etc. Ensure that you keep the application involved up-to-date to avoid falling victim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

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

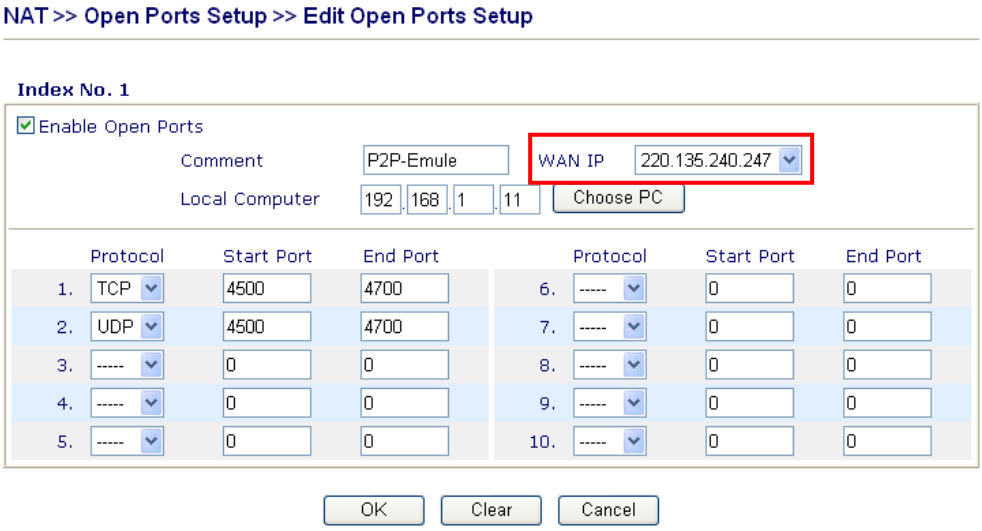


Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
Comment	Specify the name for the defined network service.
Aux. WAN IP	Display the private IP address of the local host that you specify in WAN Alias.
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.



However, if you previously have set up **WAN Alias** in **Internet Access>>PPPoE/PPPoA** or **Internet Access>>MPoA,** you will find that **WAN IP** appeared for your selection.



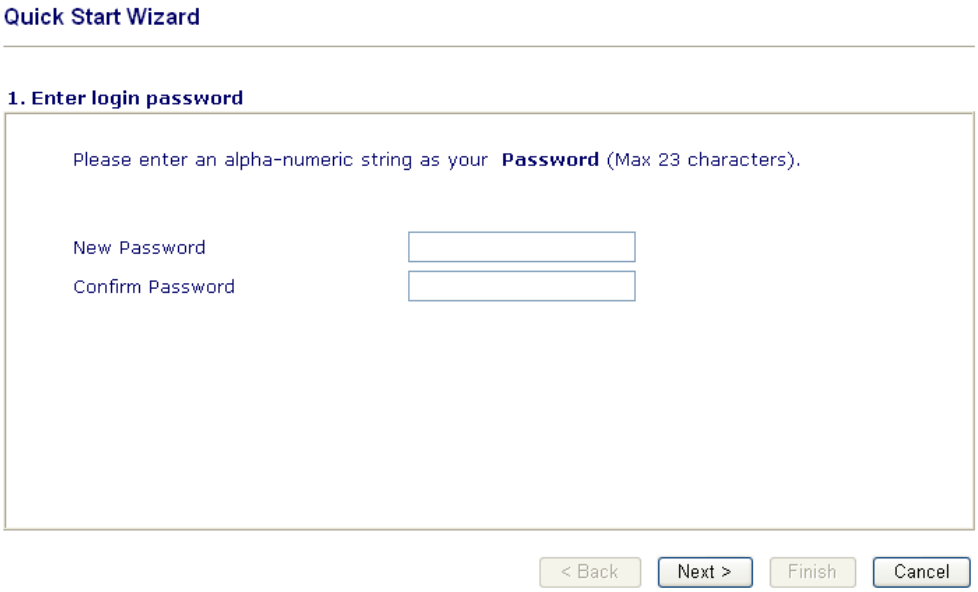
Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
Local Computer	Enter the private IP address of the local host or click Choose PC to select one.
Choose PC	Click this button and, subsequently, a window having a list of private IP addresses 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 Firewall

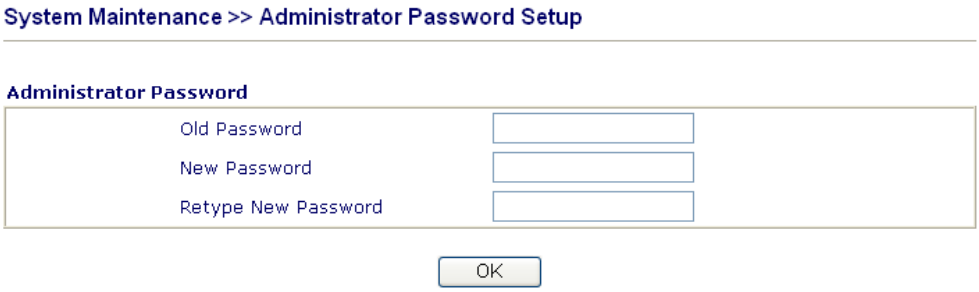
3.4.1 Basics for Firewall

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:

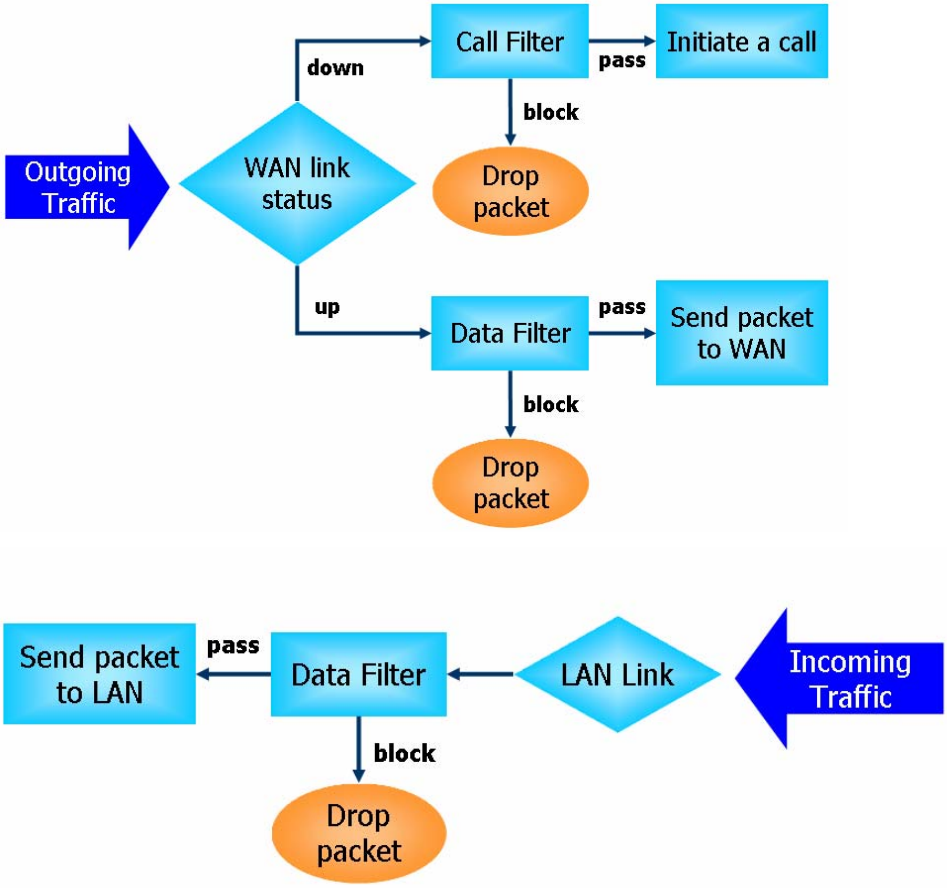
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection
- URL Content Filter

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.

Instant Messenger (IM) and Peer-to-Peer (P2P) Application Blocking

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. To address these needs, we provide IM and P2P blocking functionality.

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

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

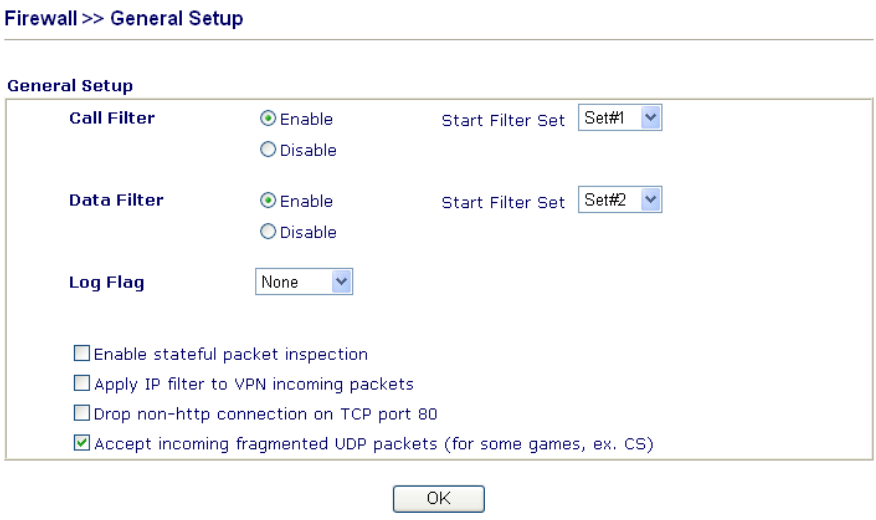
We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary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

3.4.2 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, **Enable Stateful packet inspection**, **Apply IP filter to VPN incoming packets**, **Drop non-http connection on TCP port 80**, and **Accept incoming fragmented UDP packets**.

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.

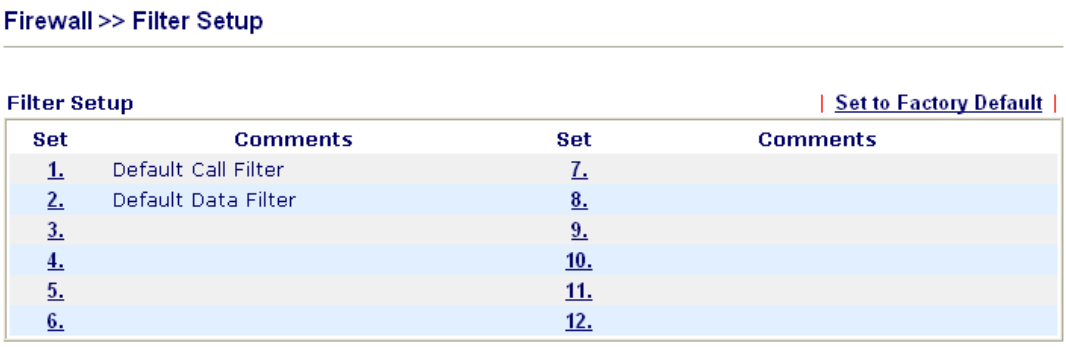
Log Flag — For troubleshooting needs you can specify the filter log here.
None - The log function is not activated.

Block - All blocked packets will be logged.
Pass - All passed packets will be logged.
No Match - The log function will record all packets that are not matched.
Note that the filter log will be displayed on the Telnet terminal when you type the ***log -f*** command.

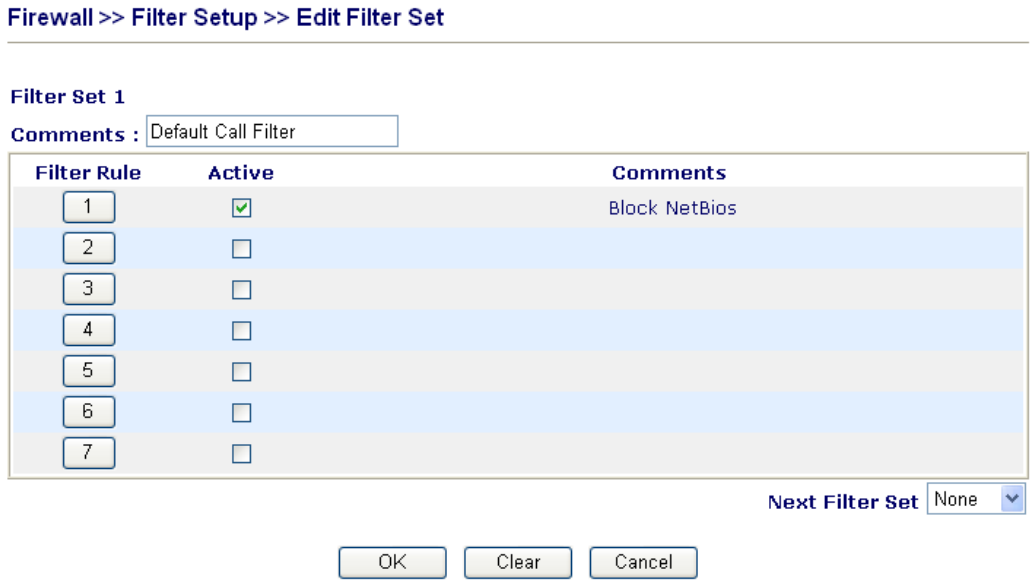
Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable "Accept Incoming Fragmented UDP Packets". By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable "Accept Incoming Fragmented UDP Packets".

3.4.3 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.

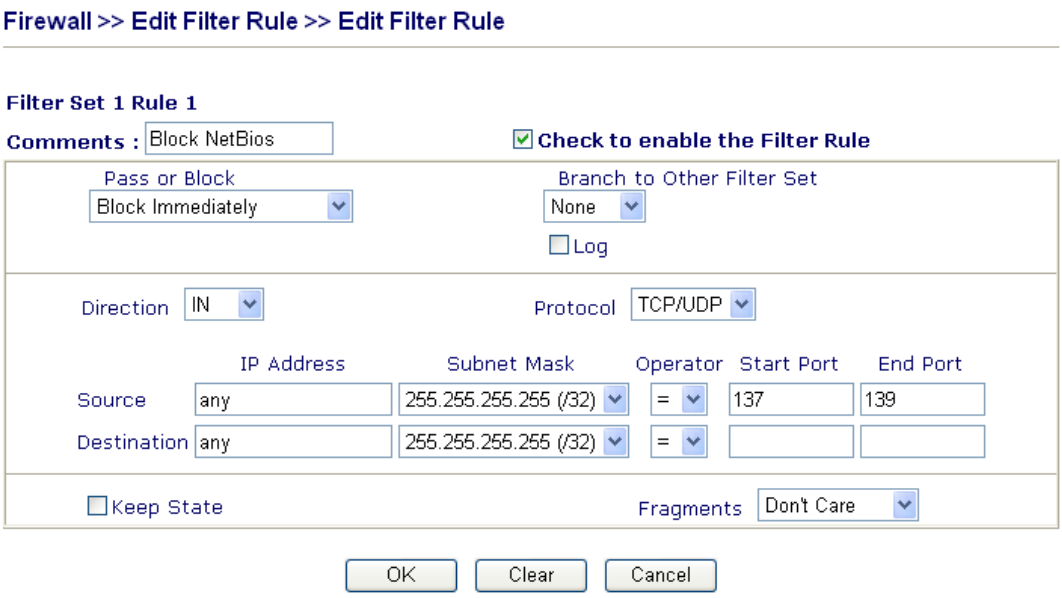


Filter Rule Click a button numbered (1 ~ 7) to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.

Active Enable or disable the filter rule.

Comment	Enter filter set comments/description. Maximum length is 23–character long
Next Filter Set	Set the link to the next filter set to be executed after the current filter set. Do not make many filter sets a loop.

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

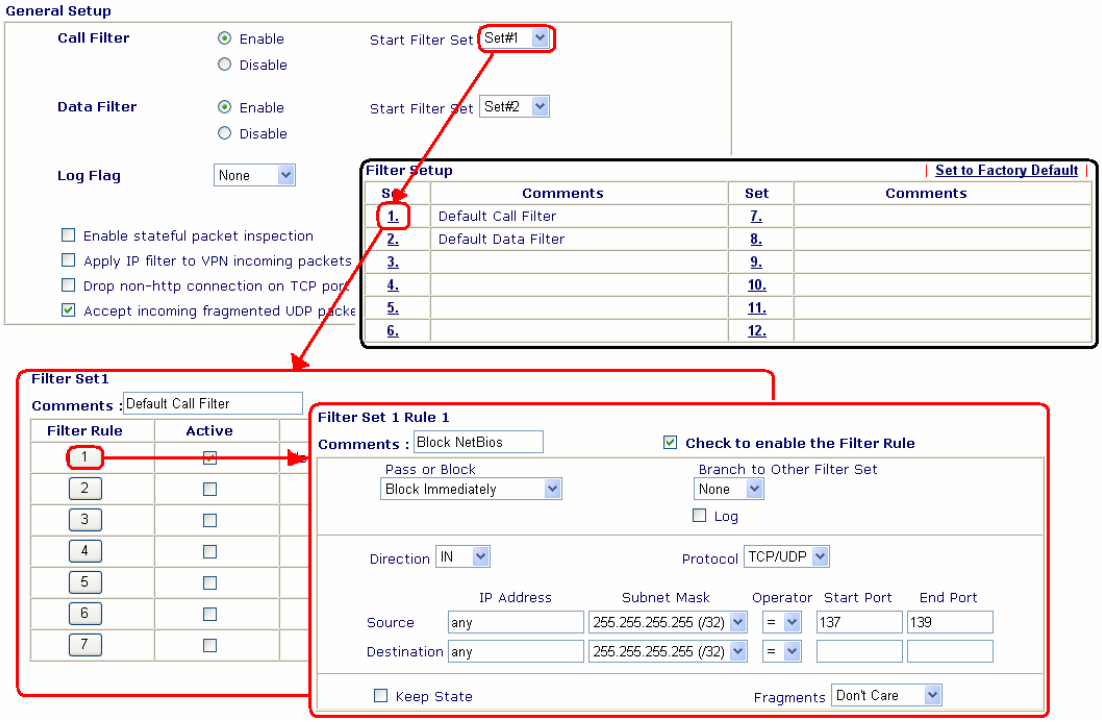


Comments	Enter filter set comments/description. Maximum length is 14-character long.
Check to enable the Filter Rule	Check this box to enable the filter rule.
Pass or Block	Specifies the action to be taken when packets match the rule. **Block Immediately -** Packets matching the rule will be dropped 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 Set	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 drop-down menu.
Log	Check this box to enable the log function. Use the Telnet command ***log-f*** to view the logs.
Direction	Set the direction of packet flow. It is for **Data Filter** only. For the **Call Filter**, this setting is not available since **Call Filter** is only applied to outgoing traffic.
Protocol	Specify the protocol(s) which this filter rule will apply to.
IP Address	Specify a source and destination IP address for this filter rule to apply to. Place the symbol "!" before a specific IP Address will prevent this rule from being applied to that IP address. To apply the rule to all IP address, enter **any** or leave the field blank.

Subnet Mask	Select the **Subnet Mask** for the IP Address column for this filter rule to apply from the drop-down menu.
Operator, Start Port and End Port	The operator column specifies the port number settings. If the **Start Port** is empty, the **Start Port** and the **End Port** column will be ignored. The filter rule will filter out any port number. ***(=)*** If the End Port is empty, the filter rule will set the port number to be the value of the Start Port. Otherwise, the port number ranges between the Start Port and the End Port (including the Start Port and the End Port). ***(!=)***If the End Port is empty, the port number is not equal to the value of the Start Port. Otherwise, this port number is not between the Start Port and the End Port (including the Start Port and End Port). ***(>)*** Specify the port number is larger than the Start Port (includes the Start Port). ***(<)*** Specify the port number is less than the Start Port (includes the Start Port).
Keep State	This function should work along with Direction, Protocol, IP address, Subnet Mask, Operator, Start Port and End Port settings. It is used for Data Filter only. Keep State is in the same nature of modern term Stateful Packet Inspection. It tracks packets, and accept the packets with appropriate characteristics showing its state is legal as the protocol defines. It will deny unsolicited incoming data. You may select protocols from any, TCP, UDP, TCP/UDP, ICMP and IGMP.
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.

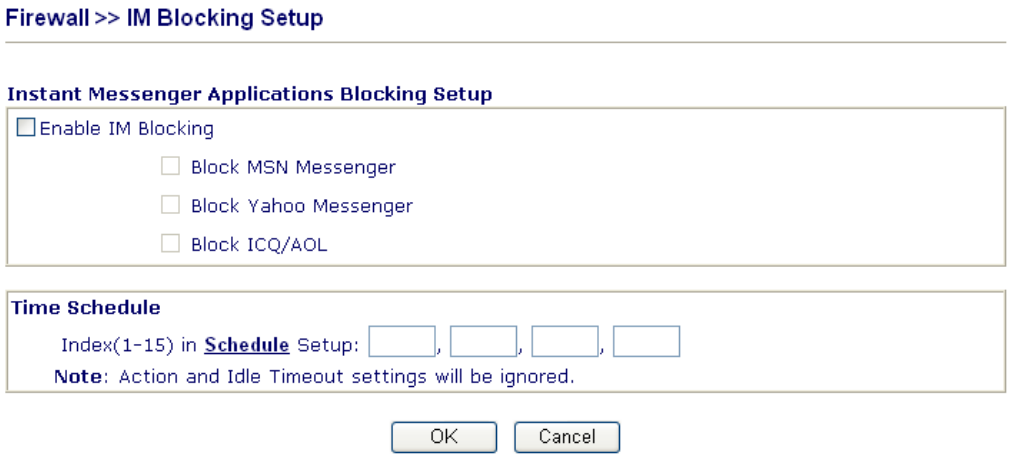
Example

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.



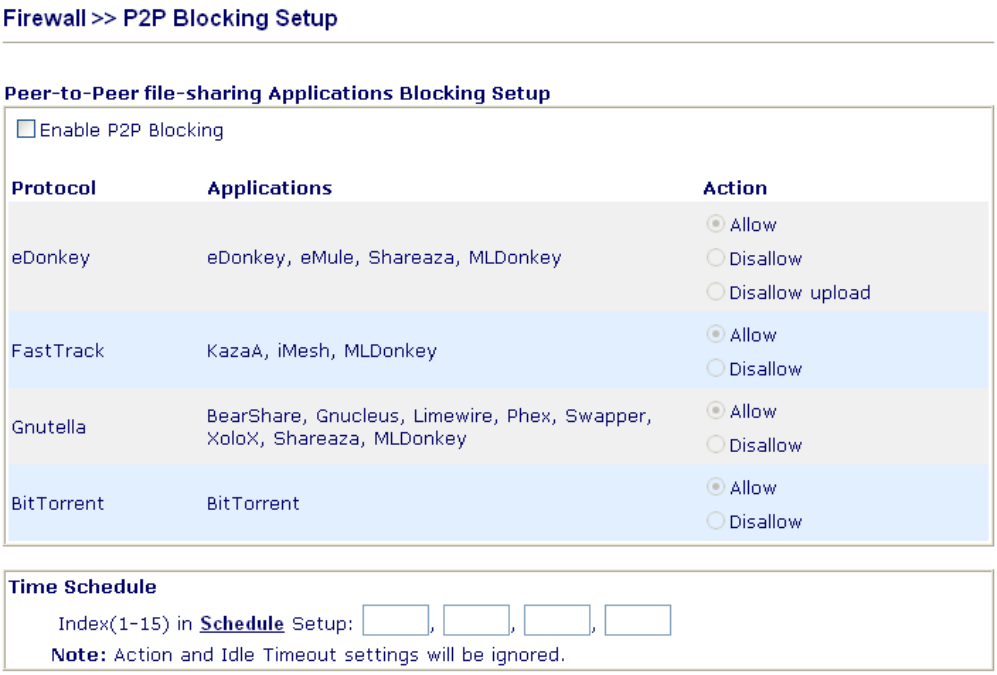
3.4.4 IM Blocking

IM Blocking means instant messenger blocking. Click **Firewall** and click **IM Blocking** to open the setup page. You will see a list of common IM (such as MSN, Yahoo, ICQ/AQL) applications. Check **Enable IM Blocking** and select the one(s) that you want to block. To block selected IM applications during specific periods, enter the number of the scheduler predefined in **Applications>>Call Schedule**.



3.4.5 P2P Blocking

P2P is the short name of peer to peer. Click **Firewall** and click **P2P Blocking** to open the setup page. You will see a list of common P2P applications. Check **Enable P2P Blocking** and select the one(s) to block. To block selected P2P applications during specific periods, enter the number of the scheduler predefined in **Applications>>Call Schedule**.

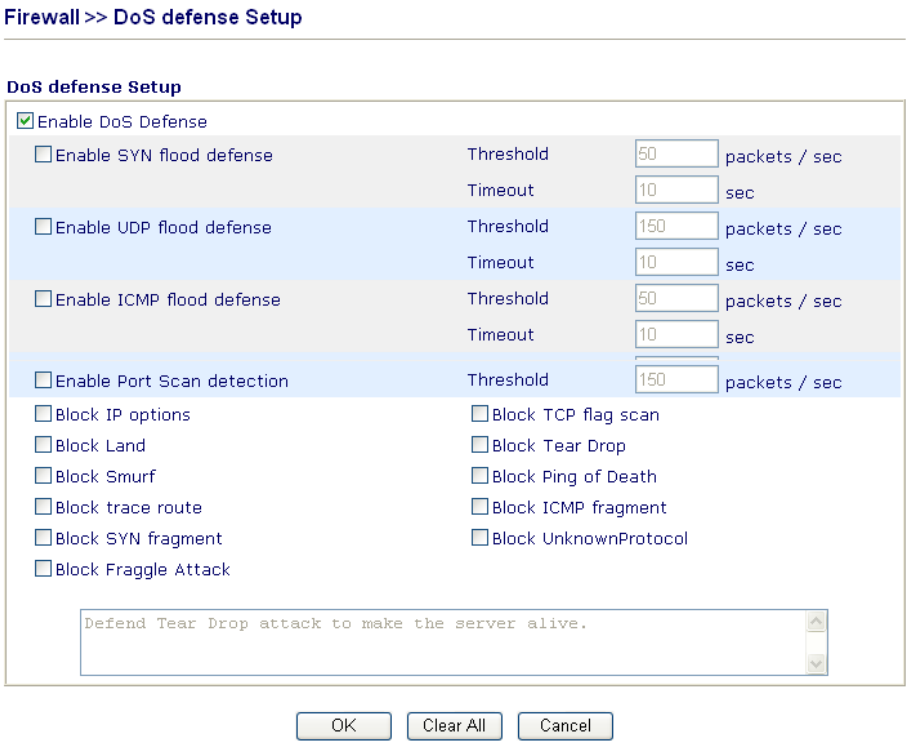


Action Specify the action for each protocol.
Allow – Allow the client to access into the application through the specified protocol.
Disallow – Forbid the client to access into the application through the specified protocol.
Disallow upload – Forbid the client to access into the application through the specified protocol for downloading. Yet uploading is allowed.

3.4.6 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

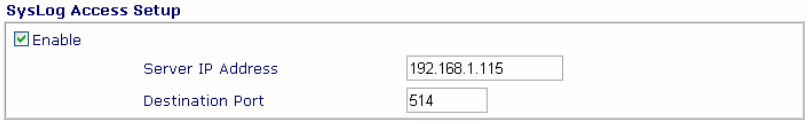
	detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning. By default, the Vigor router sets the threshold as 150 packets per second.
Block IP options	Check the box to activate the Block IP options function. The Vigor router 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

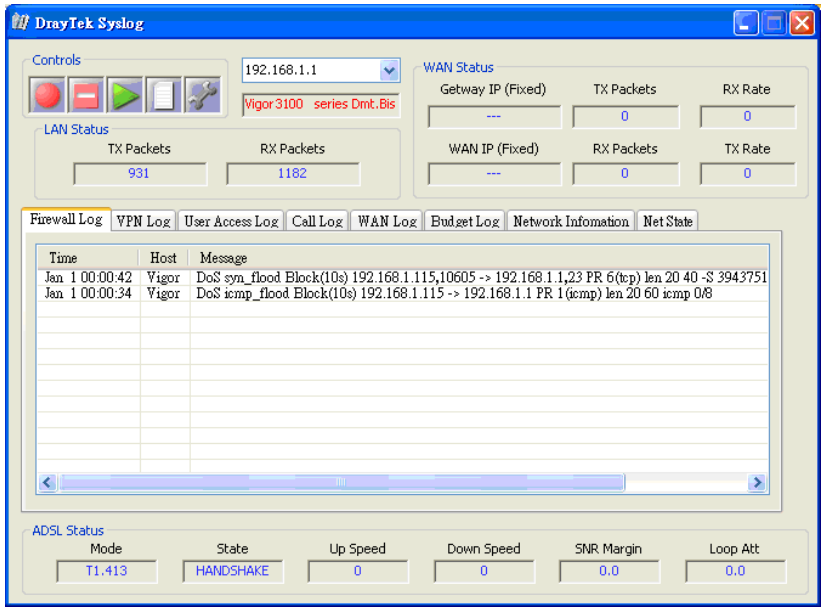
indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.

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. (Refer to Chapter 13 System Maintenance Syslog Access Setup for detail information.)

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.





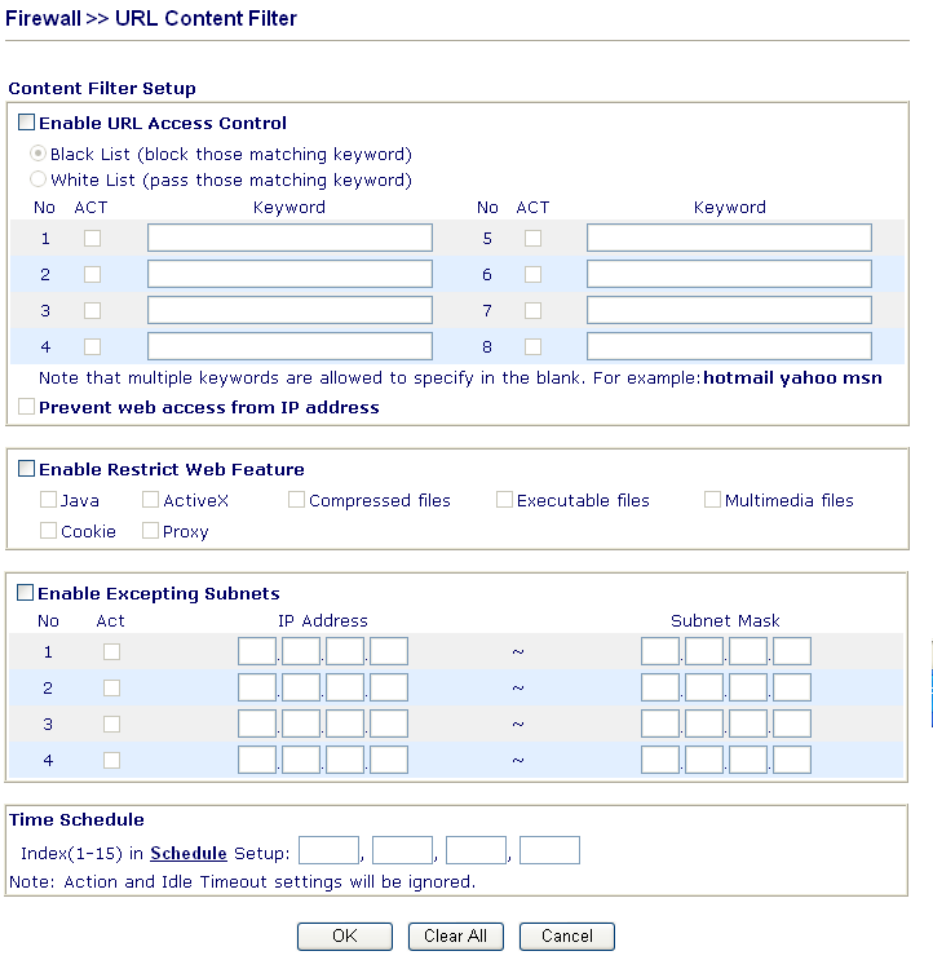
3.4.7 URL Content Filter

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 **Firewall** and click **URL Content Filter** to open the setup page.



Enable URL Access Control	Check the box to activate URL Access Control.
Black List (block those matching keyword)	Click this button to restrict accessing into the corresponding webpage with the keywords listed on the box below.
White List (pass those matching keyword)	Click this button to allow accessing into the corresponding webpage with the keywords listed on the box below.
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. ***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**
Enable Excepting Subnets	Four entries are available for users to specify some specific IP addresses or subnets so that they can be free from the *URL Access Control*. To enable an entry, click on the empty checkbox, named as **ACT**, in front of the appropriate entry.
Time Schedule	Specify what time should perform the URL content filtering facility.

3.4.8 Web Content Filter

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

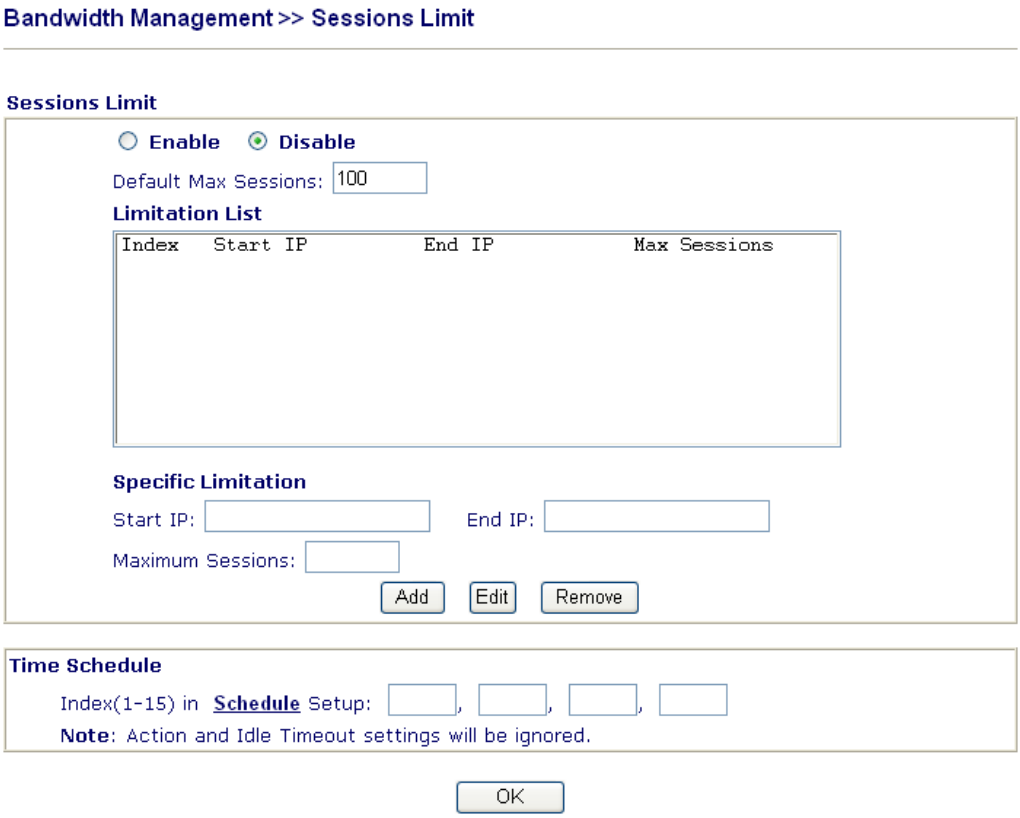
For this section, please refer to **Web Content Filter** user's guide.

3.5 Bandwidth Management

3.5.1 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.

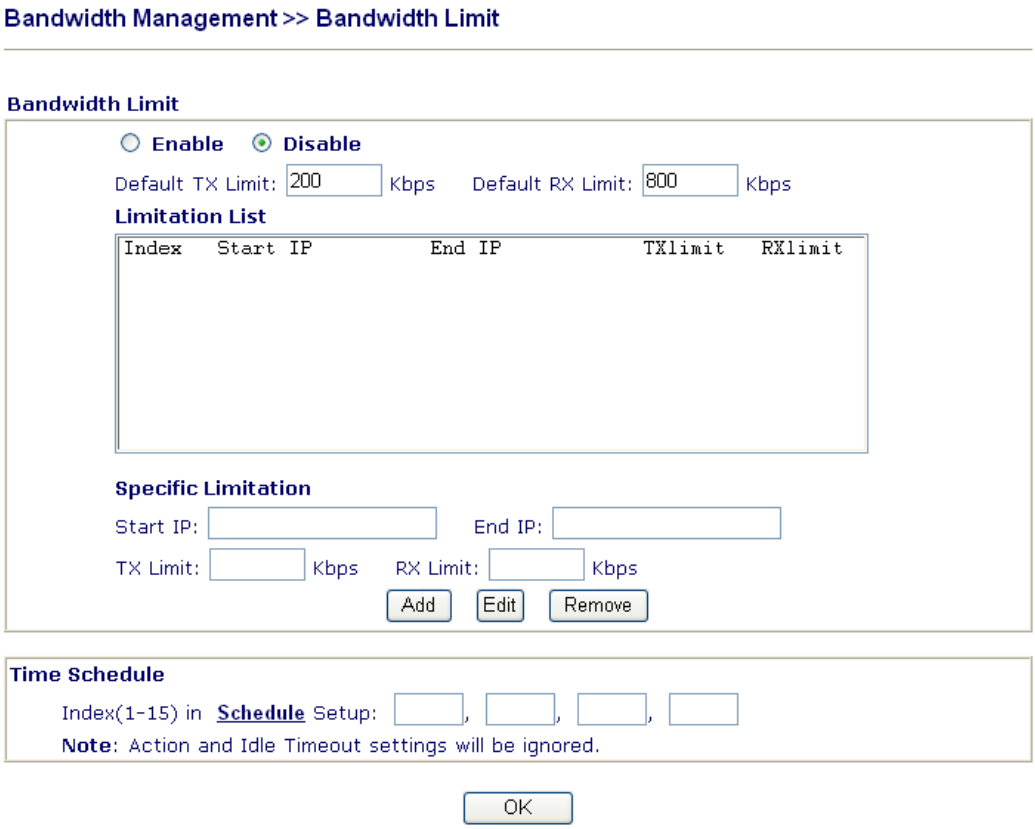
Enable	Click this button to activate the function of limit session.
Disable	Click this button to close the function of limit session.
Default Max session	Defines the default session number used for each computer in LAN.
Limitation List	Displays a list of specific limitations that you set on this web page.
Start IP	Defines the start IP address for limit session.
End IP	Defines the end IP address for limit session.
Maximum Session	Defines the available session number for 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.

Remove	Remove 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.

3.5.2 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.
Remove	Remove 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.

3.5.3 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:

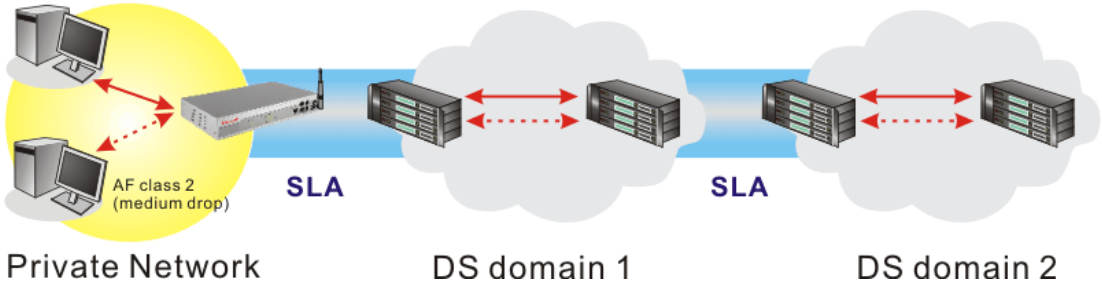
- Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- Scheduling: Based on classification of service level to assign packets to queues and associated service types

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.

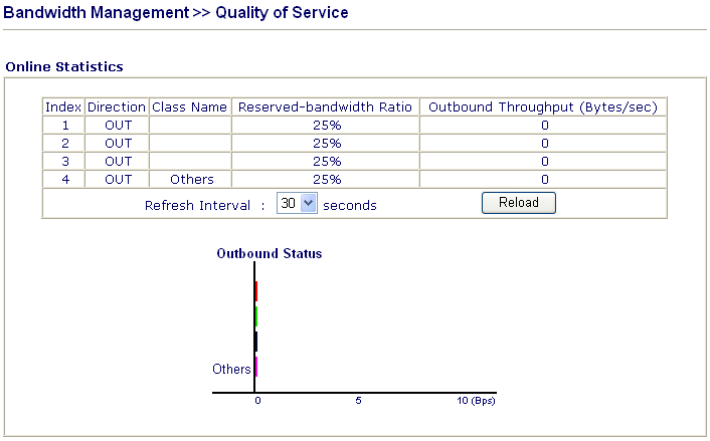


However, each node may take different attitude toward packets with high priority marking since it may bind with the business deal of SLA among different DS domain owners. It's not easy to achieve deterministic and consistent high-priority QoS traffic throughout the whole network with merely Vigor router's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

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

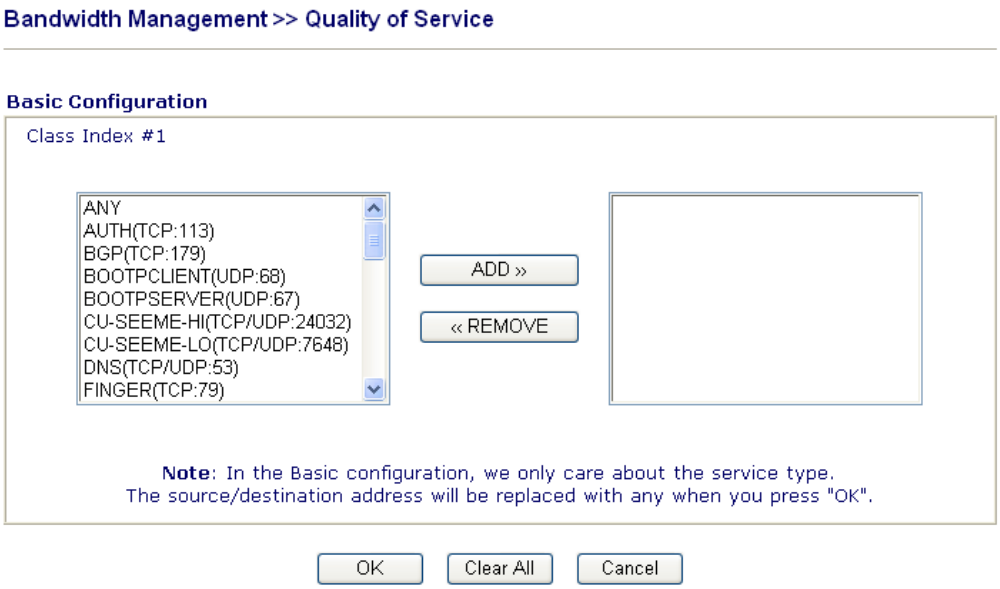
Enable the QoS Control	The factory default for this setting is checked.
Direction	Define which traffic the QoS Control settings apply to. **IN-** apply to incoming traffic only. **OUT-**apply to outgoing traffic only. **BOTH-** apply to both incoming and outgoing traffic.
Index	The group index number of QoS Control settings. There are total 4 groups.
Class Name	Define the name for the group index.
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**.

Setup	There are two-level of settings: **Basic -** setup Reserved Bandwidth Ratio according to the traffic service type. We provide a list of common service types. **Advance -** custom setting of Reserved Bandwidth Ratio based on the source address, destination address, DiffServ CodePoint, and service type.
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.
Limited_bandwidth Ratio	The ratio typed here is reserved for limited bandwidth of UDP application.
On Line Statistics	Display an online statistics for quality of service for your reference.



Basic Settings for QoS

Click the **Basic** button to open basic configuration screen for each index number.

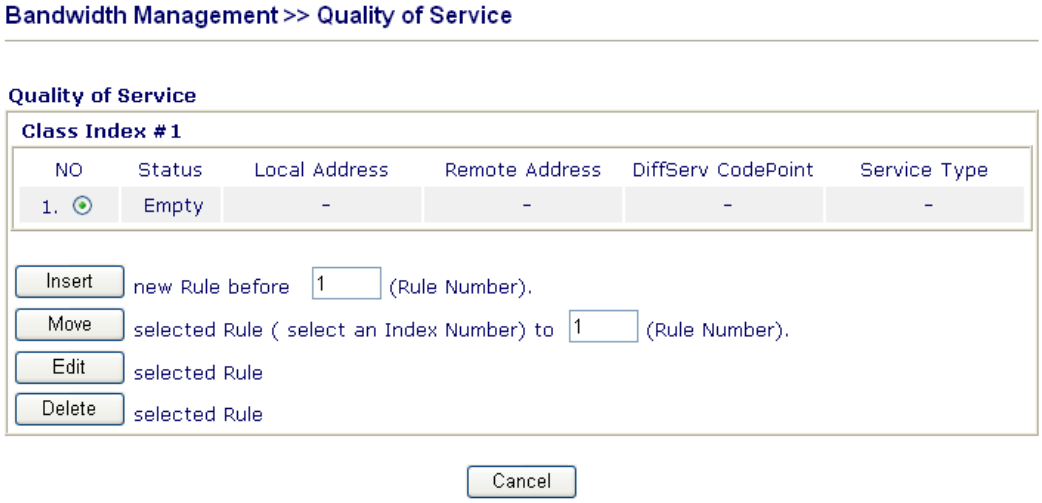


Choose one of the items from the left box and click **ADD>>**. The selected one will be shown

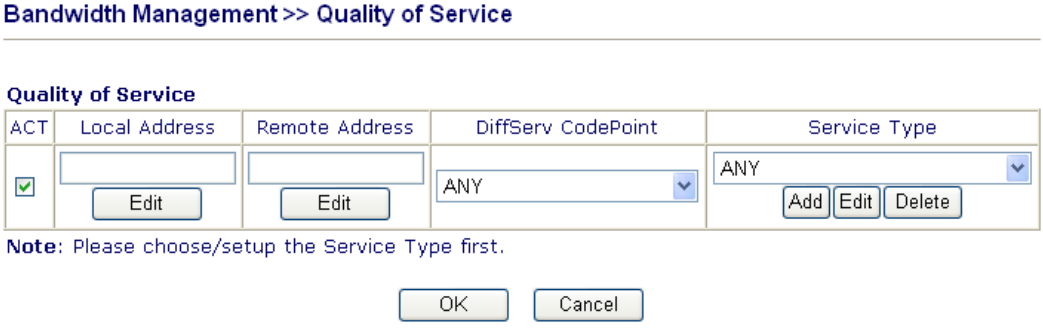
on the right box. To remove the selected on from the right box, simply choose the one again and click **<<Remove.**

Advanced Settings for QoS

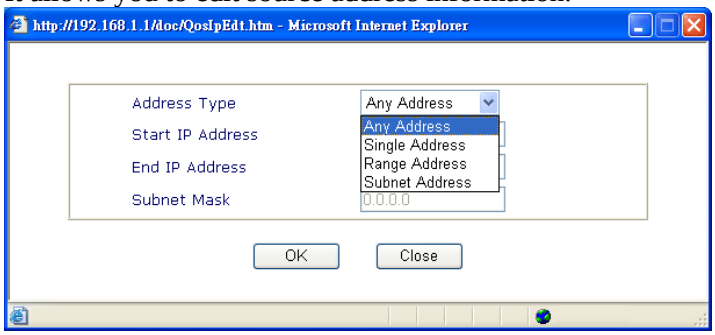
Click this button to open advanced configuration for each index number**.** You can insert, move, edit or delete select rule in this page.



For inserting a rule, click **Insert** to open the following page.



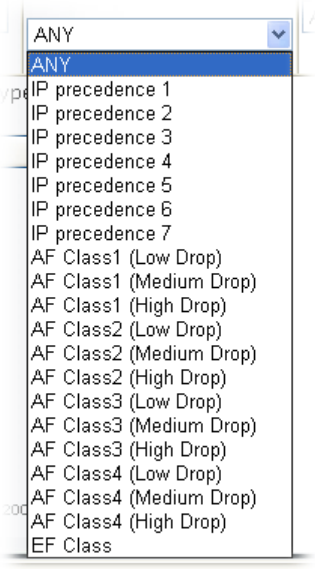
SrcEdit/DestEdit It allows you to edit source address information.



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.

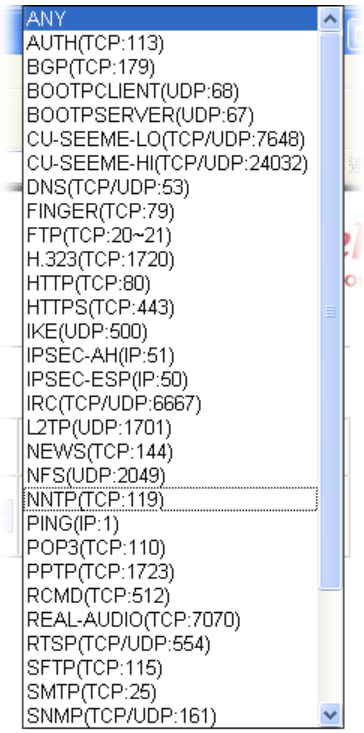
DiffServ CodePoint

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 levels of the data for processing with QoS control.

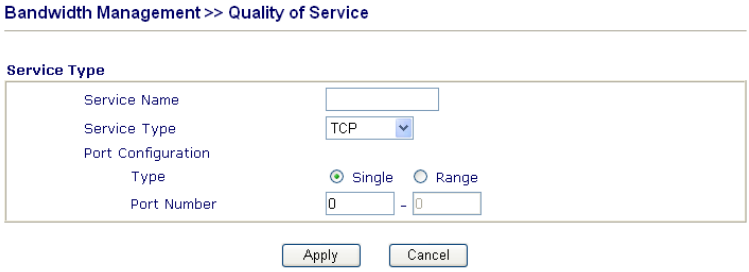


Service Type

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.



In addition, you can add a new service for your necessity by simply clicking **Add** button to access into 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.
Type for 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.
You can add a new service name for your necessity. Also, you can **Edit/Delete** to change the one that you added before.

3.6 Applications

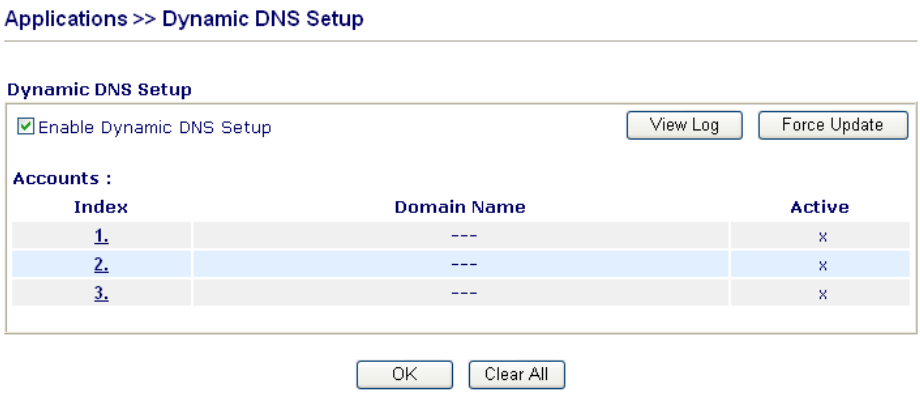
3.6.1 Dynamic DNS

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.

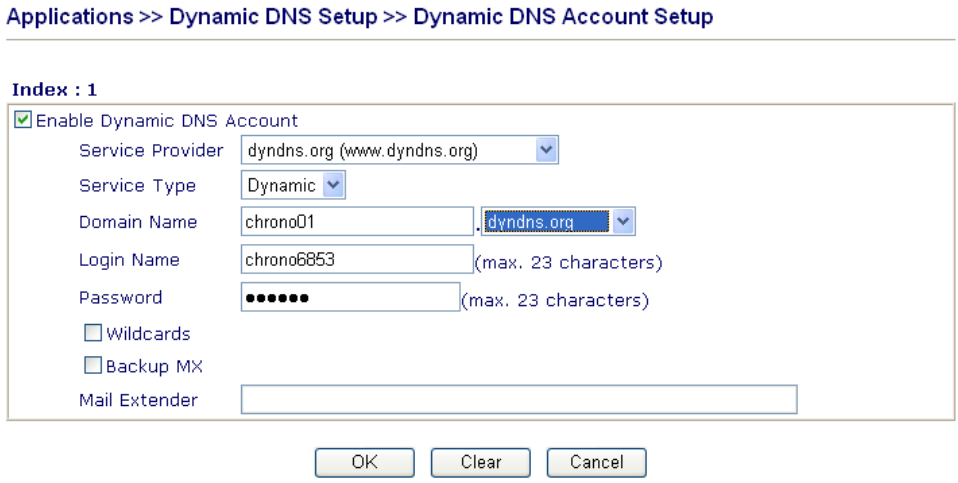
Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The router provides up to three accounts from three different DDNS service providers. Basically, Vigor routers are compatible with the DDNS services supplied by most popular DDNS service providers 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**.

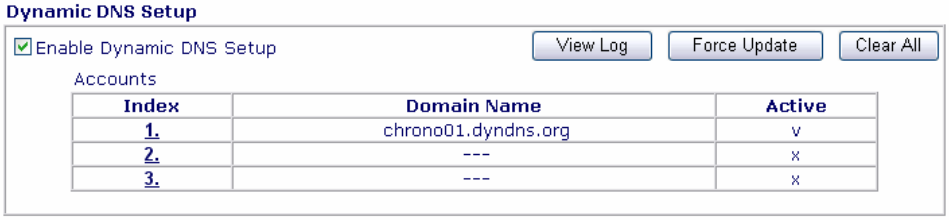


3. Select Index number 1 to add an account for the router. Check Enable Dynamic DNS Account, and choose correct Service Provider: dyndns.org, type the registered hostname: *hostname* and domain name suffix: dyndns.org in the Domain Name block. The following two blocks should be typed your account Login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



Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom, Static).
Domain Name	Type in a domain name that you applied previously.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.

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.

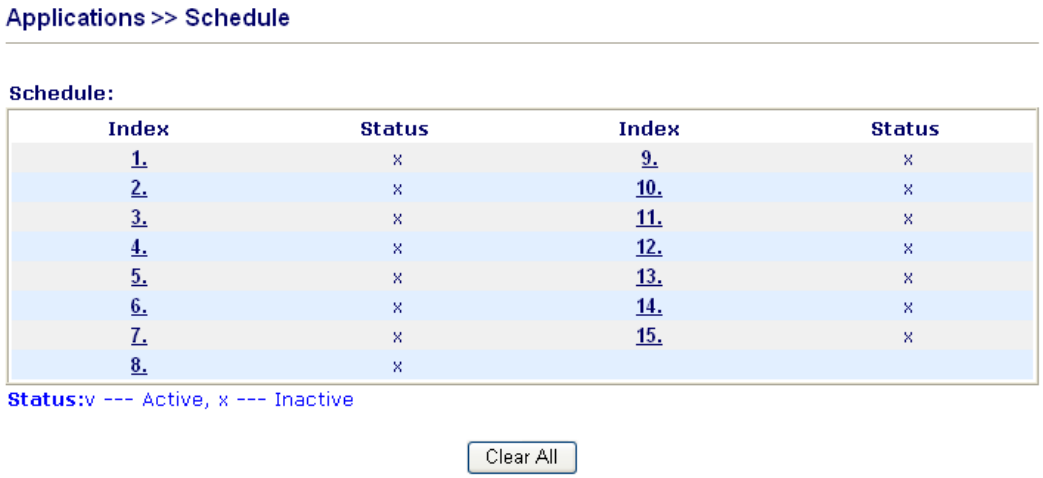
Delete a Dynamic DNS Account

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

3.6.2 Schedule

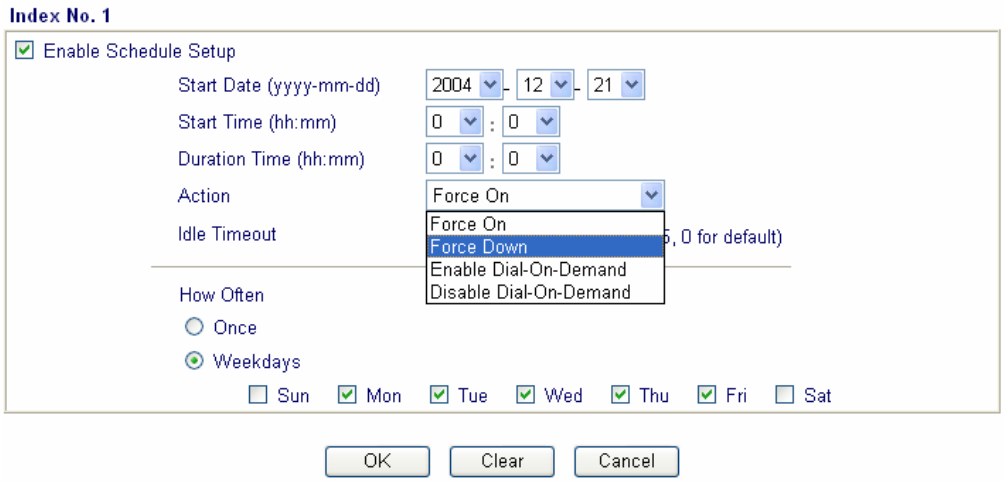
The Vigor router has a built-in real time clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the router to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users 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 Setup** menu, press **Inquire Time** button to set the Vigor router's clock to current time of your PC. The clock will reset once if you power down or reset the router. There is another way to set up time. You can inquiry an NTP server (a time server) on the Internet to synchronize the router's clock. This method can only be applied when the WAN connection has been built up.



You can set up to 15 schedules. 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 (office hour). Other time the Internet access connection should be disconnected (Force Down).

Office Hour:

(Force On)

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

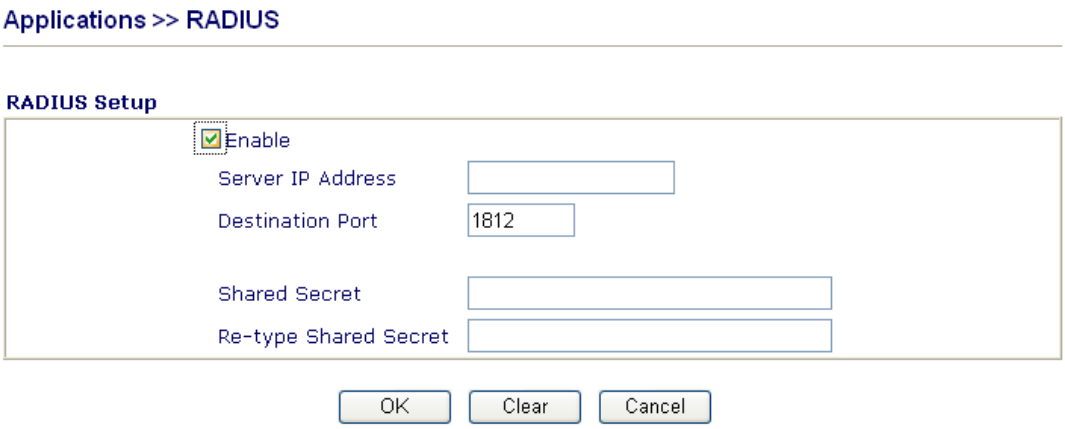
1. Make sure the PPPoE connection and **Time Setup** is working properly.
2. Configure the PPPoE always on from 9:00 to 18:00 for whole week.
3. Configure the **Force Down** from 18:00 to next day 9:00 for whole week.

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.

3.6.3 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.

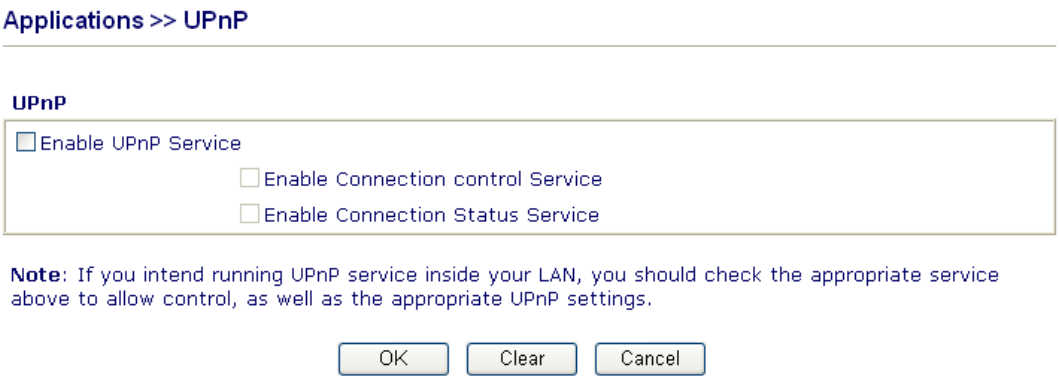
The built-in RADIUS client feature enables the router to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.



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.
Re-type Shared Secret	Re-type the Shared Secret for confirmation.

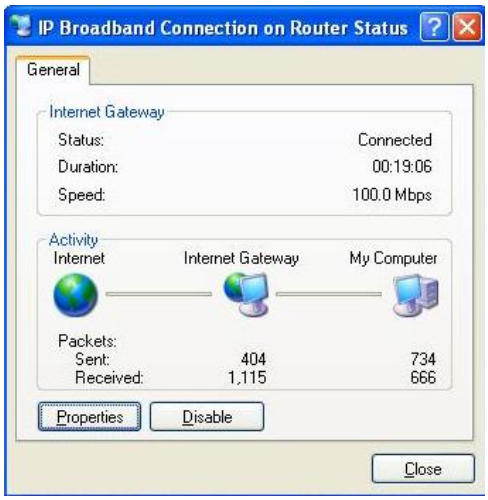
3.6.4 UPnP

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.

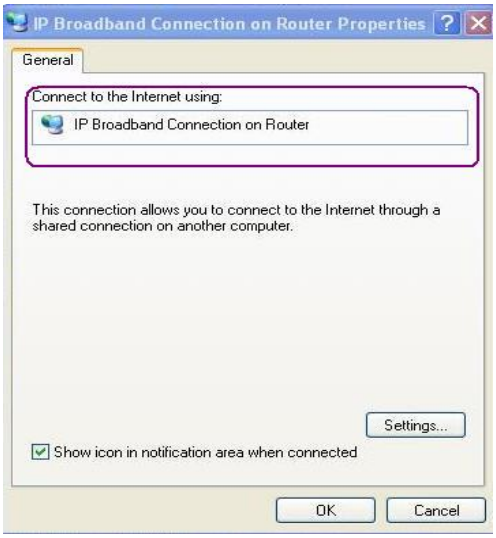


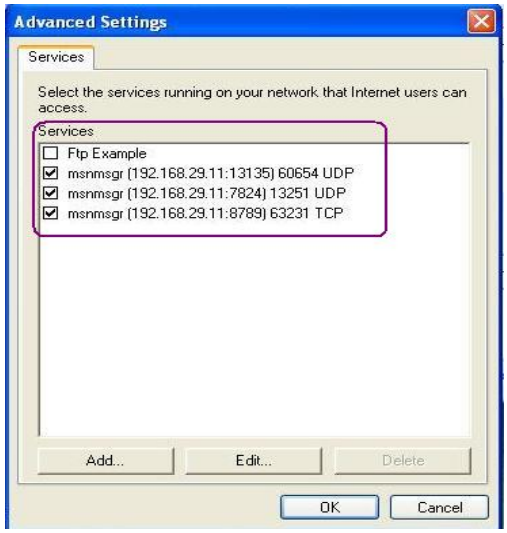
Enable UPNP Service Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

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

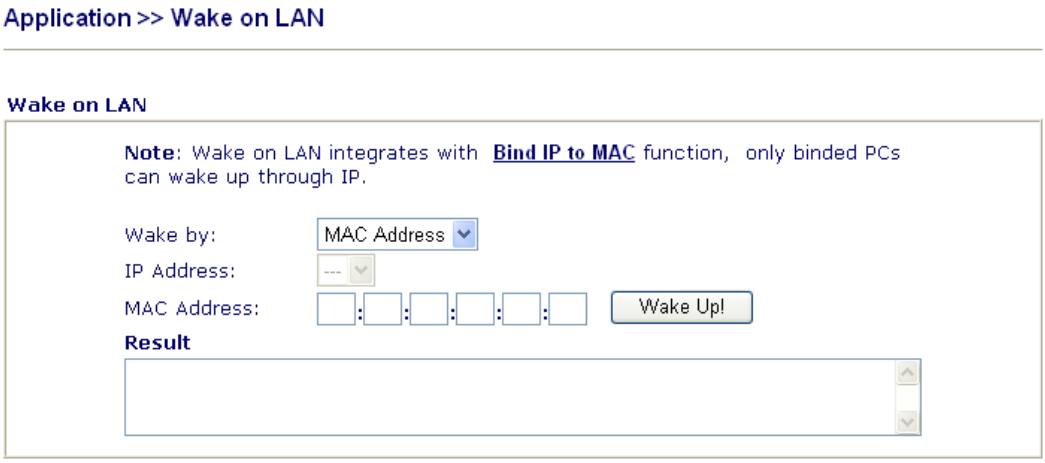
Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

- 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.

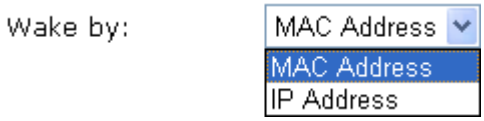
The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

3.6.5 Wake on LAN

A PC client on LAN can wake up specified PC through the router. Yet the specified PC must have installed a network card supporting WOL function. By the way, WOL function must be set as “Enable” on the BIOS setting of the specified PC.



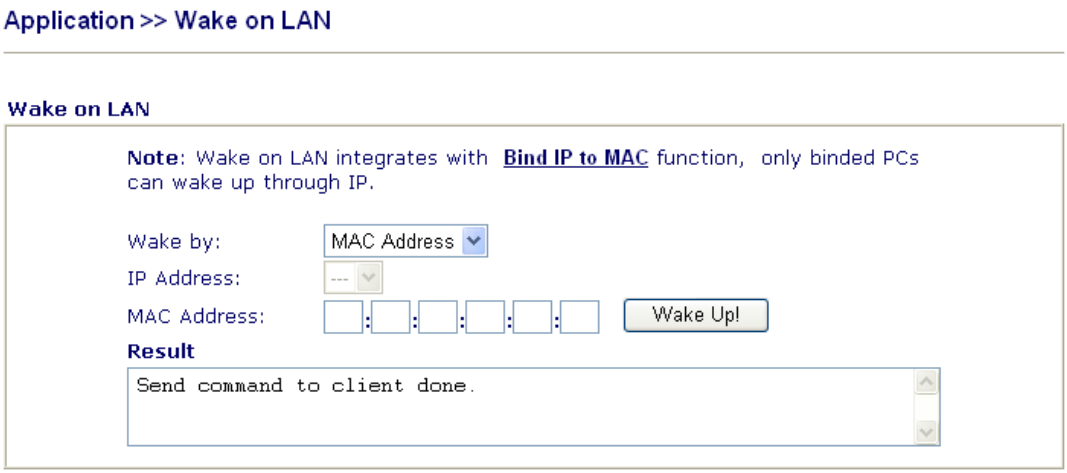
Wake by Two types provide for you to wake up the binded IP. If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the correct IP address. The IP address should be binded with MAC address configured in **Bind IP to MAC** page.



IP Address The IP addresses that have been configured in **Firewall>>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.

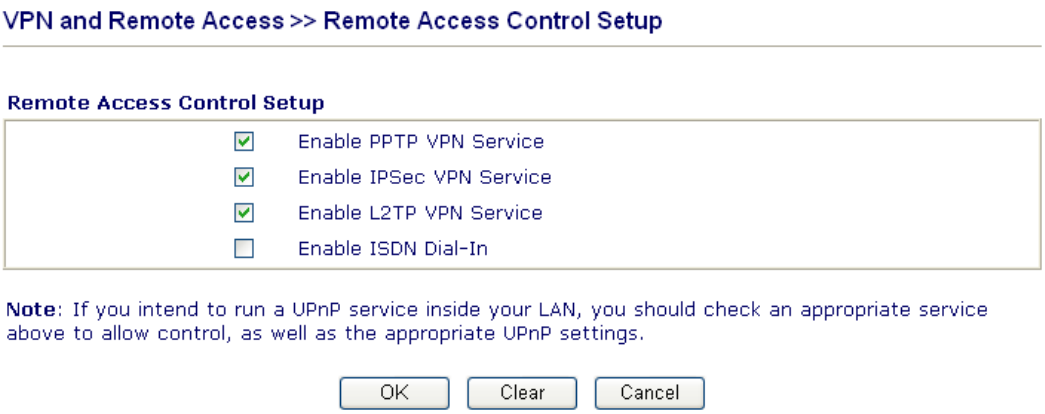


3.7 VPN and Remote Access

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.

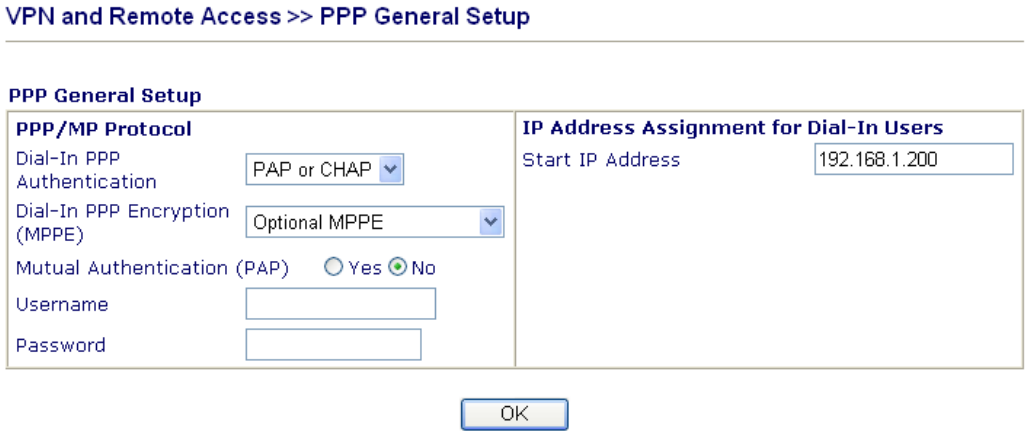
3.7.1 Remote Access Control

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



3.7.2 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 40-bit MPPE encryption method is not available, then 128-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 bits) 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 192.168.1.202 to be the Start IP Address.

3.7.3 IPSec General Setup

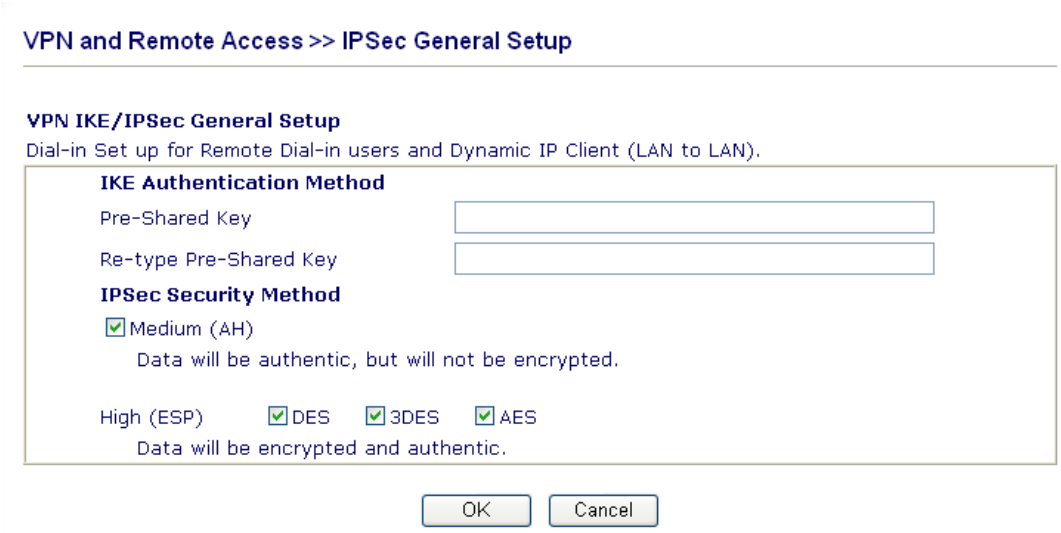
In **IPSec General Setup,** there are two major parts of configuration.

There are two phases of IKE/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) and/or Encapsulating Security Payload (ESP) for the following IKE exchange and mutual examination of the secure tunnel establishment.

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. Vigor supports IPSec used ESP to encrypt the data payload. There are two encryption methods in IPSec: Transport and Tunnel. Transport mode encrypts only the data portion, a.k.a. payload, of each packet, but not the header. Transport mode is used in L2TP over IP Sec. The more secure Tunnel mode encrypts both the header and the payload. Tunnel mode is used in IPSec. ESP can be used alone or in conjunction with AH.

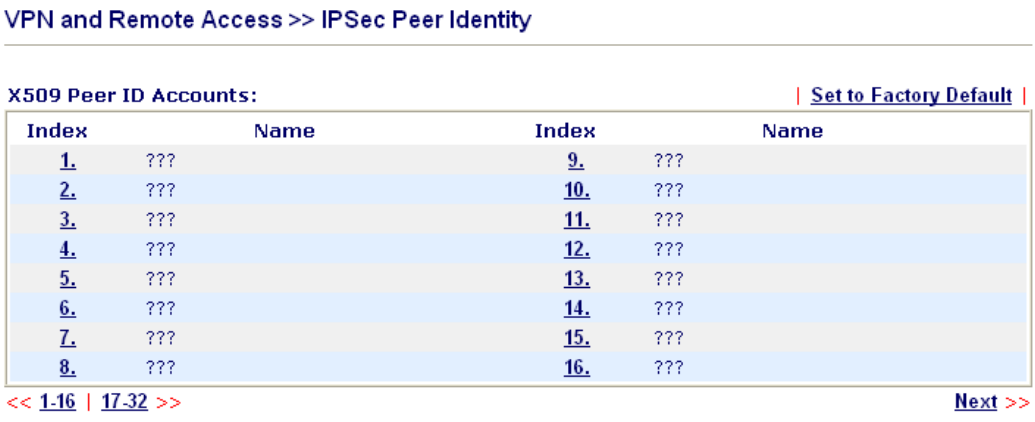


IKE Authentication Method This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec and IPSec tunnel.
Pre-Shared Key -Currently only support Pre-Shared Key authentication.
Pre-Shared Key- Specify a key for IKE authentication
Re-type Pre-Shared Key-Confirm the pre-shared key.

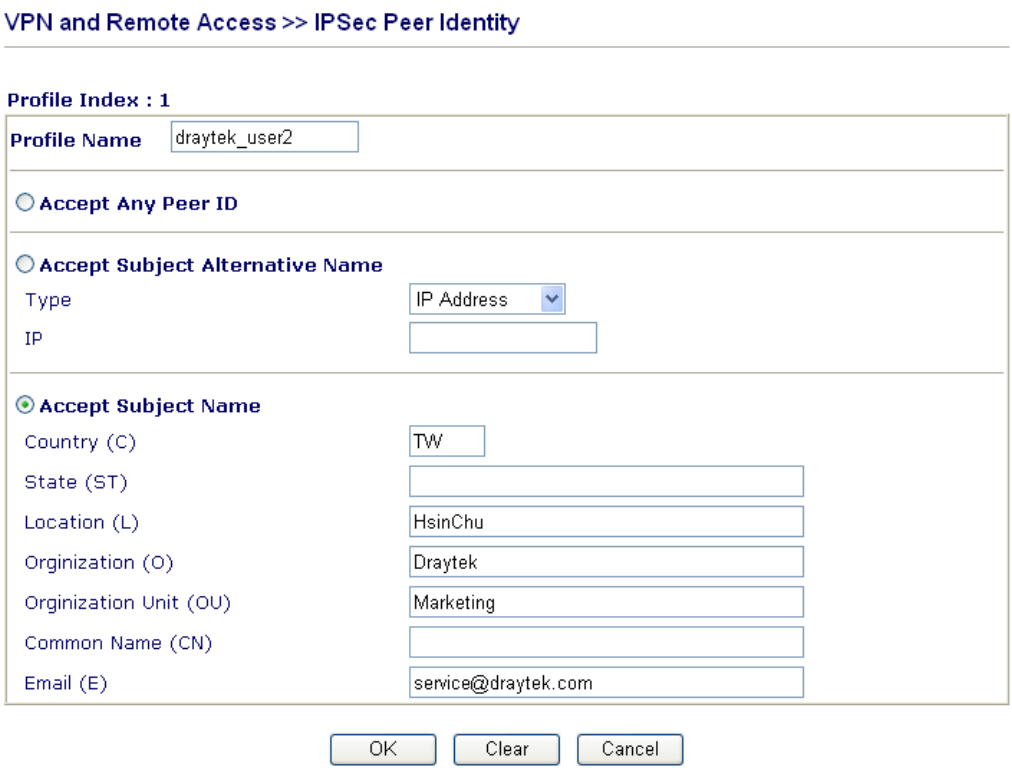
IPSec Security Method **Medium** - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
High - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data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

3.7.4 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 32 entries of digital certificates for peer dial-in users.



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.

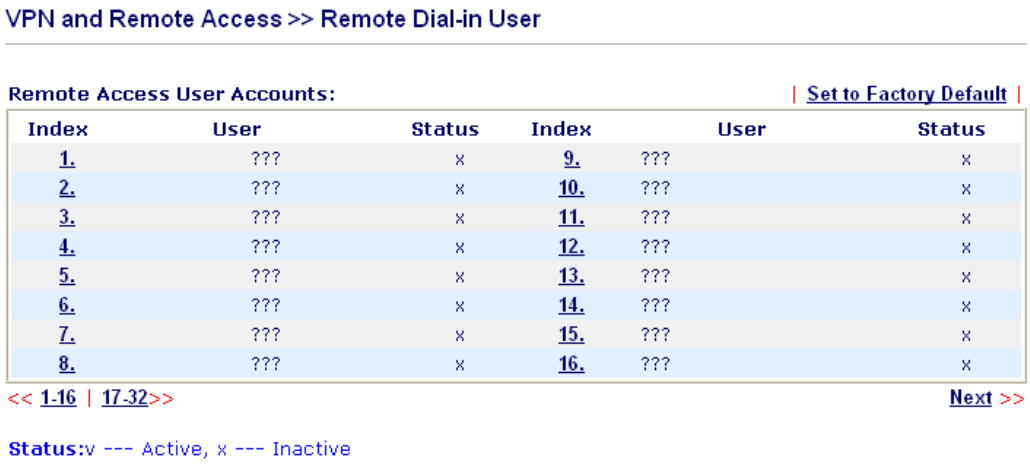


Profile Name	Type in a name in this file.
Accept Any Peer ID	Click to accept any peer regardless of its identity.
Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be **IP Address, Domain,** or **E-mail Address**. 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)**.

3.7.5 Remote Dial-In User

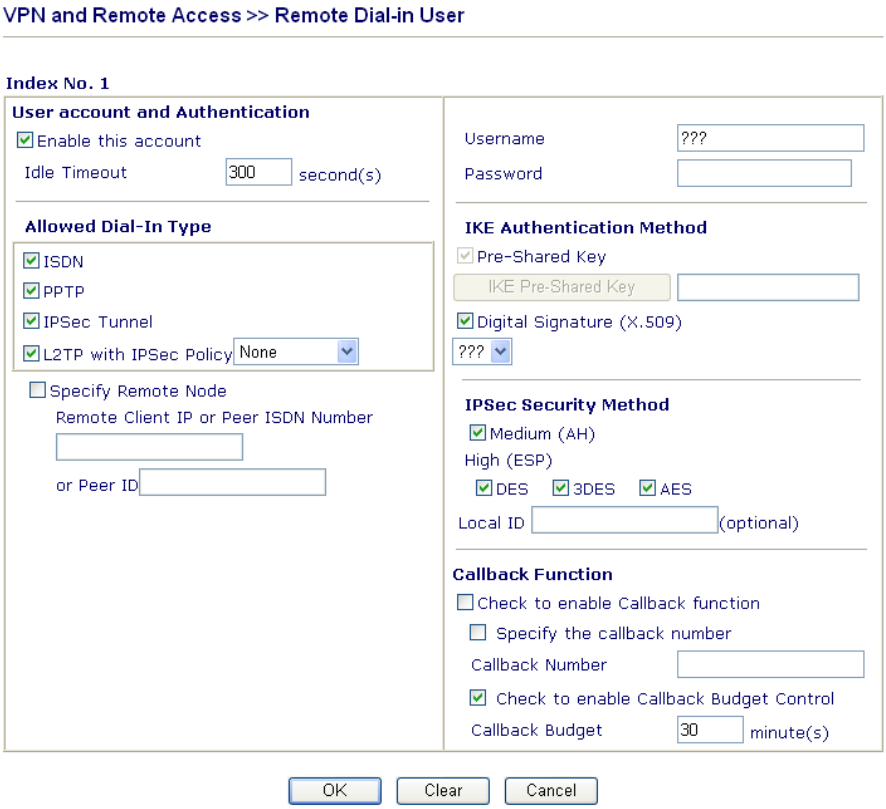
You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in or build the VPN connection. You may set parameters including specified connection peer ID, connection type (ISDN, VPN including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec)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

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



Set to Factory Default	Click to clear all indexes.
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.



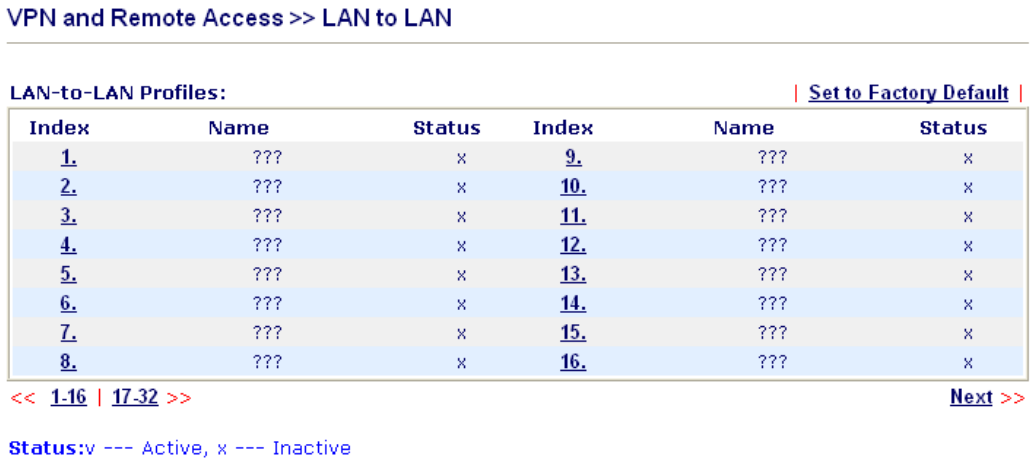
Enable this account	Check the box to enable this function. **Idle Timeout-** If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.
ISDN	Allow the remote ISDN dial-in connection. You can further set up Callback function below. You should set the User Name and Password of remote dial-in user below
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 a 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. N**ice 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 or peer ID (should be the same as the ID you set in the Local ID of IKE advanced settings window). Enter Peer ISDN number if you select ISDN above. Also, you should

	further specify the corresponding security methods on the right side. **Uncheck the checkbox**-This means the connection type you select above will apply the authentication methods and security methods in the **general settings**.
User Name	This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. This field is also applicable if you select ISDN.
Password	This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. This field is also applicable if you select ISDN.
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 w/ or w/o specify the IP address of the remote node. **Pre-Shared Key -** Input 1-63 characters as pre-shared key. **Digital Signature (X.509) -** Select one predefined in the X.509 Peer ID Profiles.
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. **Local ID -** Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional.
Callback Function	The callback function provides a callback service only for the ISDN dial-in user. The router owner 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.

3.7.6 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 (ISDN, VPN including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

The router provides up to 32 profiles, which also means supporting 32 VPN tunnels simultaneously. The following figure shows the summary table.

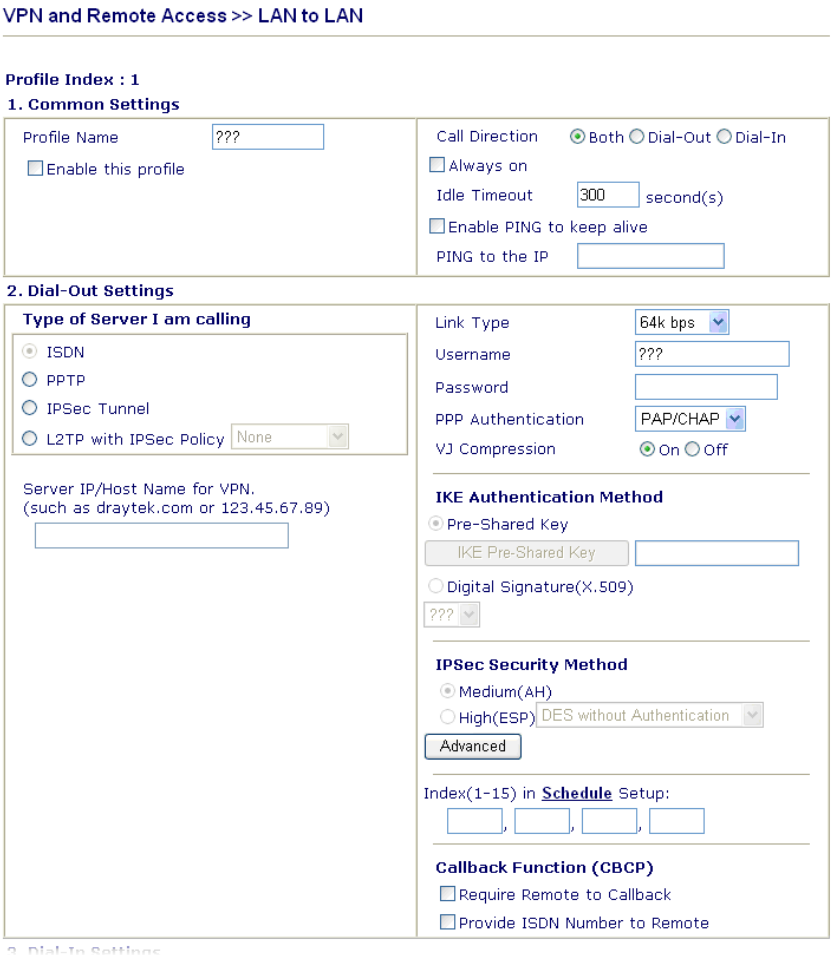


Set to Factory Default Click to clear all indexes.

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.



Profile Name	Specify a name for the profile of the LAN-to-LAN connection.
Enable this profile	Check here to activate this profile.
Call Direction	Specify the allowed call direction of this LAN-to-LAN profile. **Both**:-initiator/responder **Dial-Out**- initiator only **Dial-In-** responder only.
Always On 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.
ISDN	Build ISDN dial-out connection to the server. 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.
PPTP	Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server.
IPSec Tunnel	Build an IPSec VPN connection to the server through Internet.
L2TP-with IPsec…	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 PPTP or L2TP with or without IPSec policy above. This field is also applicable if you select ISDN.
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above. This field is also applicable if you select ISDN.
PPP Authentication	This field is applicable when you select PPTP or L2TP with or without IPSec policy above. This field is also applicable if you select ISDN. PAP/CHAP is the most common selection due to wild compatibility.
VJ compression	This field is applicable when you select PPTP or L2TP with or without IPSec policy above. This field is also applicable if you select ISDN. 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.

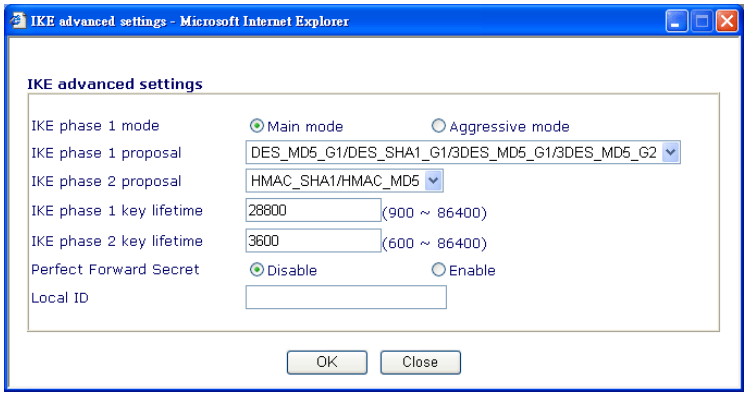
Medium

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. 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 as show below:

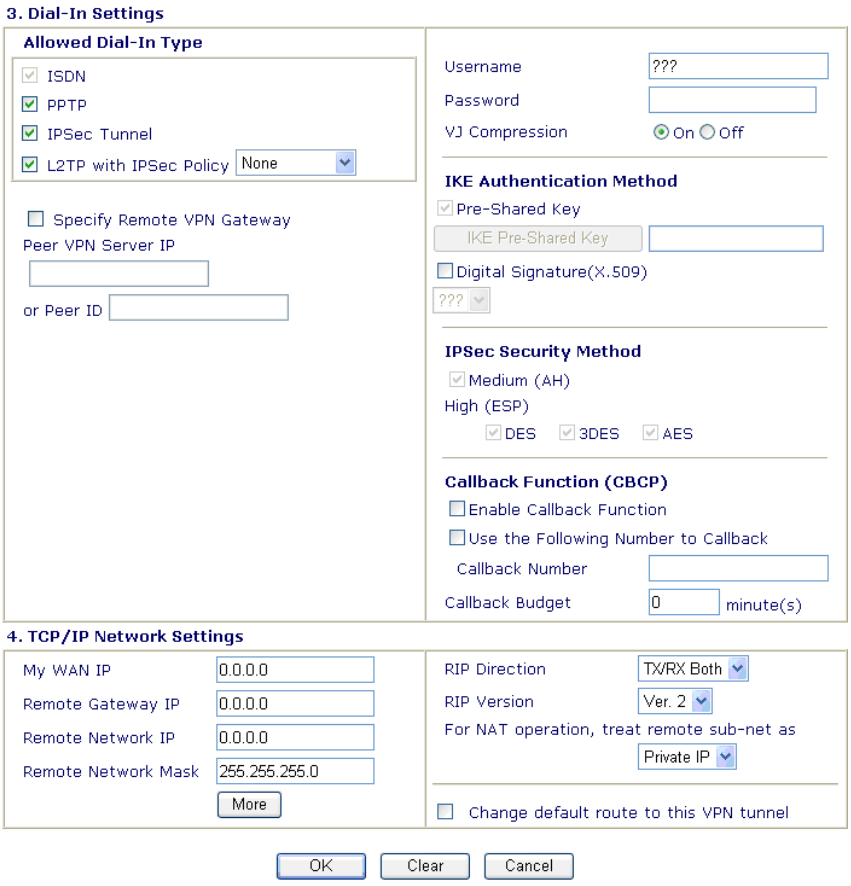


IKE phase 1 mode -Select from **Main** mode and **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPSec session. However,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

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 a 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 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 PPTP or L2TP with or without IPSec policy above. This field is also applicable if you select ISDN.
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above. This field is also applicable if you select ISDN.
VJ Compression	VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP with or without IPSec policy above. This field is also applicable if you select ISDN.
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

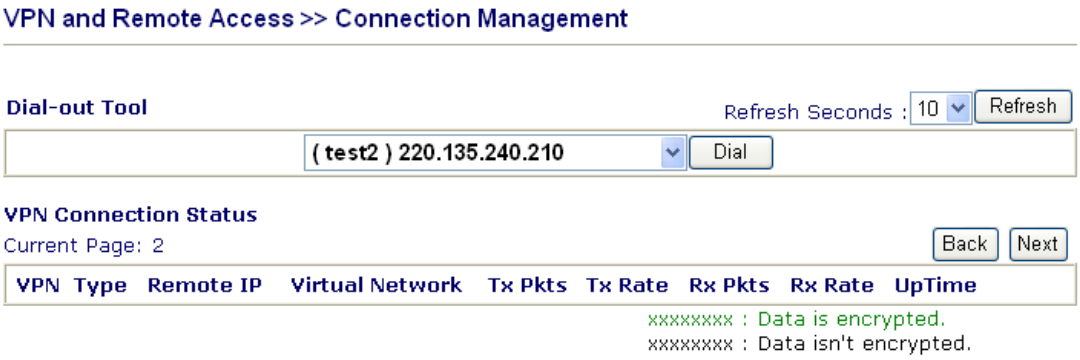
	authenticated, but not be encrypted. By default, this option is active. **High-** Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
Callback Function	The callback function provides a callback service only for the ISDN dial-in user. The router owner 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 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 WAN IP address from the remote router during the IPCP negotiation phase. If the WAN IP address is fixed by remote side, specify the fixed IP address here.
Remote Gateway IP	This field is only applicable when you select 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 IP address from the remote router during the IPCP negotiation phase. If the WAN IP address is fixed by remote side, specify the fixed IP address here.
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 router 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.
RIP Version	Select the RIP protocol version. Specify Ver. 2 for greatest compatibility.
For NAT operation, treat remote sub-net as	While communicating with remote subnet, the router can treat it as private subnet by sending packets with the router's private IP address, or treat it as public subnet by sending

packets with the router's public IP address.

Change default route to this VPN tunnel — 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.

3.7.7 Connection Management

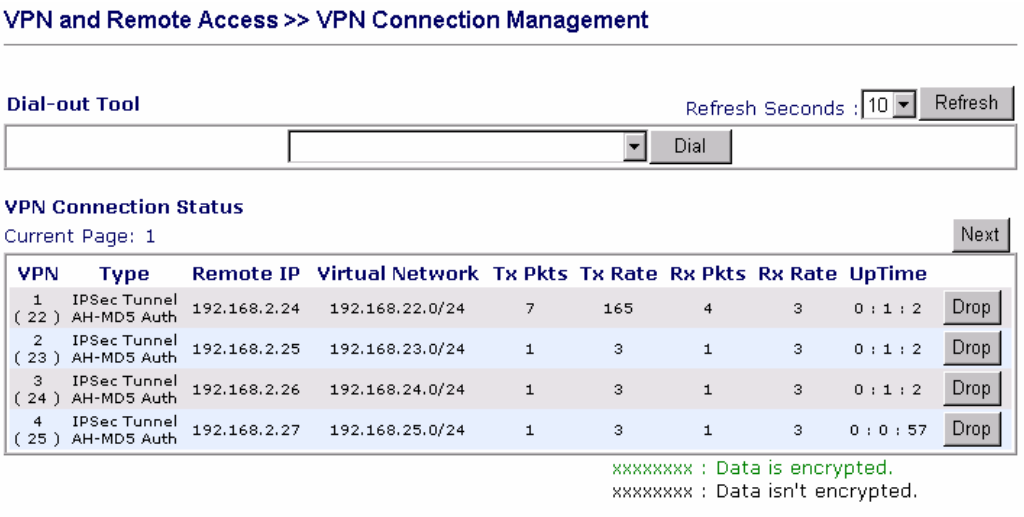
You can find the summary table of all VPN connections. You may disconnect any VPN connection by clicking Drop button. You may also aggressively Dial-out by using Dial-out Tool and clicking **Dial** button.



Dial — Click this button to execute dial out function.

Refresh Seconds — Choose the time for refresh the dail information among 5, 10, an 30.

Refresh — Click this button to refresh the whole connection status.



3.8 Certificate Management

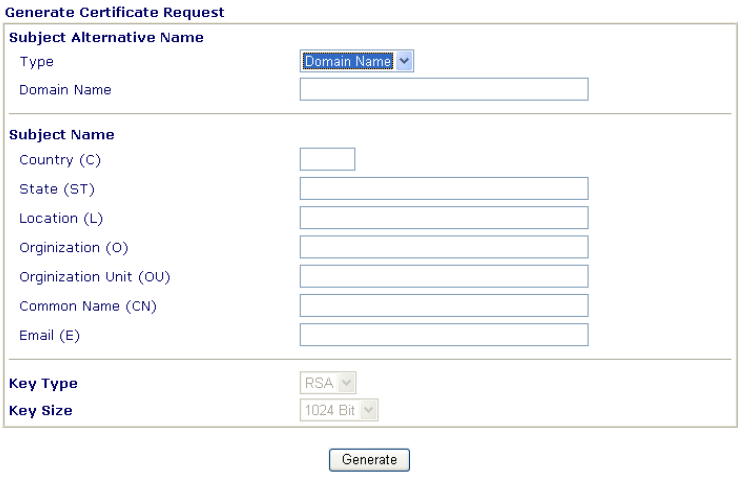
A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is 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.

3.8.1 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.

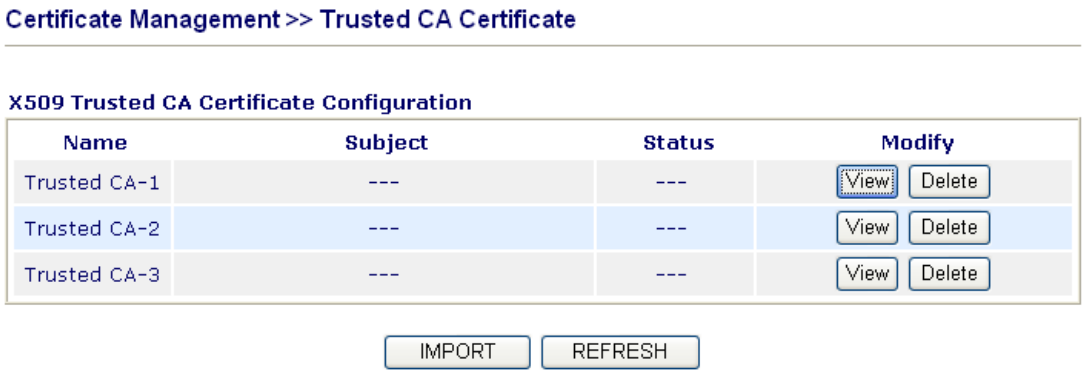
Import Click this button to import a saved file as the certification information.

Refresh	Click this button to refresh the information listed below.
View	Click this button to view the detailed settings for certificate request.

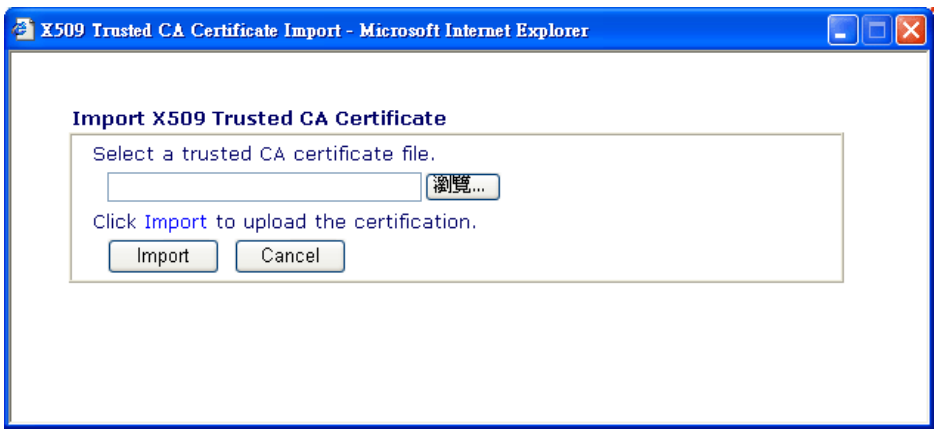
After clicking Generate, the generated information will be displayed on the window below:

3.8.2 Trusted CA Certificate

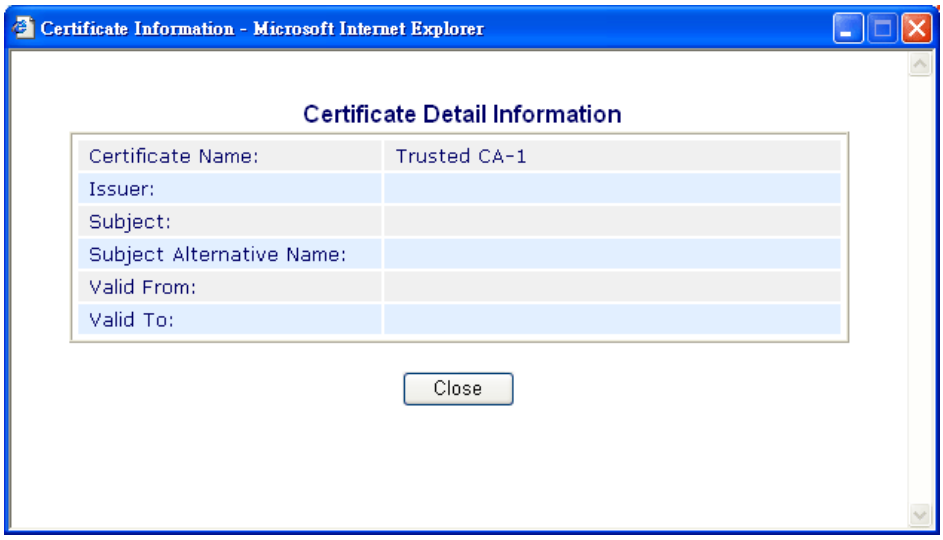
Trusted CA certificate lists three sets of trusted CA certificate.



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.



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.



3.9 Wireless LAN

This function is used for G models only.

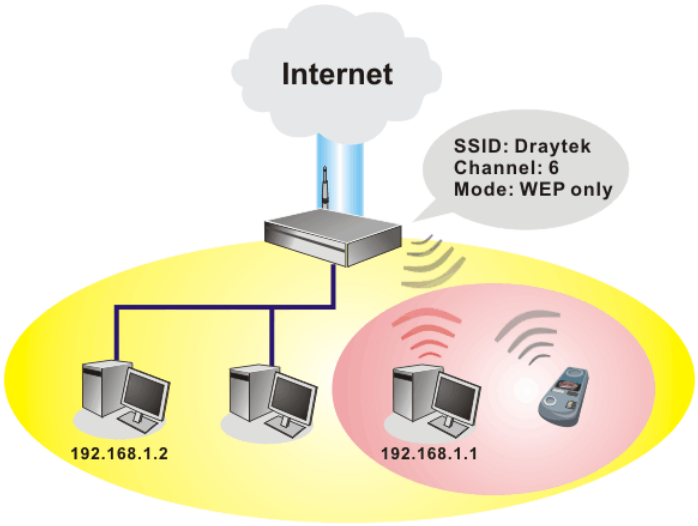
3.9.1 Basic Concepts

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

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11g protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology Super G ™ to lift up data rate up to 108 Mbps*. Hence, you can finally smoothly enjoy stream music and video.

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

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



Security Overview

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

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

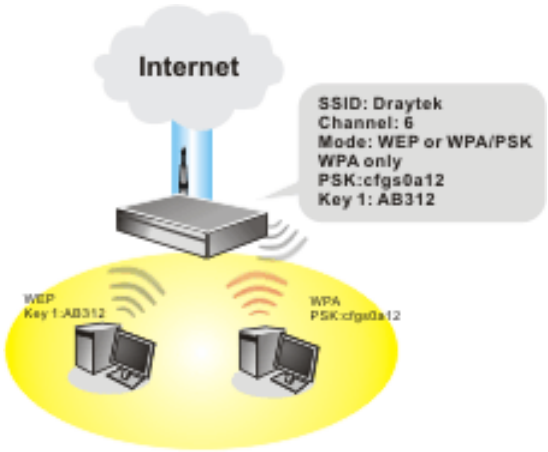
WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

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

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

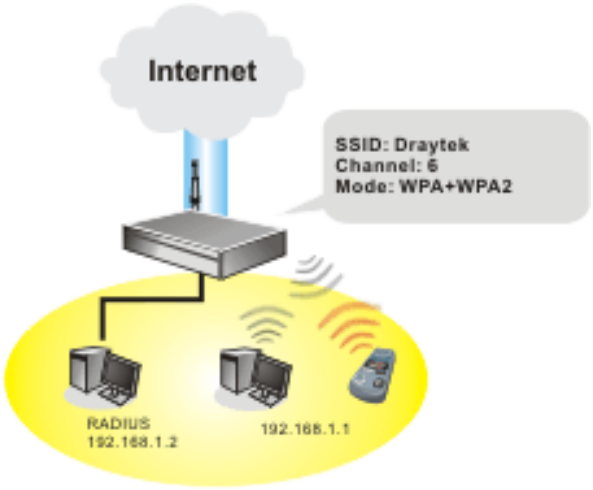
Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless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

Example 1



Example 2

Example 3

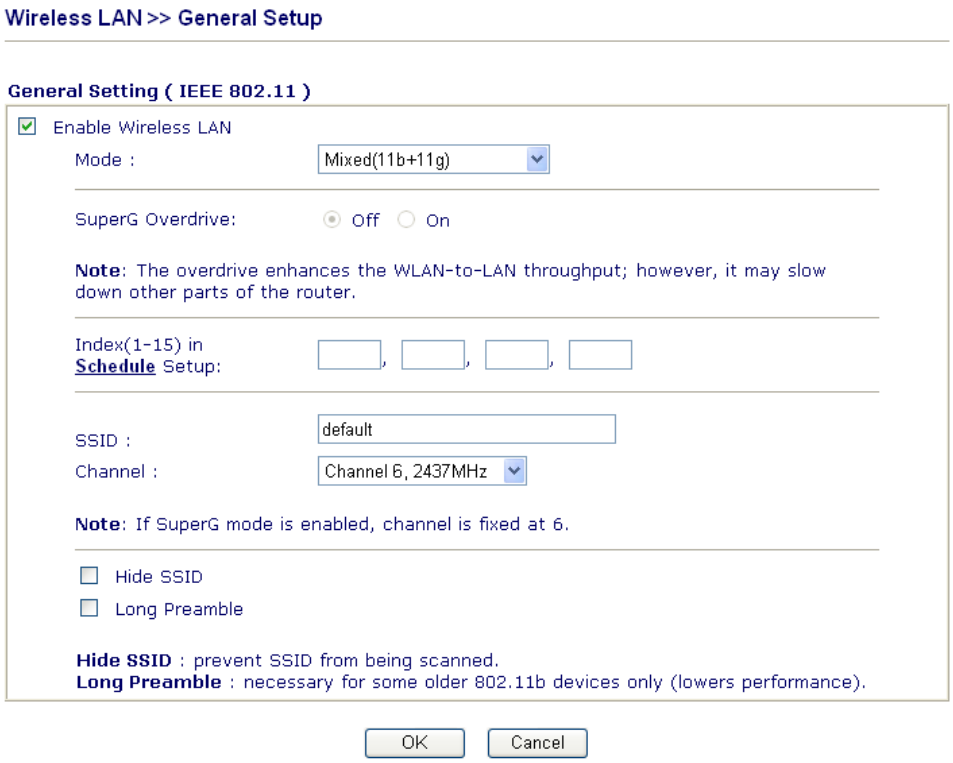


Separate the Wireless and the Wired LAN- WLAN Isolation enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate means neither of the parties can access each other. To elaborate an example for business use, you may set up a wireless LAN for visitors only so they can connect to Internet without hassle of the confidential information leakage. For a more flexible deployment, you may add filters of MAC addresses to isolate users' access from wired LAN.

Manage Wireless Stations - Station List will display all the station in your wireless network and the status of their connection.

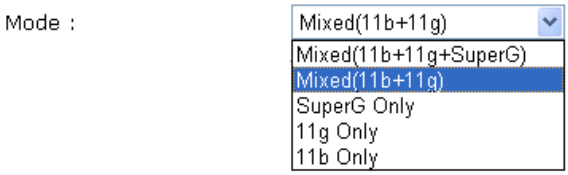
3.9.2 General Setup

By clicking the **General Settings**, a new web page will appear so that you could configure the SSID and the wireless channel. Please refer to the following figure for more information.



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

Mode — Select an appropriate wireless mode.
Mixed (11b+11g+SuperG) - The radio can support IEEE802.11b, IEEE802.11g and SuperG protocols simultaneously.
Mixed (11b+11g) - The radio can support both IEEE802.11b and IEEE802.11g protocols simultaneously.
SuperG - The radio only supports SuperG.
11g only - The radio only supports IEEE802.11g.
11b only - The radio only supports IEEE802.11b.



SuperG Overdrive — Enhance the transmission rate up to 108Mbps between the host and the clients. Generally, the maximum transmission rate is 54Mbps without such feature. Notice that the network card in client must also support SuperG. If not, the rate would be 54Mbps even if you enable this function.

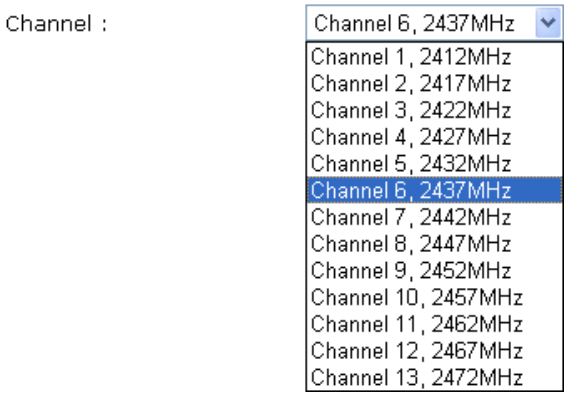
Index(1-15) — Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications** >> **Schedule** setup. The default setting of this filed is blank and the function will always work.

SSID

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

Channel

The channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference.



Hide SSID

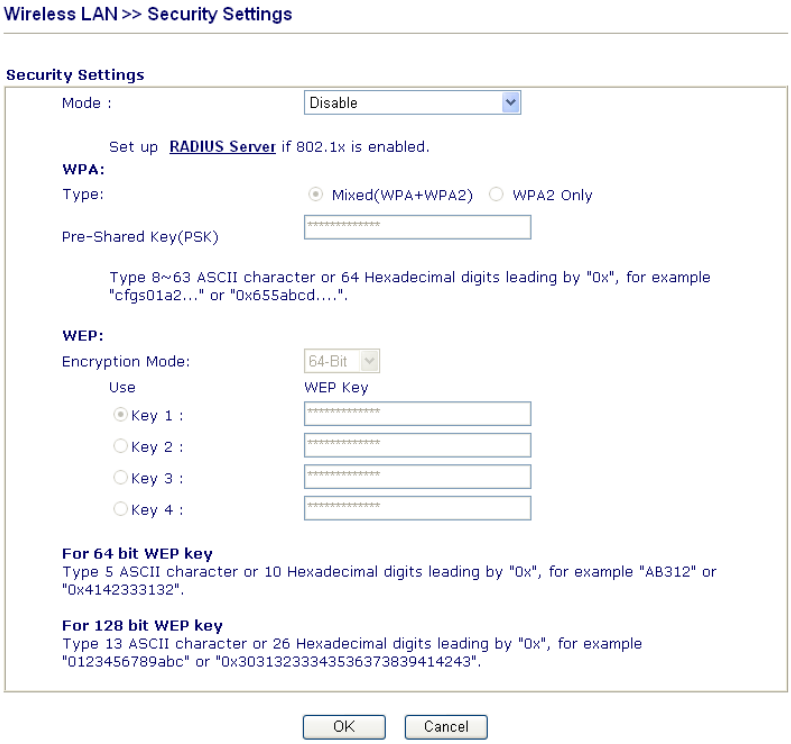
Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying.

Long Preamble

This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync filed instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Check it to use **Long Preamble** if needed to communicate with this kind of devices.

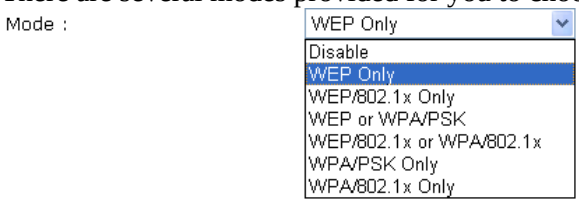
3.9.3 Security

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



Mode

There are several modes provided for you to choose.



Disable - Turn off the encryption mechanism.
WEP Only - Accept only WEP clients and the encryption key should be entered in WEP Key.
WEP/802.1x Only - Accept WEP clients with 802.1x authentication. Since the key will be auto-negotiated during authentication, the field of key setting below will be not available for input.
WEP or WPA/PSK - Accept WEP and WPA clients with legal key accordingly. Only Mixed (WPA+WPA2) is applicable if you select WPA/PSK.
WEP/802.1x or WPA/802.1x - Accept WEP or WPA clients with 802.1x authentication. Only Mixed(WPA+WPA2) is applicable if you select WPA/PSK. Since the key will be auto-negotiated during authentication, the field of key setting below will be not available for input.
WPA/PSK Only - Accept WPA clients and the encryption key should be entered in PSK. Remember to select WPA type to define either Mixed or WPA2 only in the field below.
WPA/802.1x Only - Accept WPA clients with 802.1x authentication. Remember to select WPA type to define either Mixed or WPA2 only in the field below. Since the key will be

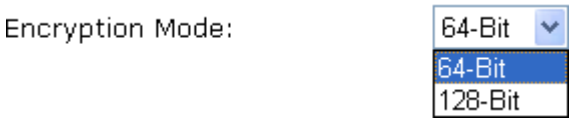
auto-negotiated during authentication, the field of key setting below will be not available for input.

WPA

The WPA encrypts each frame transmitted from the radio using the key, which either PSK entered manually in this field below or automatically negotiated via 802.1x authentication.
Type - Select from Mixed (WPA+WPA2) or WPA2 only.
Pre-Shared Key (PSK) - Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

WEP

64-Bit - For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)
128-Bit - For 128 bits WEP key, either **13** ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x41424344454647484 94A4B4C4D).

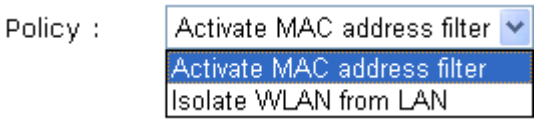


All wireless devices must support the same WEP encryption bit size and have the same key. Four keys can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

3.9.4 Access Control

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

Enable Access Control	Select to enable the MAC Address access control feature.
Policy	Select to enable any one of the following policy. Choose **Activate MAC address filter** to type in the MAC addresses for other clients in the network manually. Choose **Isolate WLAN from LAN** will separate all the WLAN stations from LAN based on the MAC Address list.
MAC Address Filter	Display all MAC addresses that are edited before. Four buttons (Add, Remove, **Client's MAC Address** - Manually enter the MAC address of wireless client.
Attribute	**s –** select it to isolate the wireless connection of the wireless client of the MAC address from LAN.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
OK	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

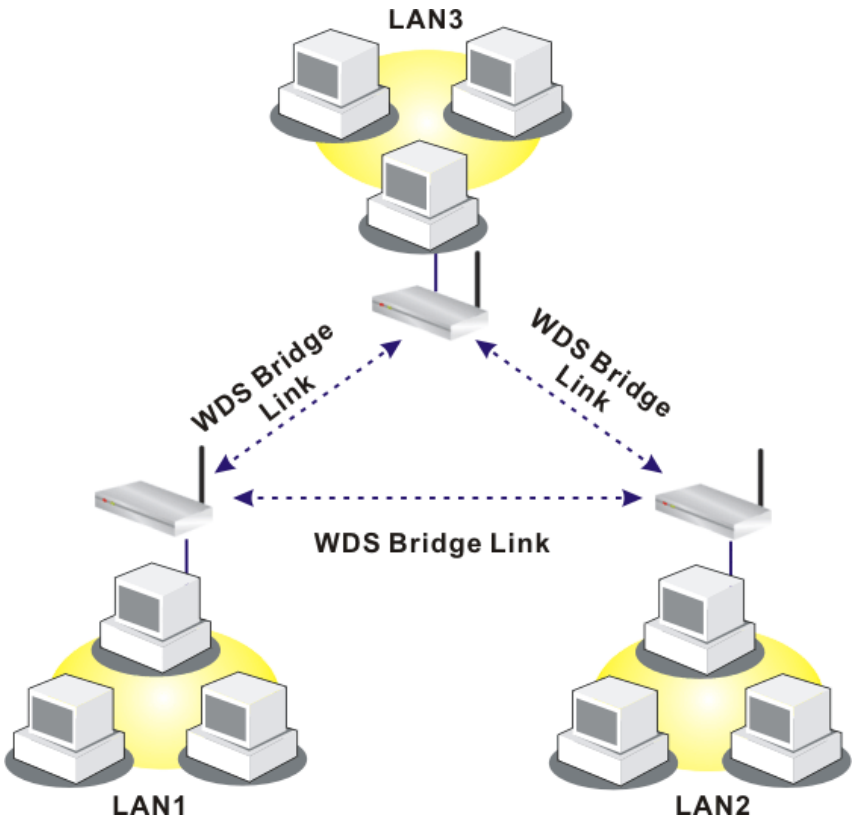


3.9.5 WDS

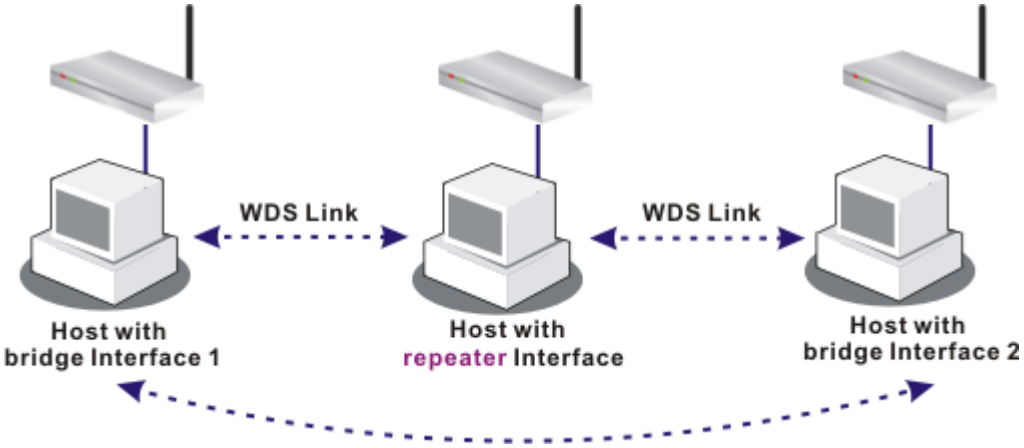
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

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

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

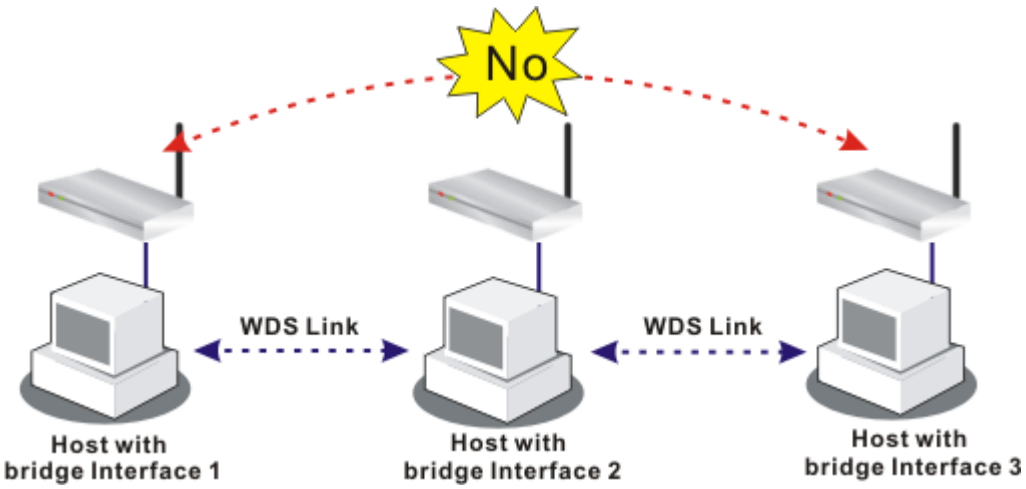


The application for the WDS-Repeater mode is depicted as below:

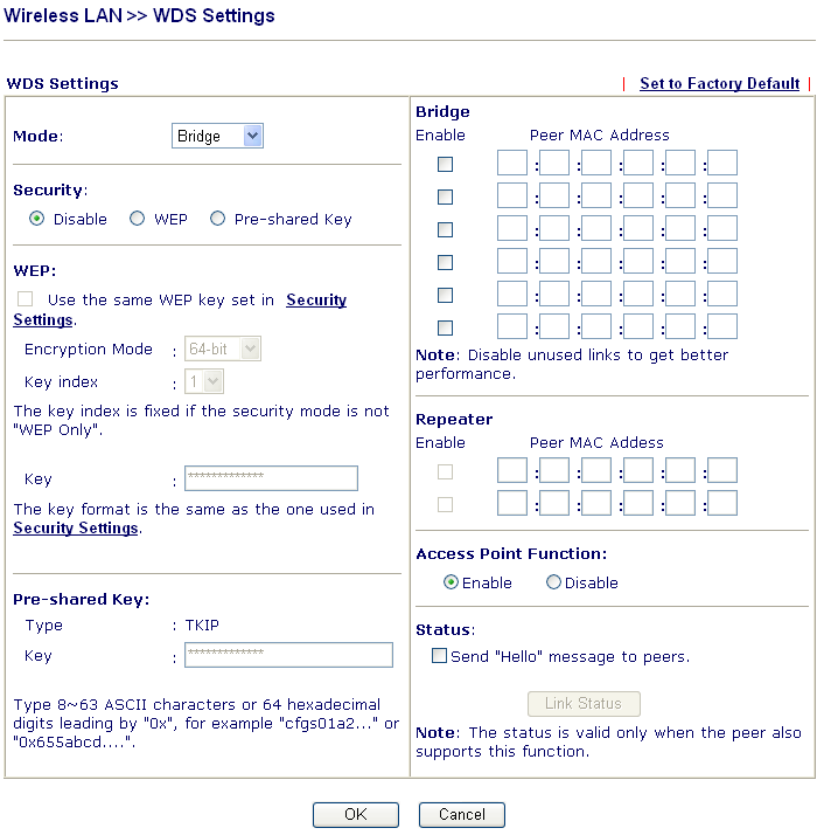


The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words,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

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

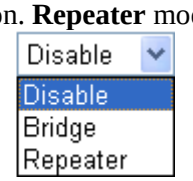


Click **WDS** from **Wireless LAN** menu. The following page will be shown.



Mode

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



Security

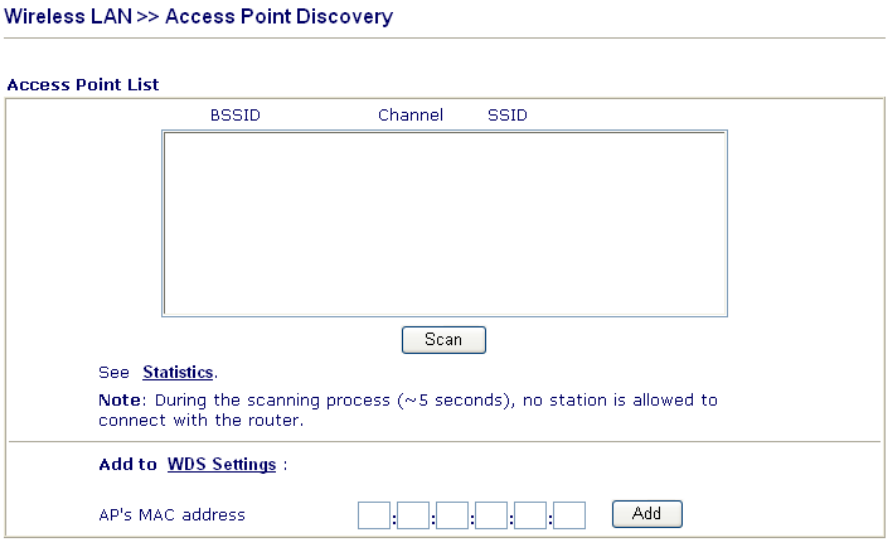
There are three types for security, **Disable**, **WEP** and **Pre-shared key**. The setting you choose here will make the

	following WEP or Pre-shared key field valid or not. Choose one of the types for the router.
WEP	Check this box to use the same key set in **Security Settings** page. If you did not set any key in **Security Settings** page, this check box will be dimmed. **Encryption Mode** - If you checked the box of **Use the same WEP key …**, you do not need to choose 64-bit or 128-bit as the Encryption Mode. If you do not check that box, you can set the WEP key now in this page. **Key Index** - Choose the key that you want to use after selecting the proper encryption mode. **Key** - Type the content for the key.
Pre-shared Key	Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by “0x”.
Bridge	If you choose Bridge as the connecting mode, please type in the peer MAC address in these fields. **Six** peer MAC addresses are allowed to be entered in this page at one time. Yet please disable the unused link to get better performance. If you want to invoke the peer MAC address, remember to check **Enable** box in the front of the MAC address after typing.
Repeater	If you choose Repeater as the connecting mode, please type in the peer MAC address in these fields. Two peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check **Enable** box in the front of the MAC address after typing.
Access Point Function	Click **Enable** to make this router serving as an access point; click **Disable** to cancel this function.
Status	It allows user to send “hello” message to peers. Yet, it is valid only when the peer also supports this function.

3.9.6 AP Discovery

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

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



If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click **Add**. Later, the MAC address of the AP will be added to the page of WDS setting.

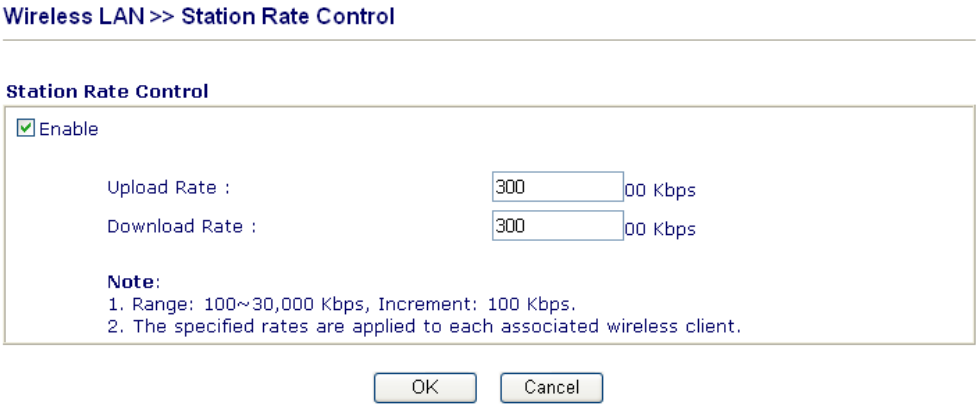
3.9.7 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code. There is a code summary below for explanation. For convenient **Access Control**, you can select a WLAN station and click **Add to Access Control** below.

Refresh	Click this button to refresh the status of station list.
Add	Click this button to add current selected MAC address into **Access Contro**l.

3.9.8 Station Rate Control

This page allows you to control the upload and download rate of each wireless client (station). Please check the box of **Enable** to invoke this setting. The range for the rate is between 100 ~ 30,000 kbps.



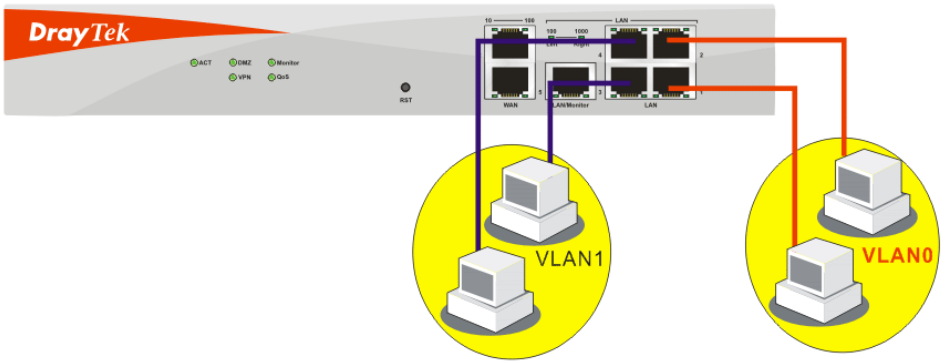
3.10 VLAN

Note: This menu is available for **Vigor3100G** model only. For Vigor3100 and Vigor3120, please refer to 3.2.4.

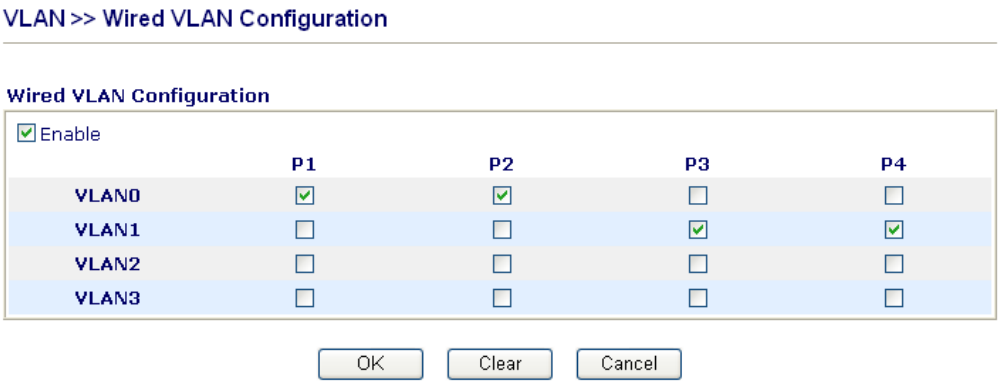
Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port.

3.10.1 Wired VLAN

PCs connected to Ethernet ports of the router can be divided into different groups and formed VLAN. PCs under the same groups can share each other information through the router and will not be peeked by other groups.



The **VLAN >> Wired VALN** allows you to configure VLAN settings through wired connection to achieve the above intention. Simply check P1 and P2 boxes on the line of VLAN0; and check P3 and P4 boxes on the line of VLAN1.



Enable Check this box to enable this function (for VLAN Configuration).

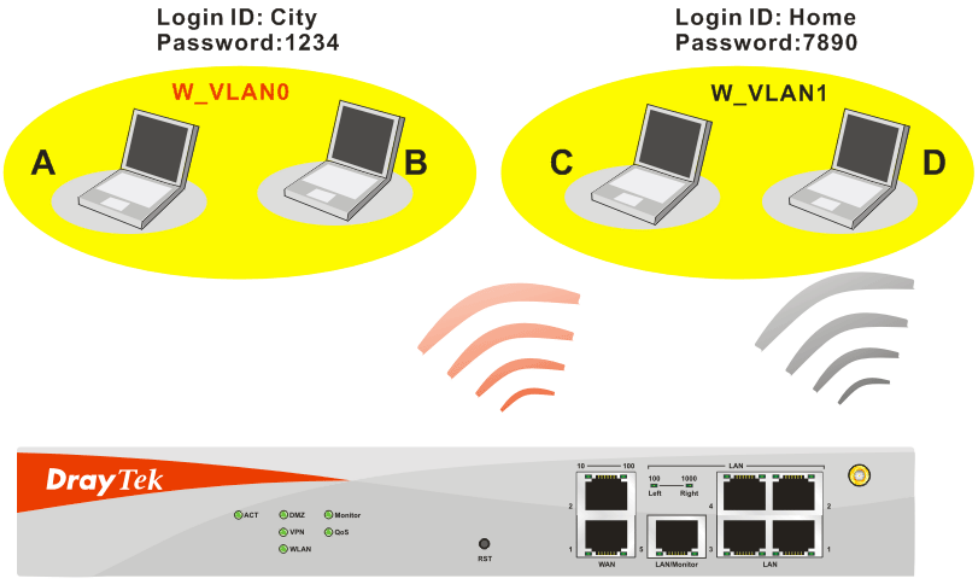
P1 – P4 Check the box to make the computer connecting to the port being grouped in specified VLAN. Be aware that each port can be grouped in different VLAN at the same time only if you check the box. For example, if you check the boxes of VLAN0-P1 and VLAN1-P1, you can make P1 to be grouped under VLAN0 and VLAN1 simultaneously.

VLAN0-3 This router allows you to set 4 groups of virtual LAN.

3.10.2 Wireless VLAN

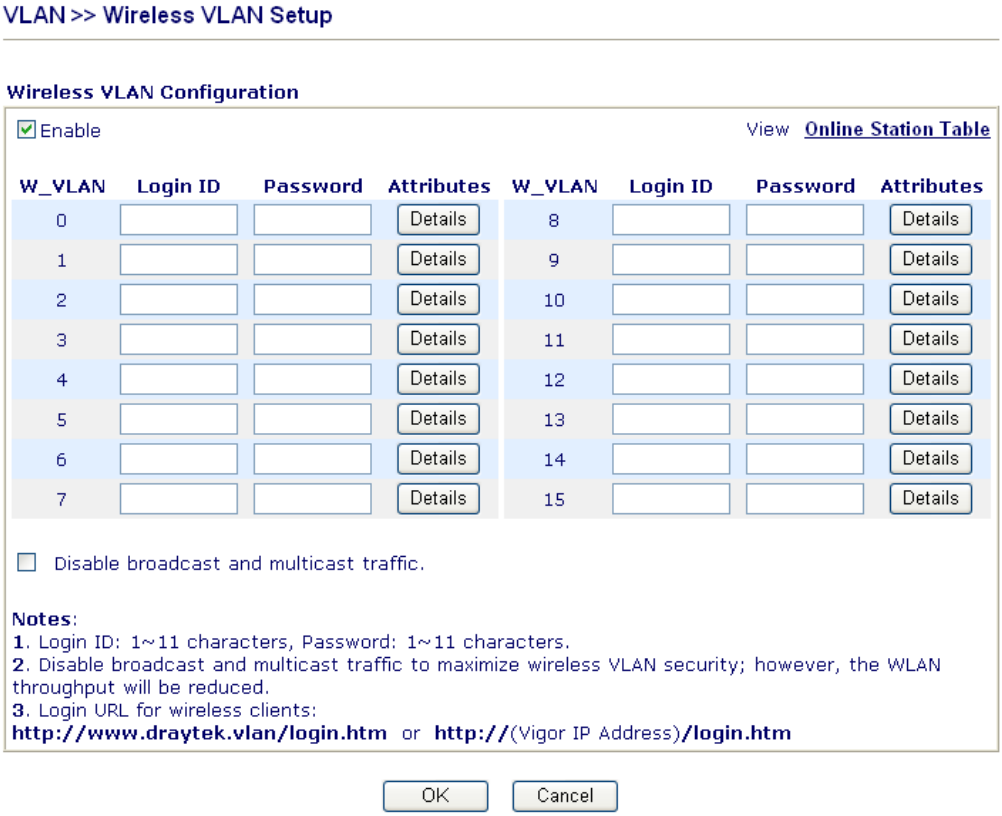
PCs (equipped with wireless network cards) connected to the router through wireless interface can be divided into different groups and formed W_VLAN. PCs under the same groups can share each other information through the router and will not be peeked by other groups.

PCs under the same groups can use same Login ID and password to access into Internet. For example, see the following graphic. Both A and B use the same login ID (City) and password (1234). Therefore, they are grouped in the same W_VLAN.



The **VLAN >> Wireless VALN** allows you to configure Wireless VLAN settings through wireless connection to achieve the above intention. Simply type Login ID and password with **City** and **1234** in the boxes of W_VLAN0. And type Login ID and password with **Home** and

7890 in the boxes of W_VLAN1. Users can configure fifteen groups of wireless VLAN in this page.

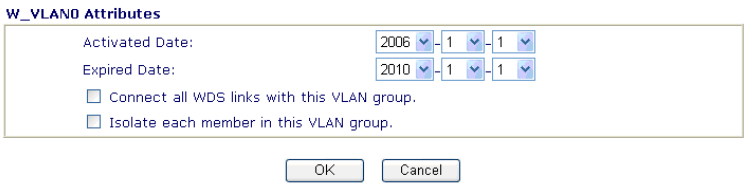


Enable Check this box to invoke wireless VLAN function.

Login ID Type Login ID for different groups of W_VLAN with 1 to 11 characters.

Password Type password for different groups of W_VLAN with 1 to 11 characters.

Details Click this button to set additional attributes settings for W_VLAN.



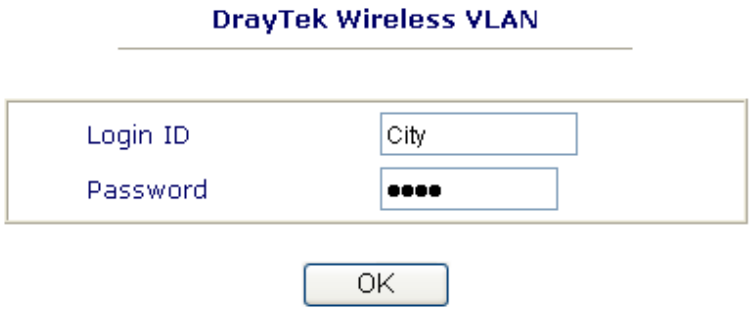
Activated Date – Use the drop down lists to set the activated date for the wireless VLAN. The wireless VLAN function will be available when the time is arrival.
Expired Date – Use the drop down lists to set the expired date for the wireless VALN. This function will be invalid when the time is arrival.
Connect all WDS links with this VALN group – Check this box to activate this connection.
Isolate each member in this VLAN group – Check this box to isolate all the members in this VLAN group and not allow the information sharing among them.

Disable broadcast and multicast traffic	Check this box to prevent broadcast and multicast traffic forwarding to all W_VLAN.

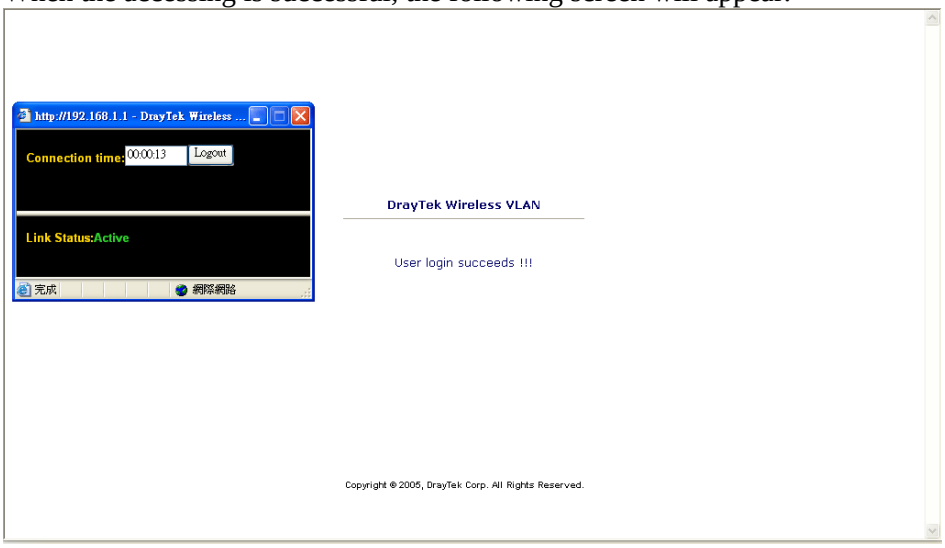
How can you (wireless client) access into Internet?

After finishing the configuration of wireless VLAN, the wireless clients connecting to this router must do the following steps to access into Internet.

1. Open a browser and type http://www.draytek.vlan/login.htm or http://(vigor router's IP address)/login.htm on the address line.
2. The following screen will appear.

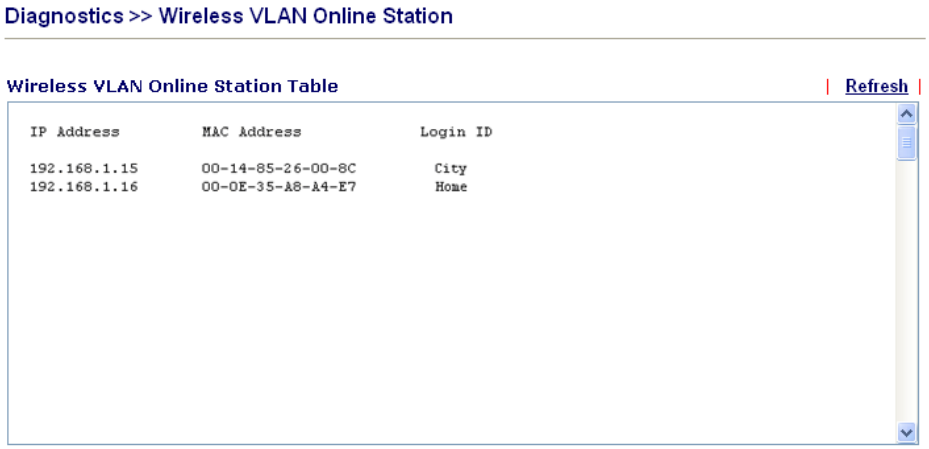


3. Type in Login ID and Password that was configured in Wireless VLAN Setup page. In this case, we choose the configuration set in first group of W_VLAN (City and 1234).
4. When the accessing is successful, the following screen will appear.



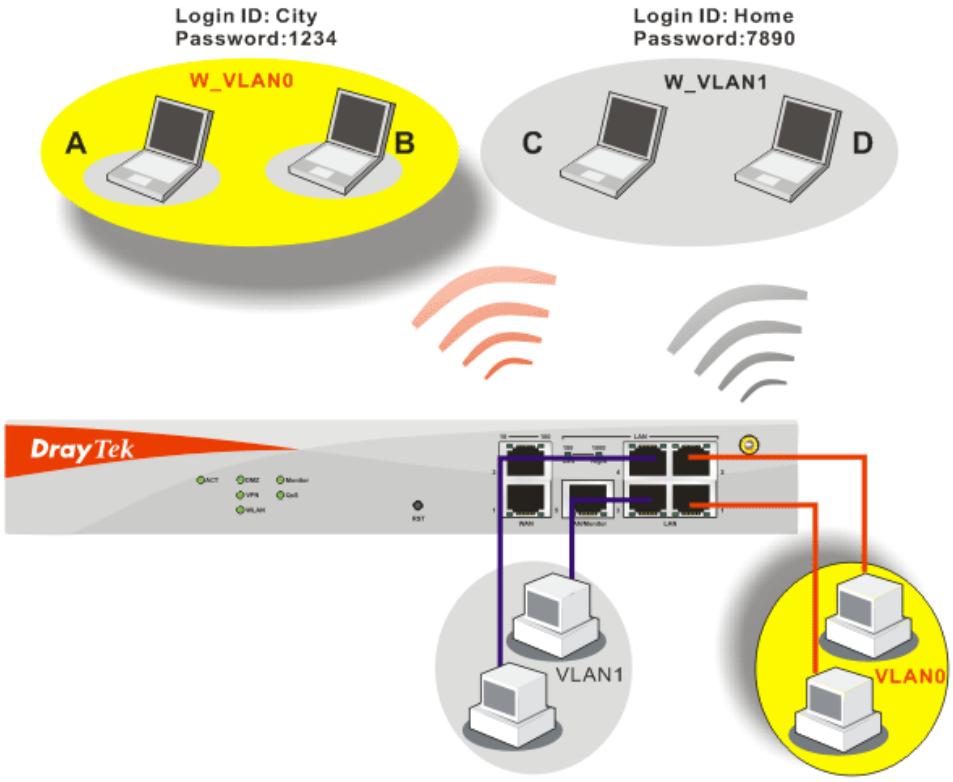
Note: The floating window with connection time will be shown on the screen till you logout.

5. You can go to **Diagnostics>>Wireless VLAN Online Station** for viewing the connection status whenever you want.

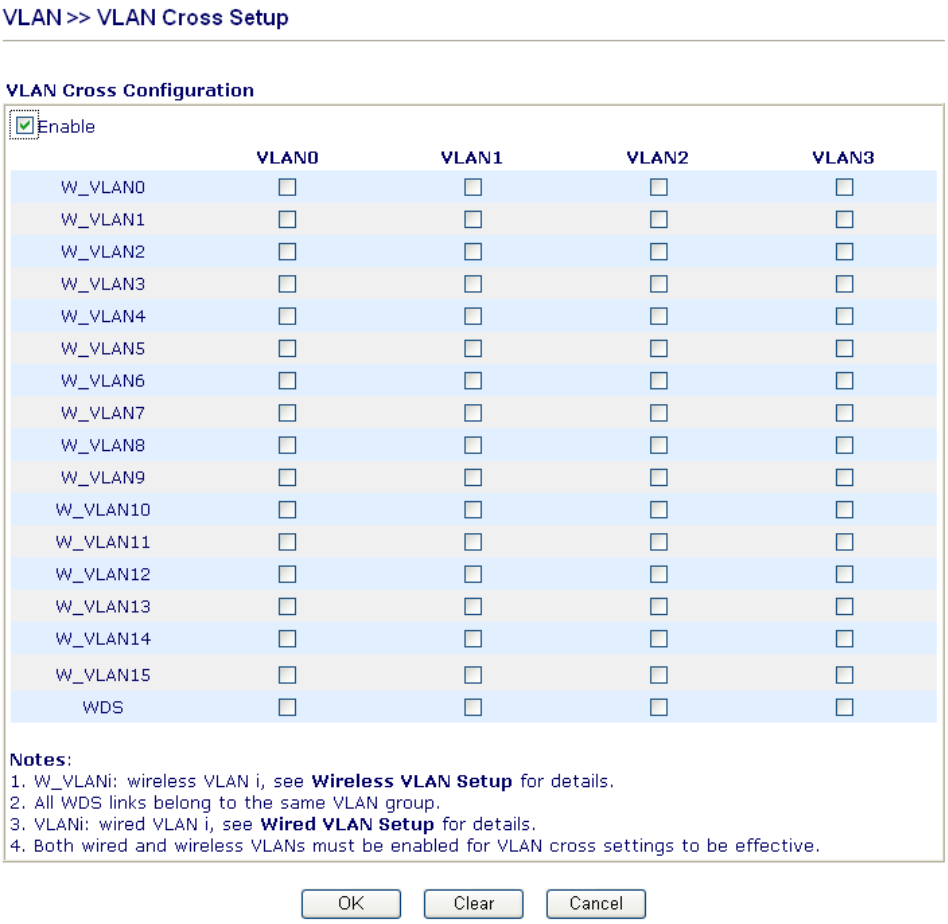


3.10.3 VLAN Cross Setup

This function allows the router to integrate VLAN and W_VLAN for managing different computers (notebooks). See the following picture for an example. With **VLAN Cross Setup**, notebook A/B and PCs on VLAN0 can share resources without difficulty.



The **VLAN >> VALN Cross Setup** allows you to set a communication bridge between computers in Wireless VLAN and wired VLAN. To achieve the intention of the above illustration, simply check the box under VLAN0 on the line of W_VLAN0.



Enable Check this box to invoke VLAN Cross Setup function.

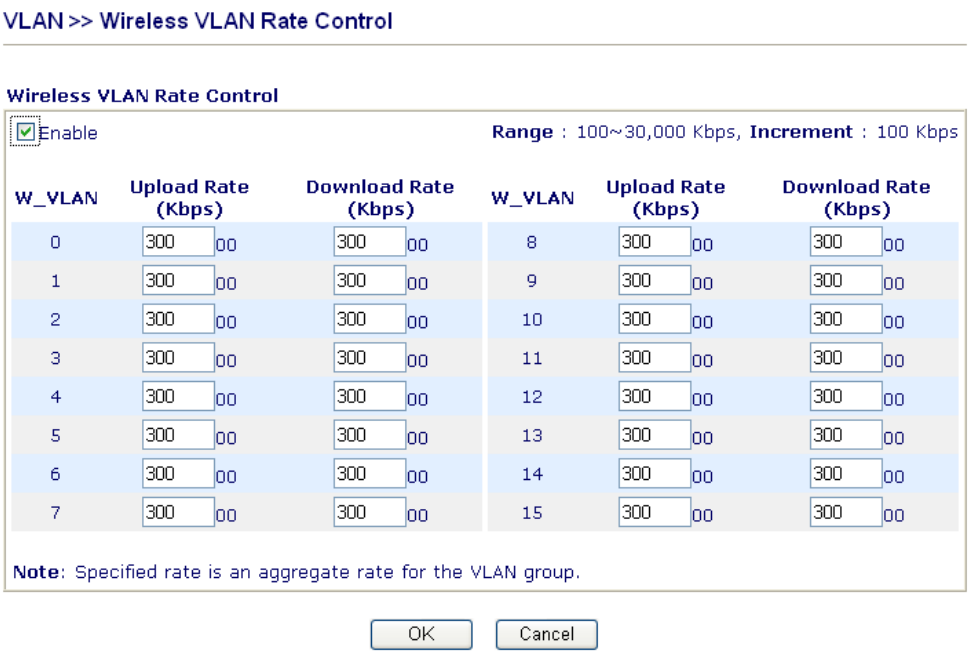
VLAN0-3 It represents the groups of virtual LAN connected by Ethernet interface.

W_VLAN0-15 It represents the groups of wireless VLAN communicated by wireless interface.

3.10.4 Wireless Rate Control

Rate Control manages the transmission rate of data in and out through the router. You can also manage the in/out rate of each wireless VLAN. Go to **VLAN** menu and select **Wireless Rate Control**. The following page will appear. Click **Enable** to invoke VLAN function.

For the rate control of wireless connection, please open VLAN menu and choose **Wireless Rate Control**. The following page will be shown for you to adjust.



Enable — Check this box to enable this function (for Rate Control). The rate control will limit the transmission rate for upload and download.

Upload Rate — It decides the rate of data transmission for output. The default setting is 300. The range must be between 100 kbps to 20,000kbps. Adjust the values according to your necessity.

Download Rate — It decides the rate of data transmission for input. The default setting is 300. The range must be between 100 kbps to 20,000kbps. Adjust the values according to your necessity.

3.11 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.

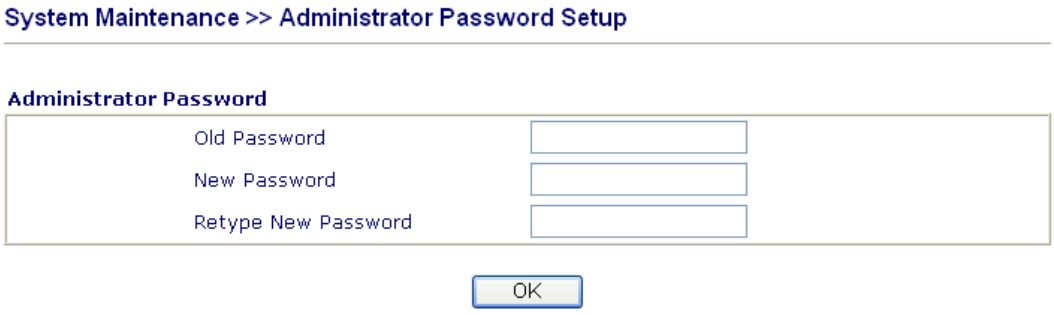
3.11.1 System Status

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	Displays the model name of the router.
Firmware Version	Displays the firmware version of the router.
Build Date/Time	Displays the date and time of the current firmware build.
MAC Address	Displays the MAC address of the LAN Interface.
1st IP Address	Displays the IP address of the LAN interface.
1st Subnet Mask	Displays the subnet mask address of the LAN interface.
DHCP Server	Displays the current status of DHCP server of the LAN interface.
MAC Address	Displays the MAC address of the WAN Interface.
IP Address	Displays the IP address of the WAN interface.
Default Gateway	Displays the assigned IP address of the default gateway.
DNS	Displays the assigned IP address of the primary DNS.

3.11.2 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.
Retype New Password	Type in the new password again.

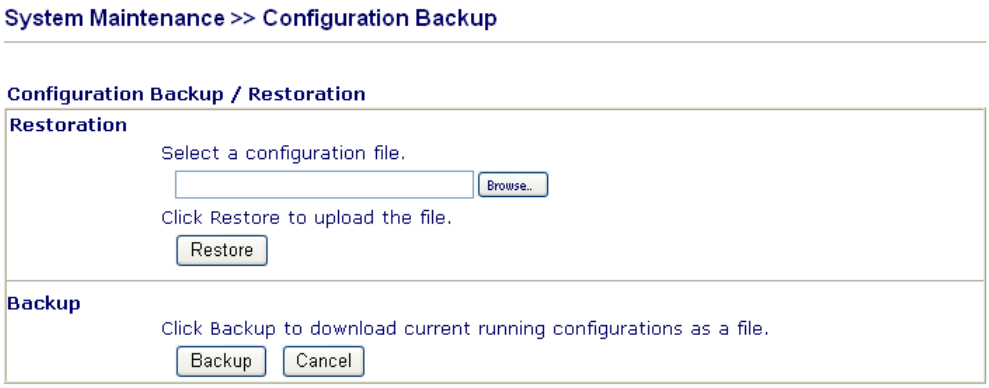
When you click OK, the login window will appear. Please use the new password to access into the web configurator again.

3.11.3 Configuration Backup

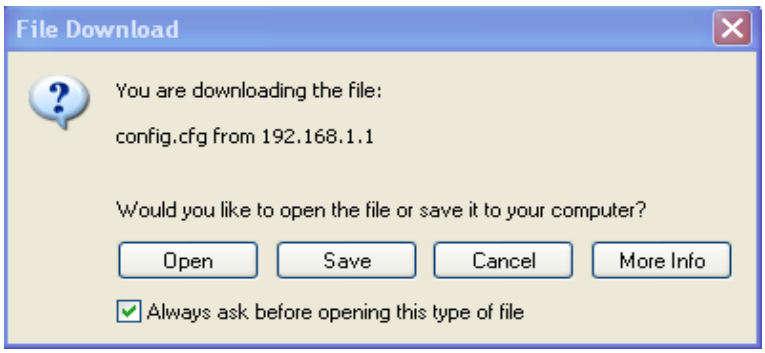
Backup the Configuration

Follow the steps below to backup your configuration.

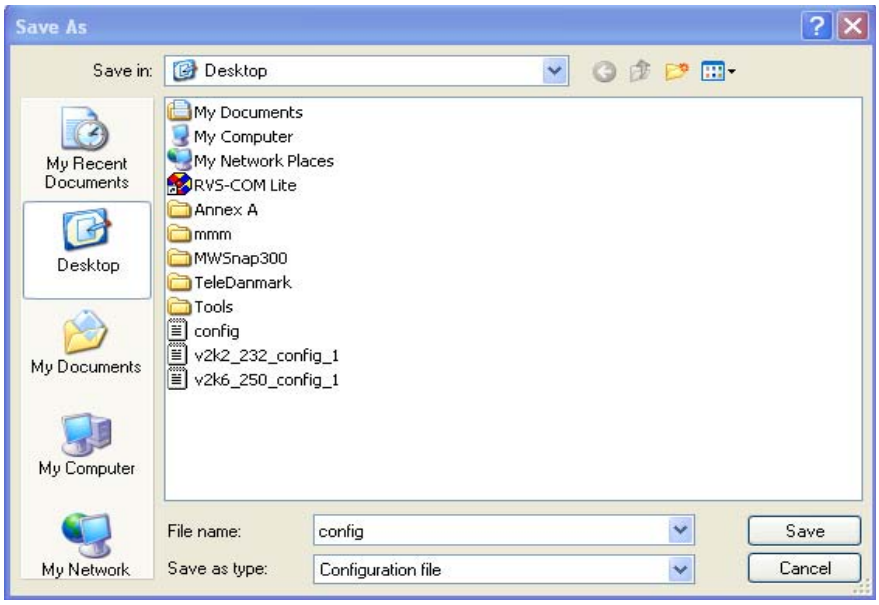
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.



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.

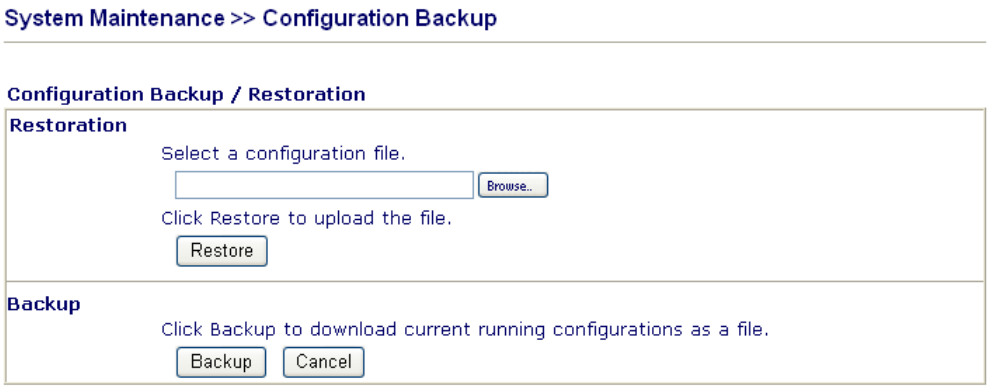


4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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.

Restore Configuration

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

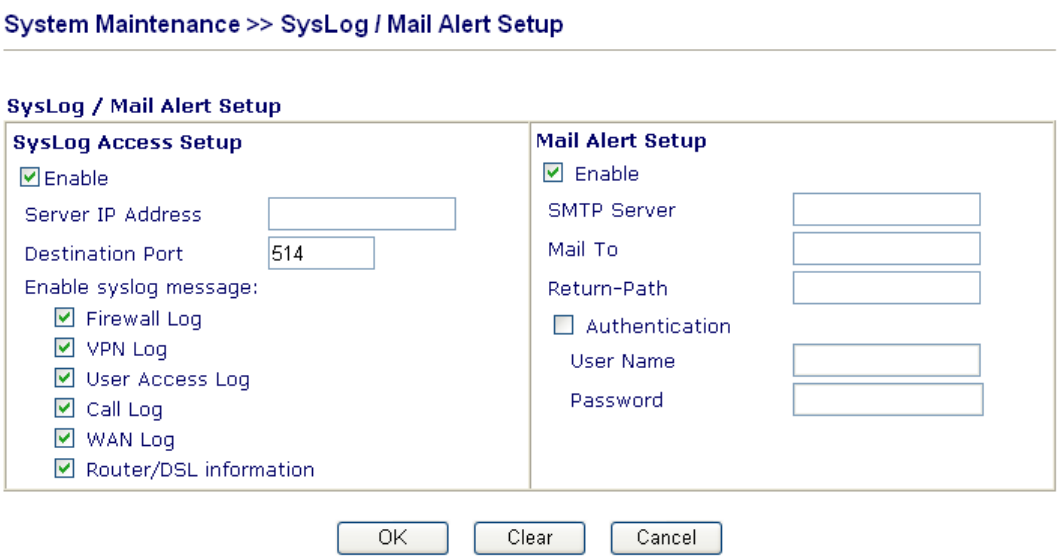


2. Click **Browse** button to choose the correct configuration file for uploading to the router.

3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

3.11.4 Syslog/Mail Alert

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

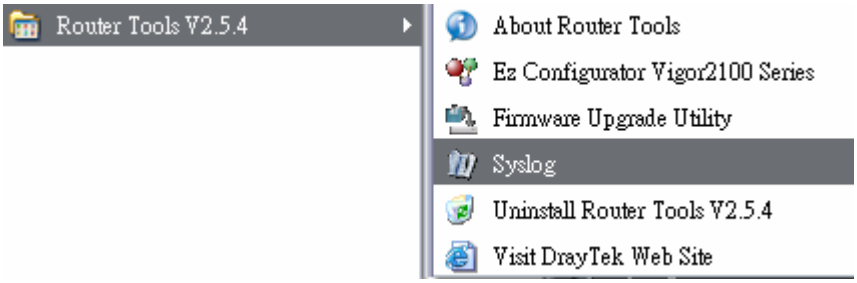


Enable	Click "**Enable**" to activate this function.
Server IP Address	The IP address of the Syslog server.
Destination Port	Assign a port for the Syslog protocol.
Enable syslog message	Check the box to display the specified log.
SMTP Server	The IP address of the SMTP server.
Mail To	Assign a mail address for sending mails out.
Return-Path	Assign a path for receiving the mail from outside.

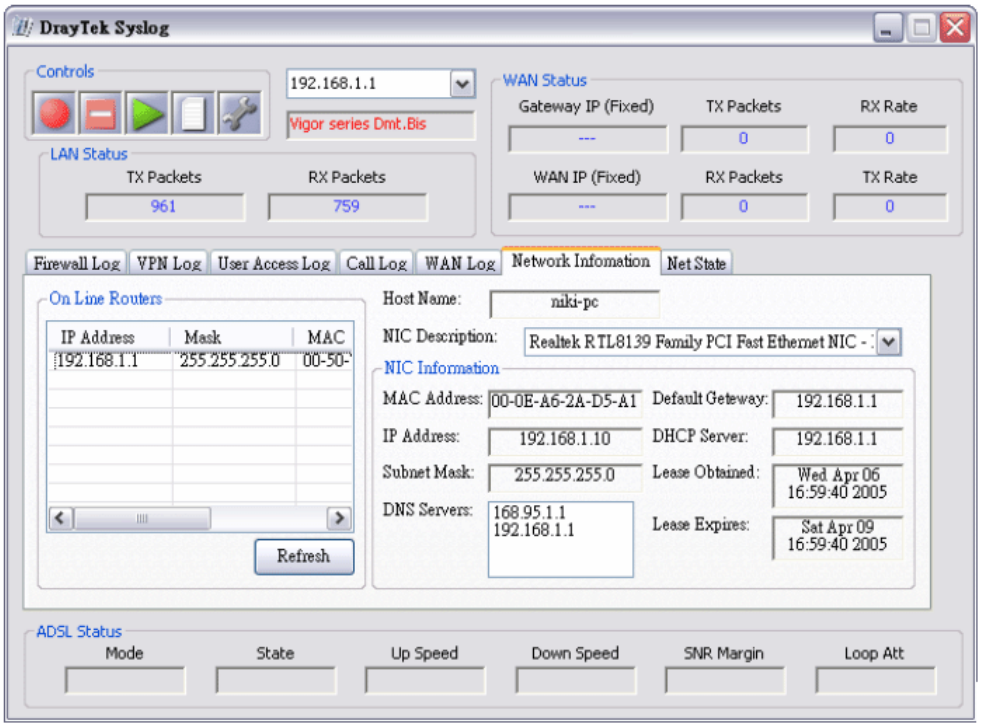
Click **OK** to save these settings.

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.

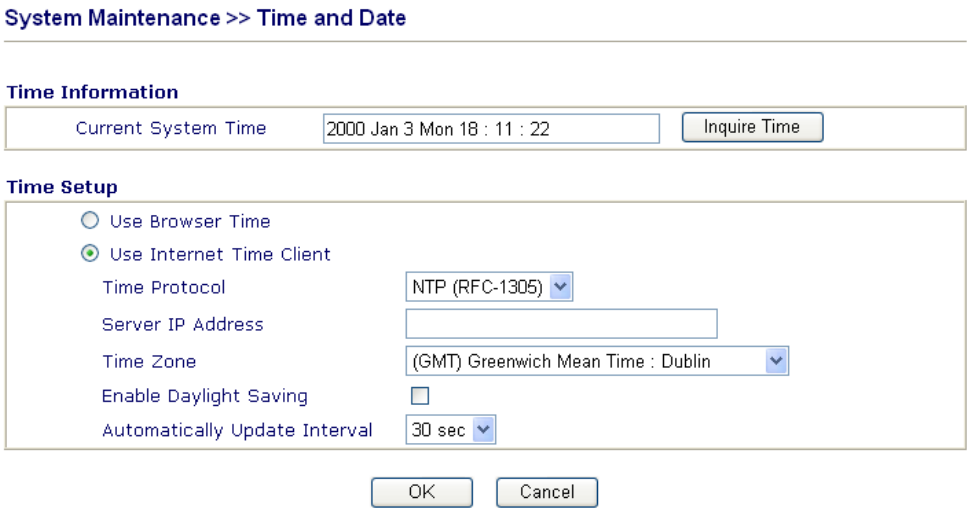


3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.



3.11.5 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 sever.

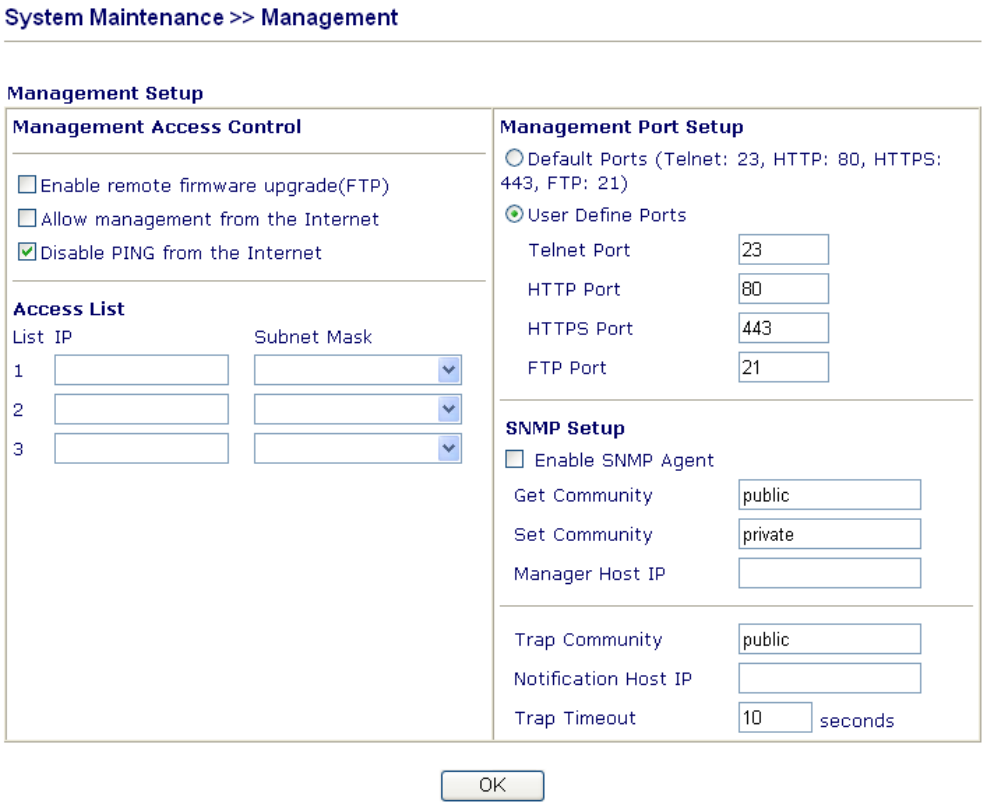
Time Zone Select the time zone where the router is located.

Automatically Update Interval Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

3.11.6 Management

The port number 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.

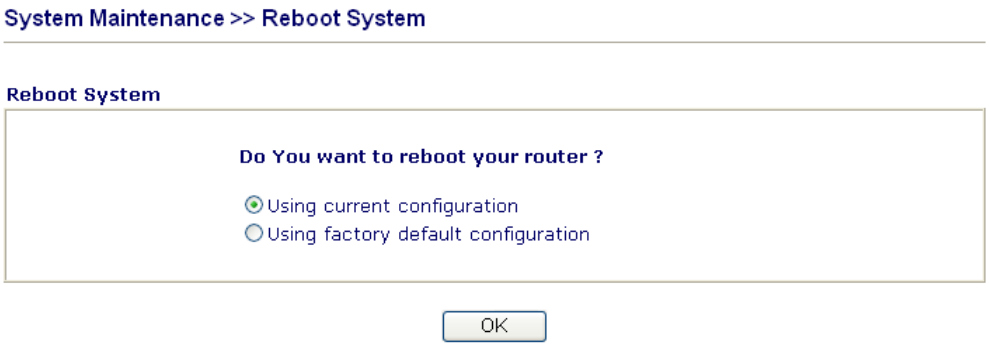


Enable remote firmware upgrade	Chick the checkbox to allow remote firmware upgrade through FTP (File Transfer Protocol).
Allow management from the Internet	Enable the checkbox to allow system administrators to login from the Internet. By default, it is not allowed.
Disable PING from the Internet	Check 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.
Default Ports	Check to use standard port numbers for the Telnet and HTTP servers.
User Defined Ports	Check to specify user-defined 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.

3.11.7 Reboot System

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



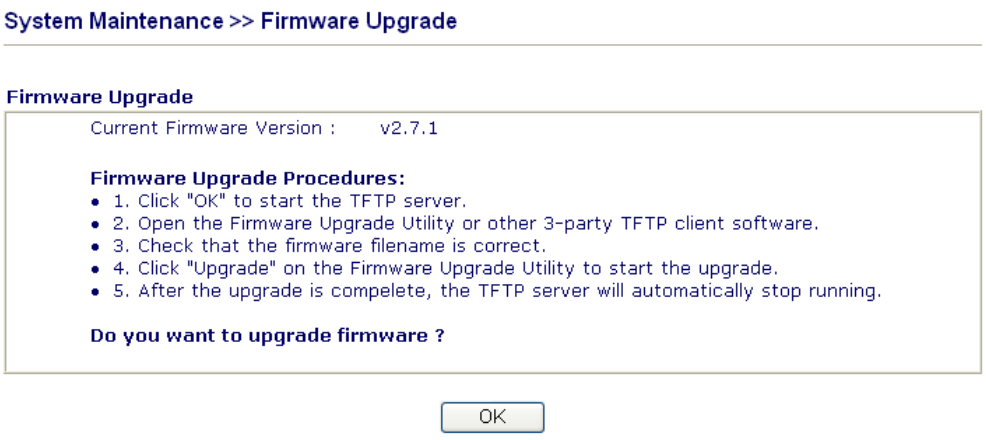
If you want to reboot the router using the current configuration, check **Using current configuration** and click **OK**. To reset the router settings to default values, check **Using factory default configuration** and click **OK**. The router will take 5 seconds to reboot the system.

3.11.8 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 steps will guide you to upgrade firmware. In the following, we use an example to explain the firmware upgrade. 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.

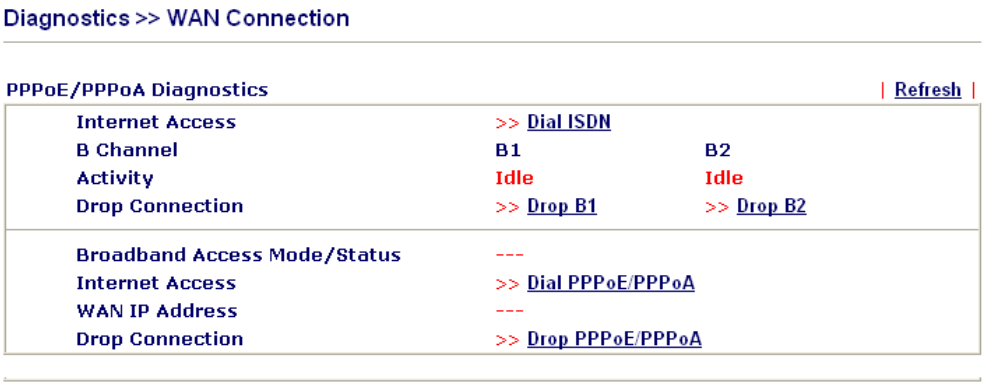


3.12 Diagnostics

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

3.12.1 WAN Connection

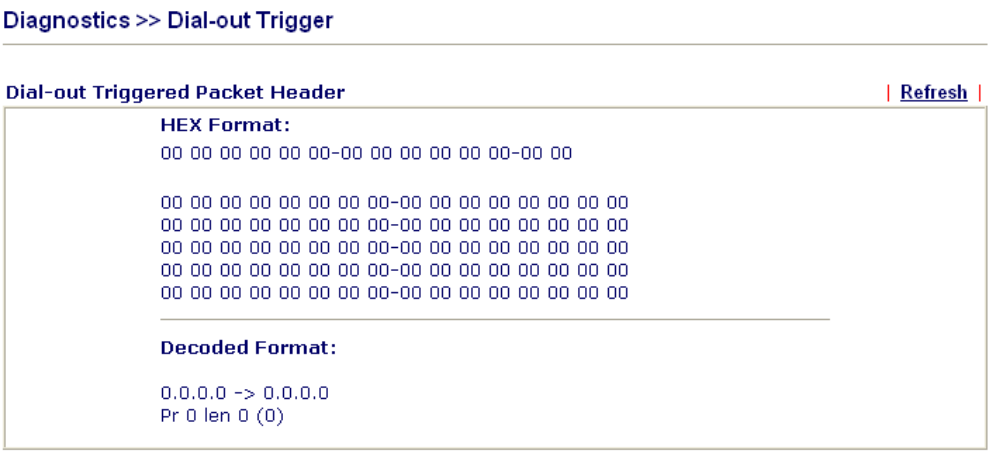
Click **Diagnostics** and click **WAN Connection** to open the web page.



Refresh	To obtain the latest information, click here to reload the page.
Broadband Access Mode/Status	Display the broadband access mode and status. If the broadband connection is active, it will show Internet access mode is enabled. If the connection is idle, it will show "**---**".
WAN IP Address	The WAN IP address for the active connection.
Dial PPPoE or PPPoA	Click it to force the router to establish a PPPoE or PPPoA connection.

3.12.2 Dial-out Trigger

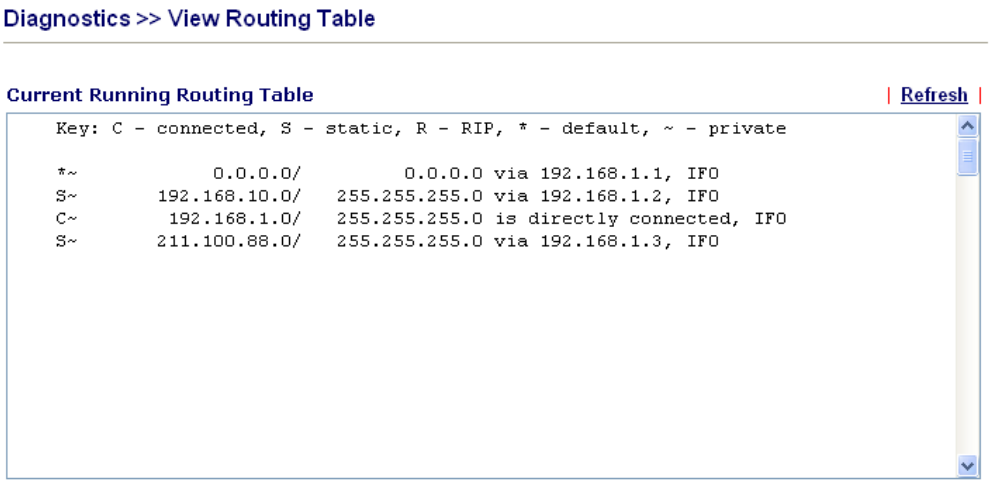
Click **Diagnostics** and click **Dial-out Trigger** to open the web page.



Refresh	Click it to reload the page.

3.12.3 Routing Table

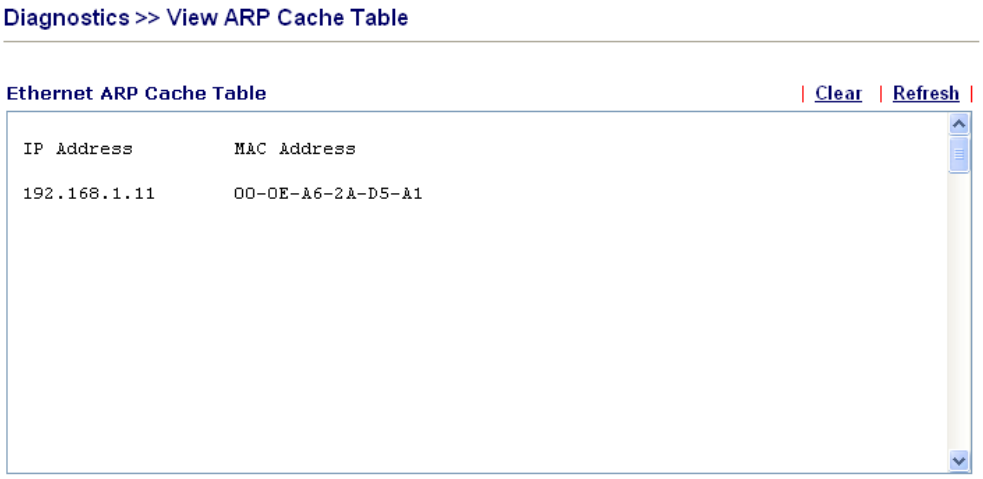
Click **Diagnostics** and click **Routing Table** to open the web page.



Refresh Click it to reload the page.

3.12.4 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.



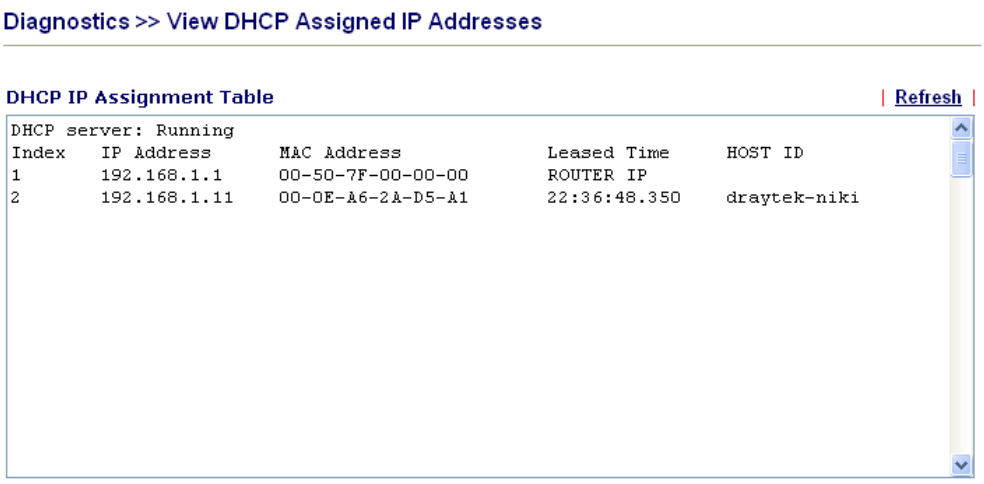
Refresh Click it to reload the page.

Clear Click it to clear the whole table.

3.12.5 DHCP Table

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

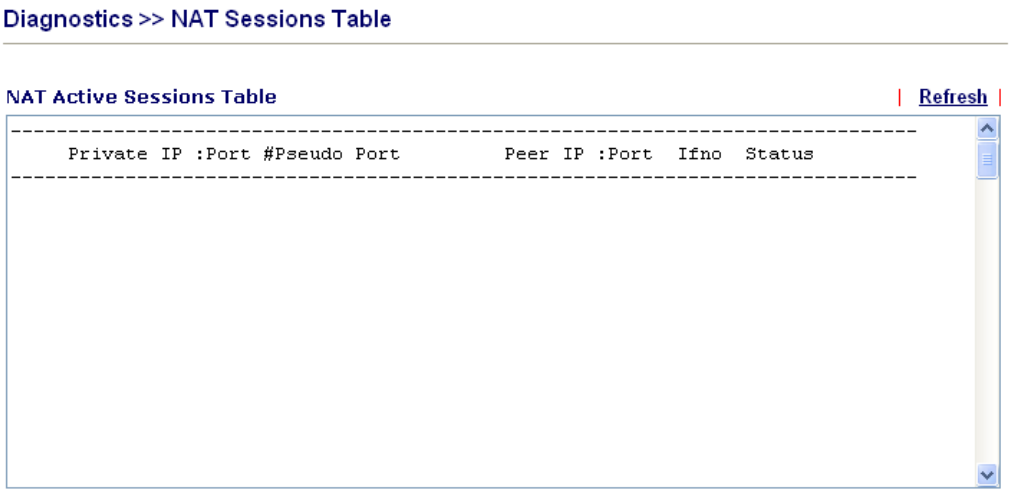
Click **Diagnostics** and click **DHCP Table** to open the web page.



Refresh Click it to reload the page.

3.12.6 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.

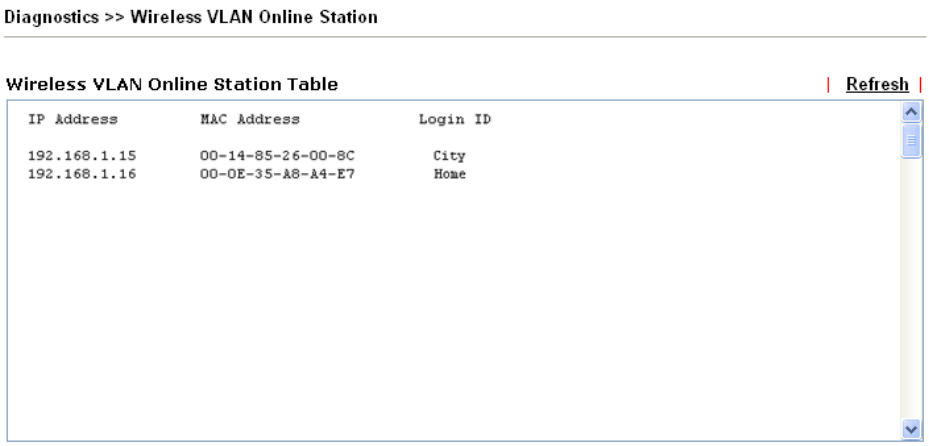
Ifno It indicates the interface of the WAN connection.

Refresh Click it to reload the page.

3.12.7 Wireless VLAN Online Station Table

This function is available for **G** model only.

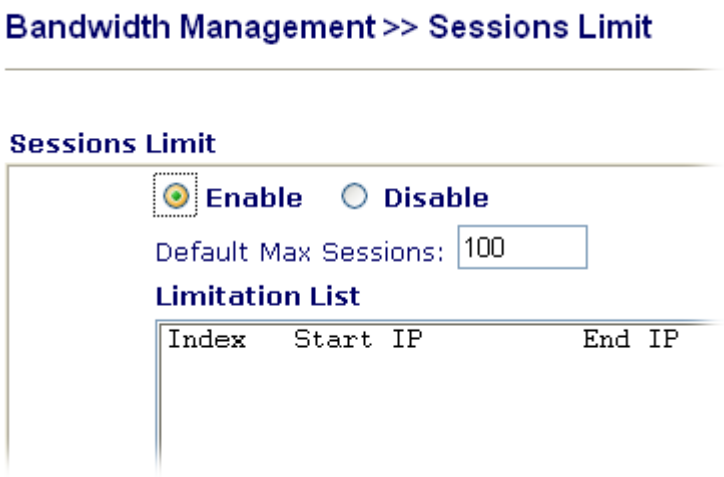
Click **Diagnostics** and click **Wireless VLAN Online Station Table to** open the web page. It will display the IP address, MAC address and Login ID information for all the Wireless VLAN stations.



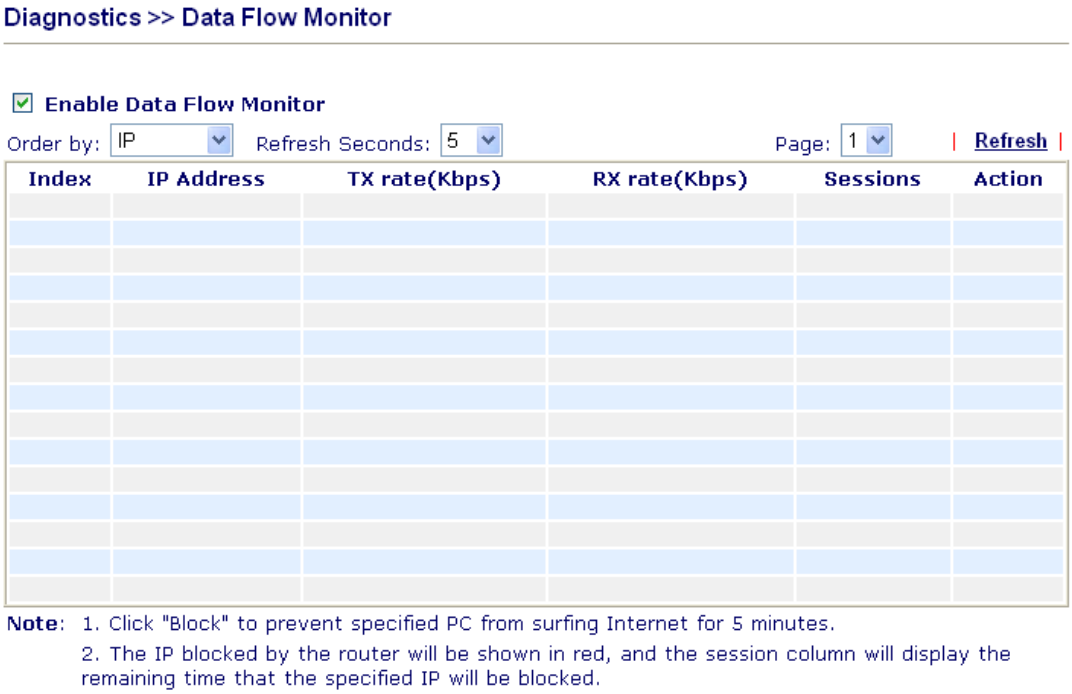
IP Address	Display the IP address of the wireless station.
MAC Address	Display the MAC address of the wireless station.
Login ID	Display the login ID that the wireless station belongs to.

3.12.8 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.

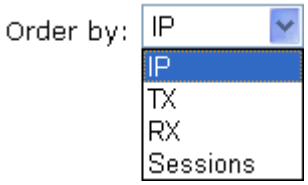


Click **Diagnostics** and click **Data Flow Monitor** to open the web page.

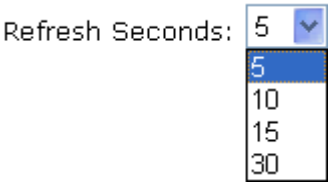


Enable Data Flow Monitor Check this box to enable this function.

Order by Use the drop down list to choose the order of data arranging.



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.

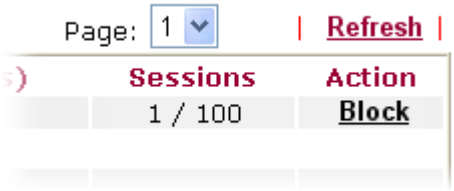
IP Address Display the IP address of the monitored device.

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.

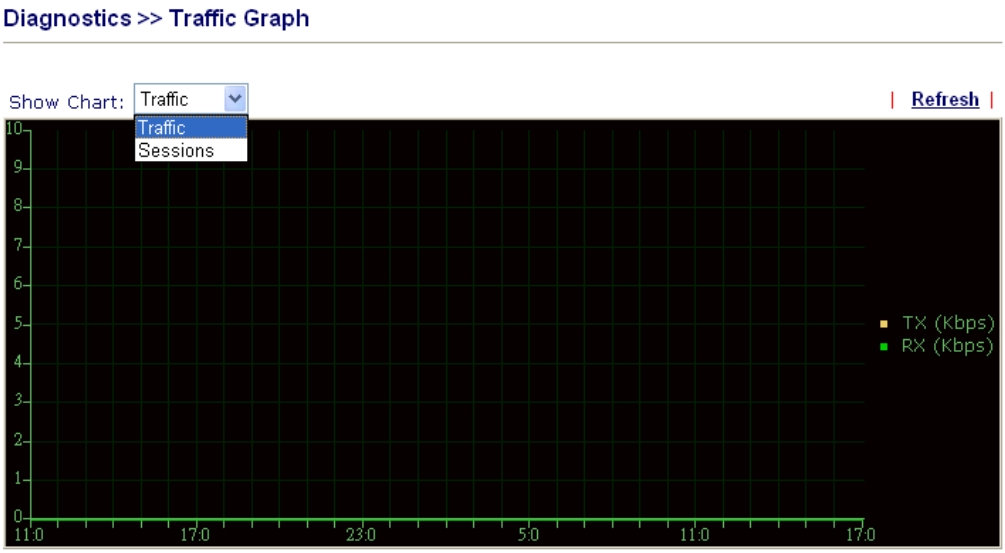
Action **Block** - can prevent specified PC accessing into Internet within 5 minutes.



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

3.12.9 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.

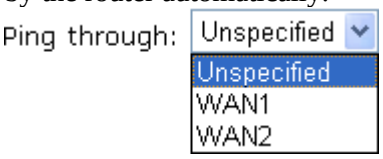


The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

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

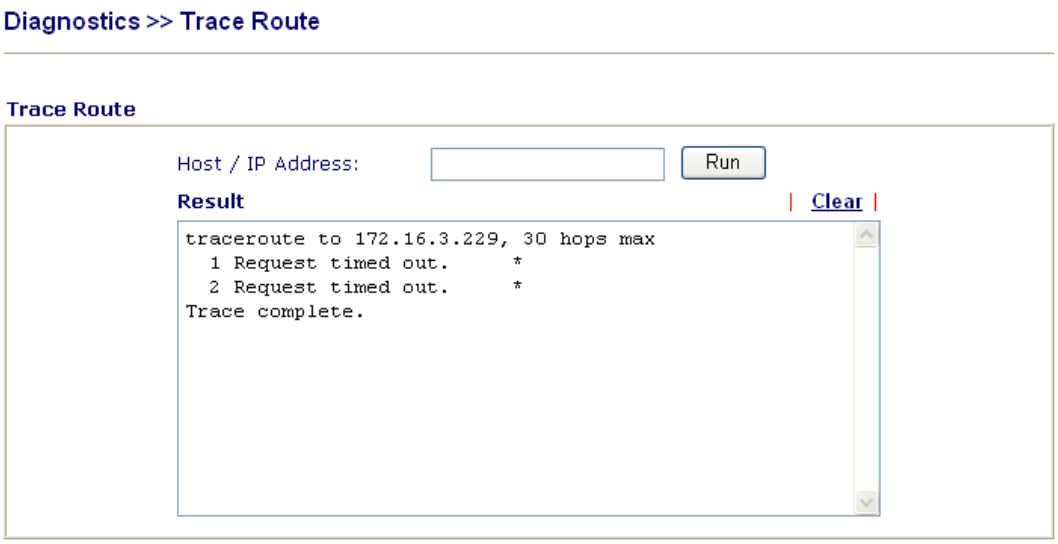
3.12.10 Ping Diagnosis

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 would like 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.

3.12.11 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.

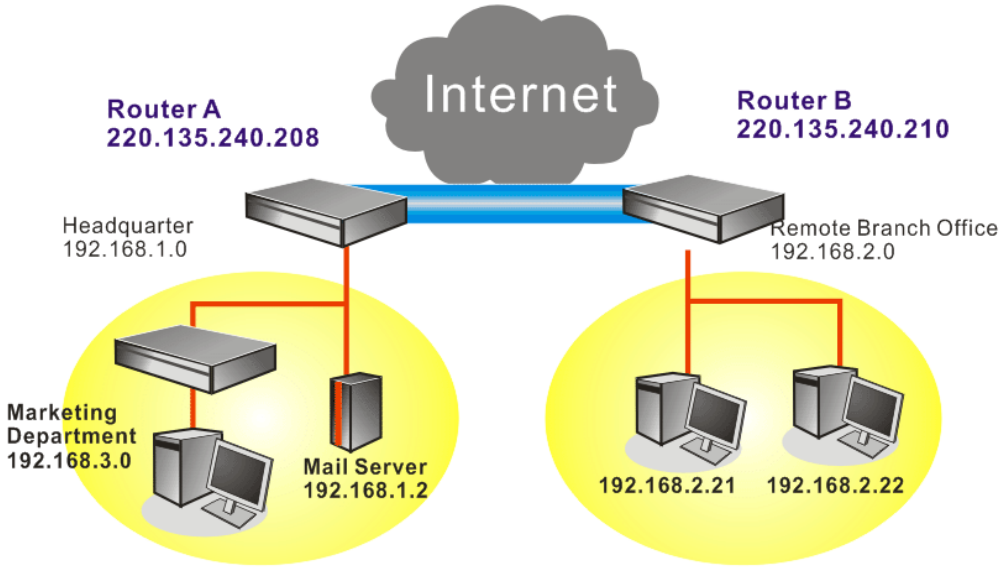


Ping through	Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the router automatically.
Host/IP Address	It indicates the IP address of the host.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

4 Application and Examples

4.1 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.

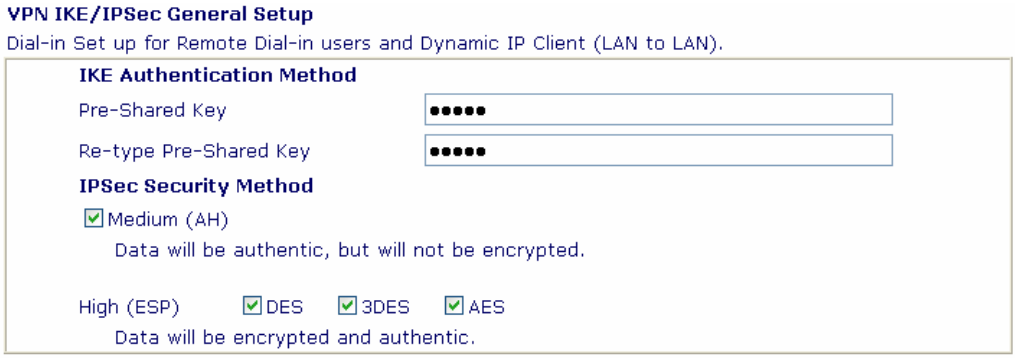


Settings in Router A in headquarter:

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

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

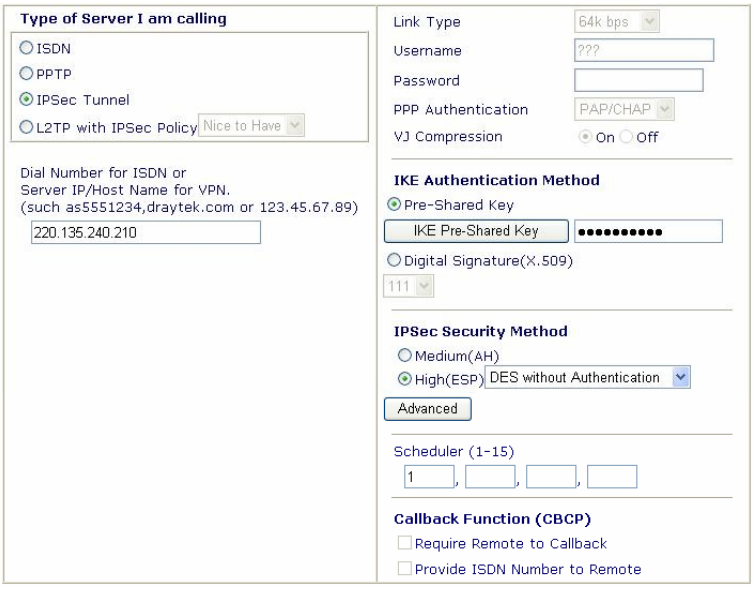
   For using **IPSec**-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.



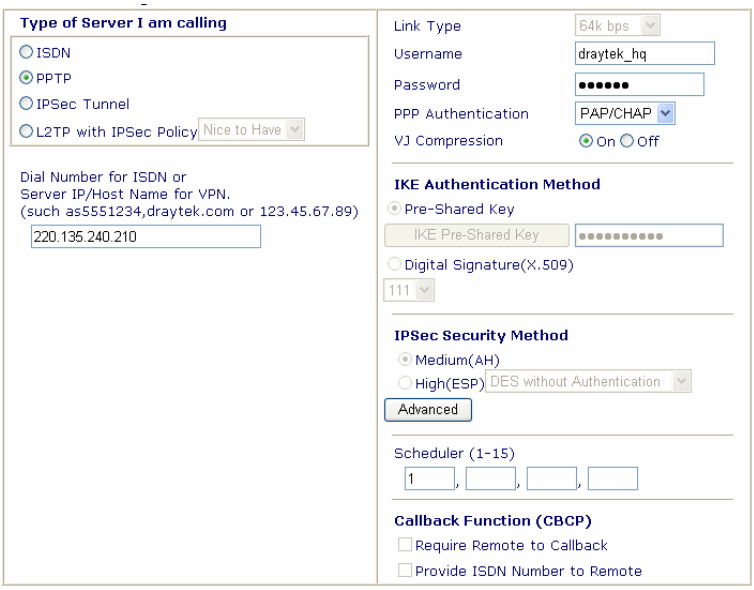
3. Go to **LAN-to-LAN**. Click on one index number to edit a profile.

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.

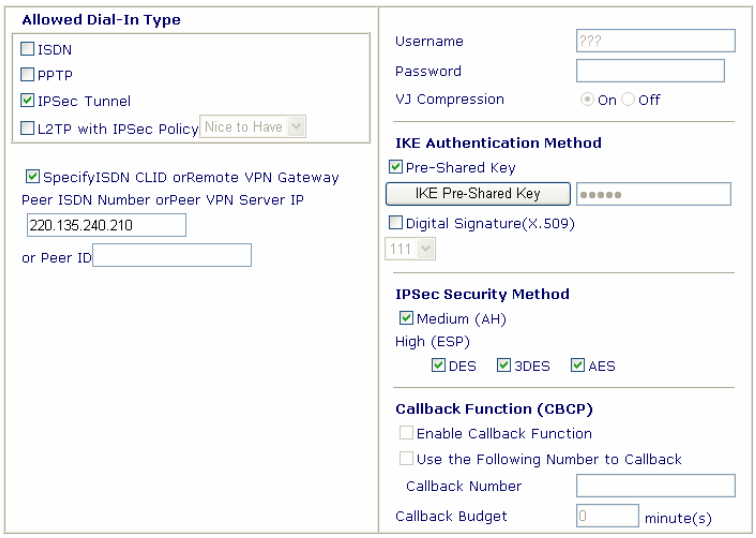


If a PPP-based service is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

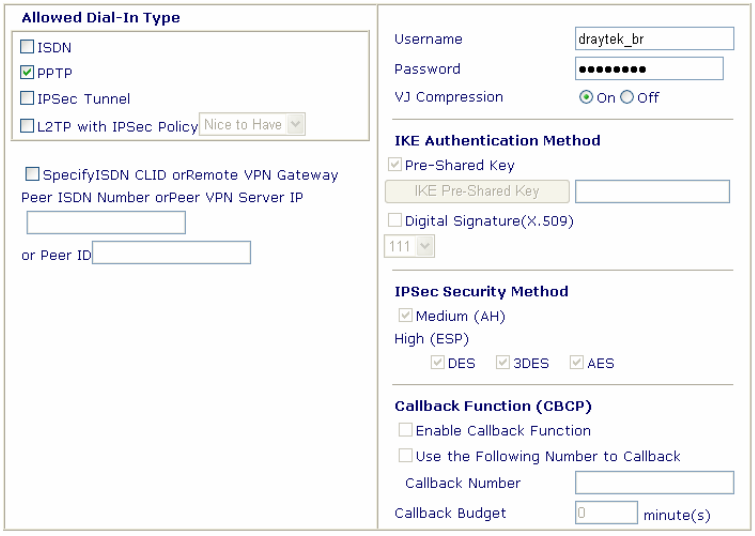


6. Set Dial-In settings to as shown below to allow Router B dial-in to build VPN connection.

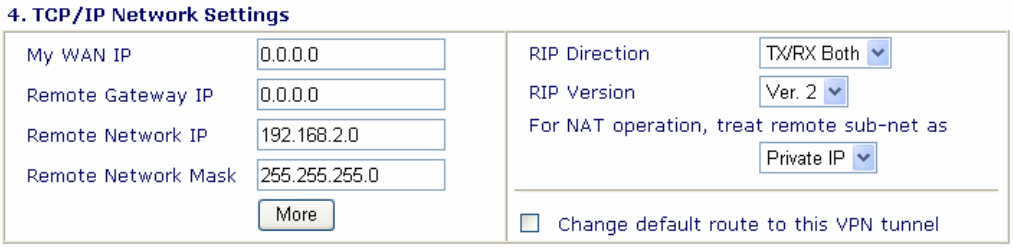
   If an IPSec-based service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.



   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.



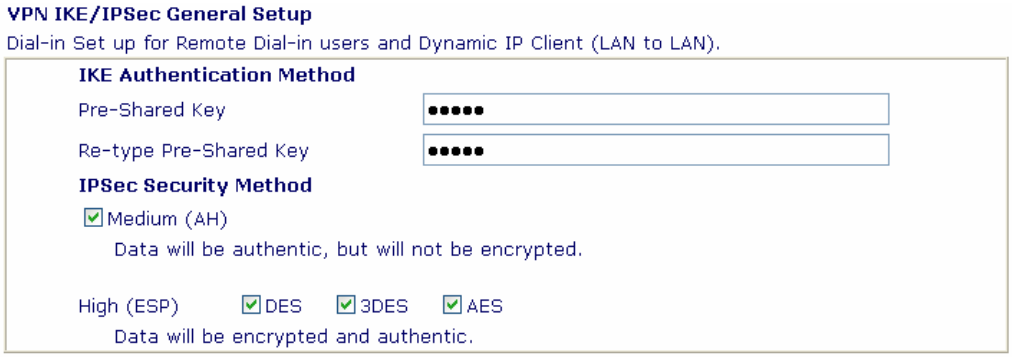
7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router A can direct the packets destined to the remote network to Router B via the VPN connection.



Settings in Router B in the remote office:

1. Go to **Remote Access Control** to enable the necessary VPN service.
2. Then, for using PPP based services, such as PPTP, L2TP, or ISDN, 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.

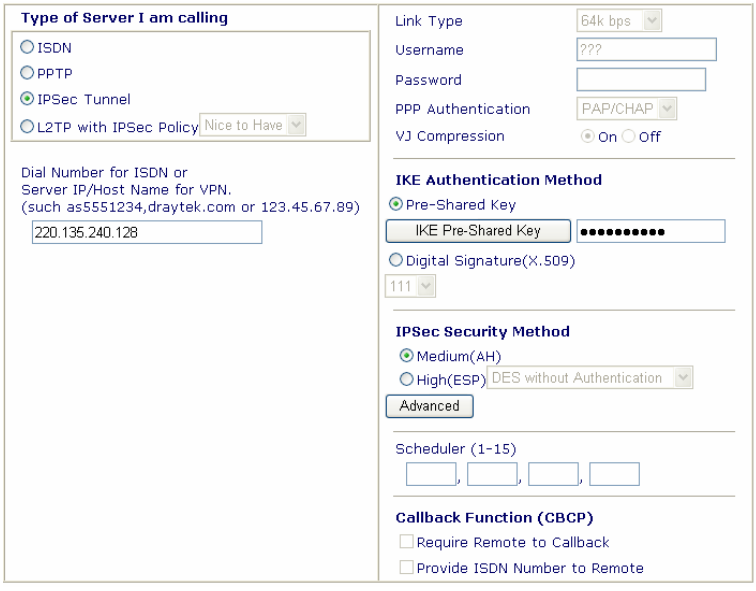


3. Go to **LAN-to-LAN**. Click on one index number to edit a profile.

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.

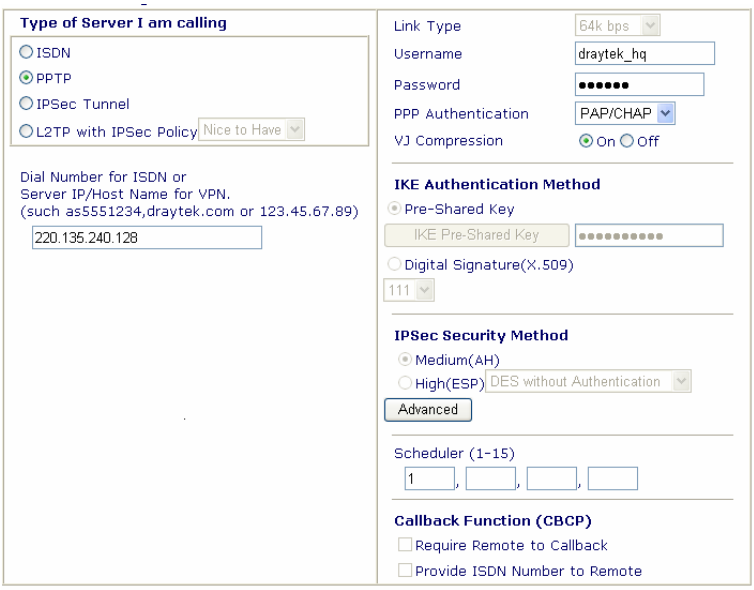
5. Set Dial-Out Settings as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

   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.



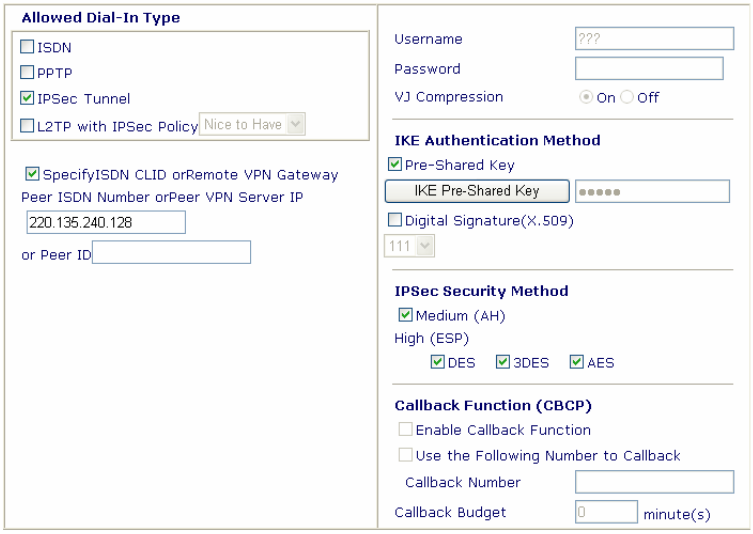
   If a PPP-based service is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out

connection.

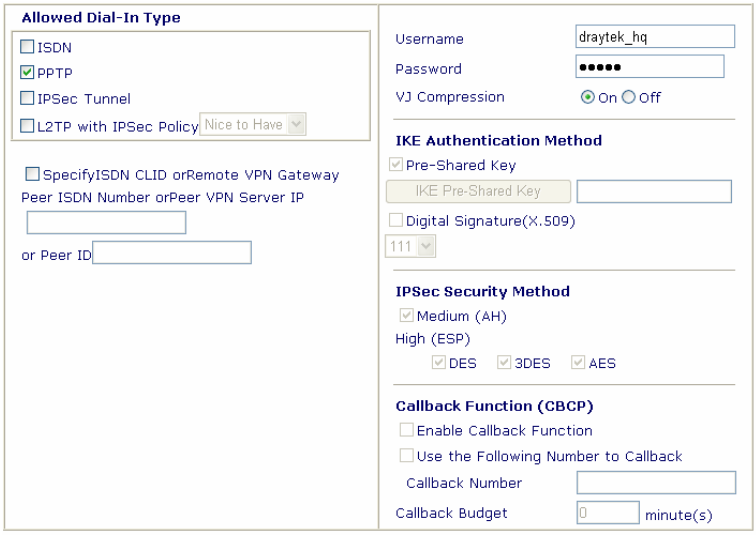


6. Set Dial-In settings to as shown below to allow Router A dial-in to build VPN connection.

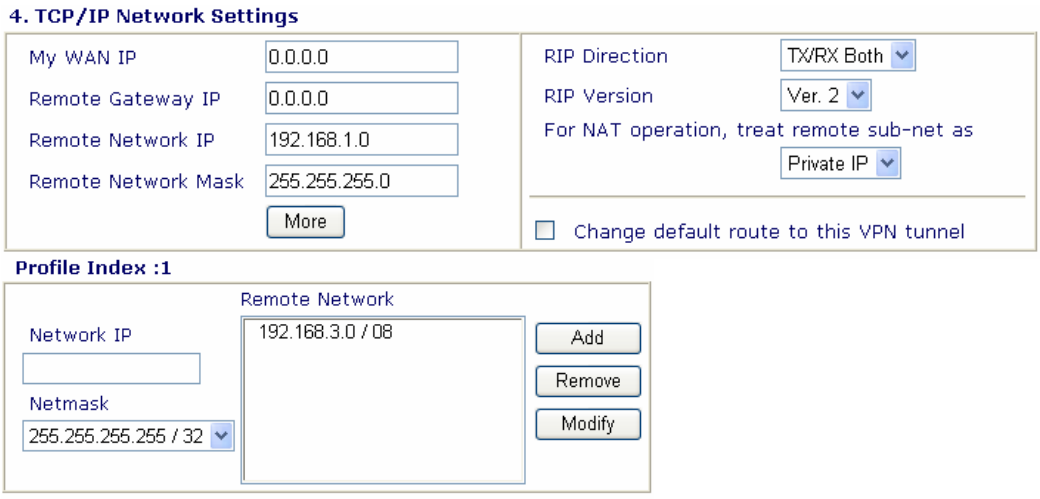
   If an IPSec-based service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.



   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.

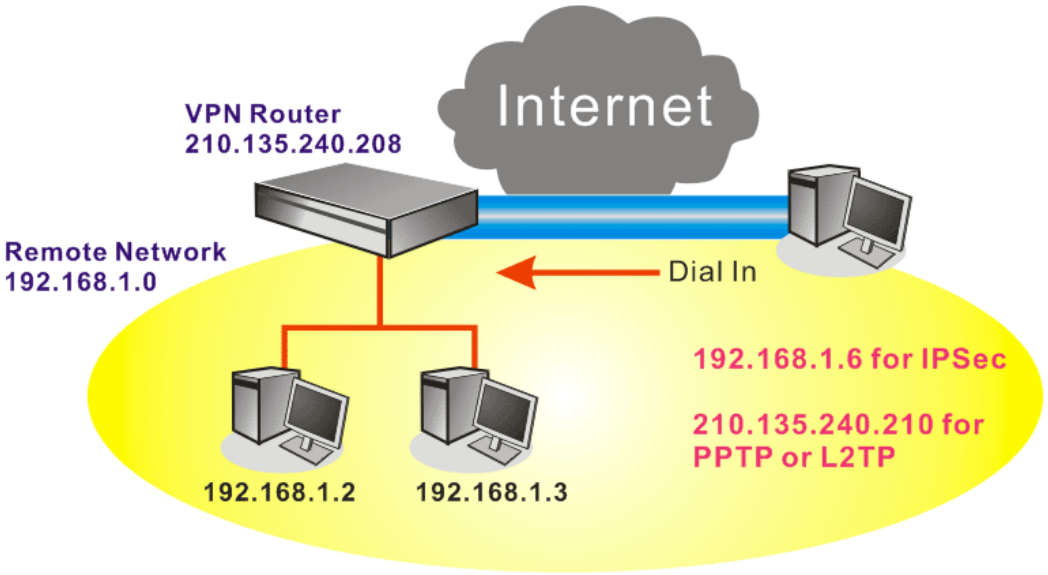


7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router B can direct the packets destined to the remote network to Router A via the VPN connection.



4.2 Create a remote dial-in user connection between the teleworker and headquarter

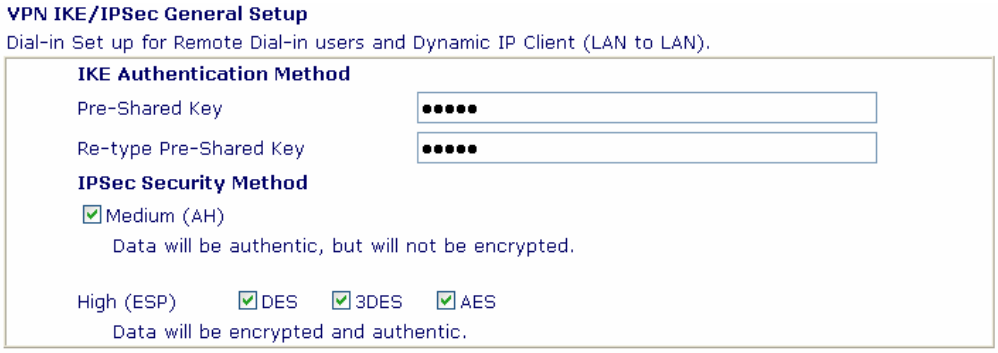
The other common case is that you, as a teleworker, may want to connect to the enterprise network securely. According to the network structure as shown in the below illustration, you may follow the steps to create a Remote User Profile and install Smart VPN Client on the remote host.



Settings in VPN Router in the enterprise office:

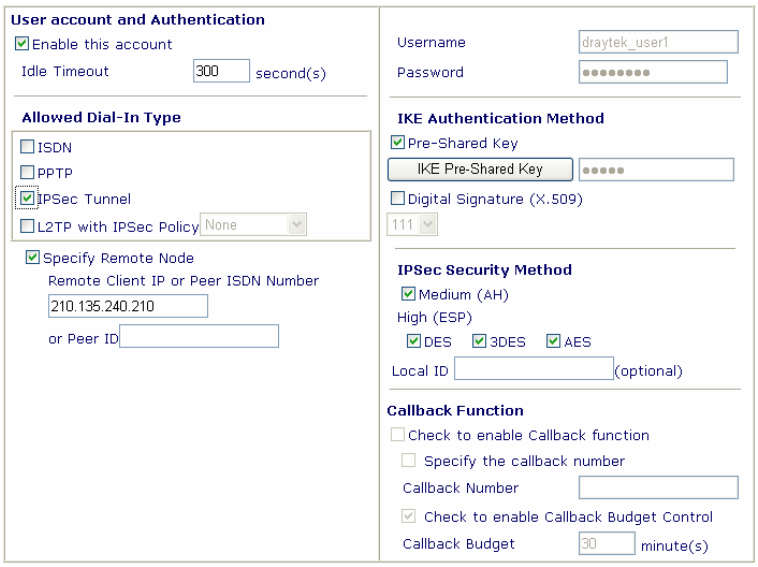
1. Go to **Remote Access Control** to enable the necessary VPN service.
2. Then, for using PPP based services, such as PPTP, L2TP, or ISDN, you have to set general settings in **PPP General Setup**.

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.

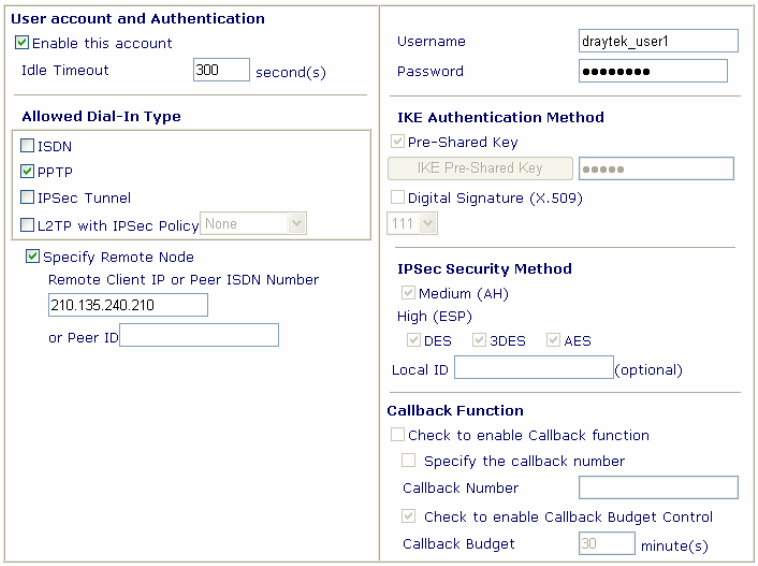


3. Go to **Remote Dial-In Users**. Click on one index number to edit a profile.
4. Set Dial-In settings to as shown below to allow the remote user dial-in to build VPN connection.

   If an IPSec-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.



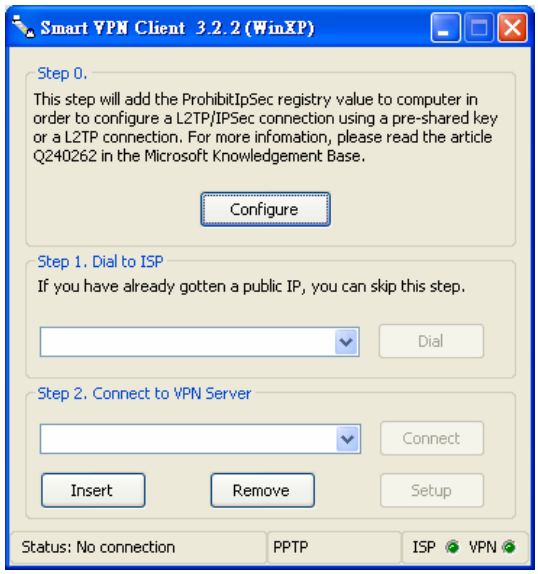
If a PPP-based service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.



Settings in the remote host:

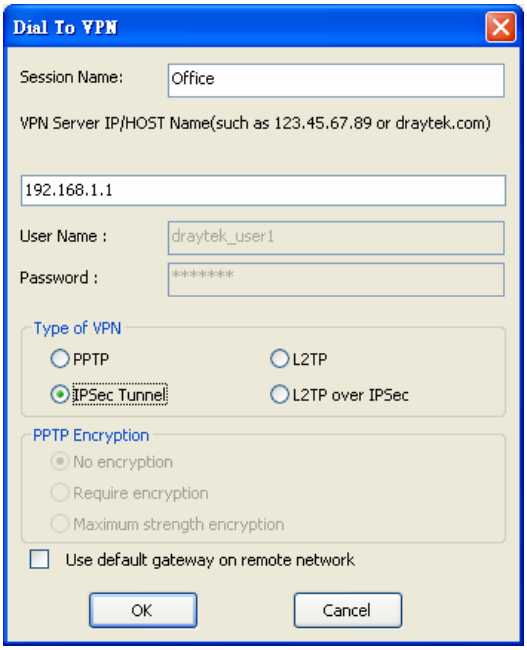
1. For Win98/ME, you may use "Dial-up Networking" to create the PPTP tunnel to Vigor router. For Win2000/XP, please use "Network and Dial-up connections" or “Smart VPN Client”, complimentary software to help you create PPTP, L2TP, and L2TP over IPSec tunnel. You can find it in CD-ROM in the package or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

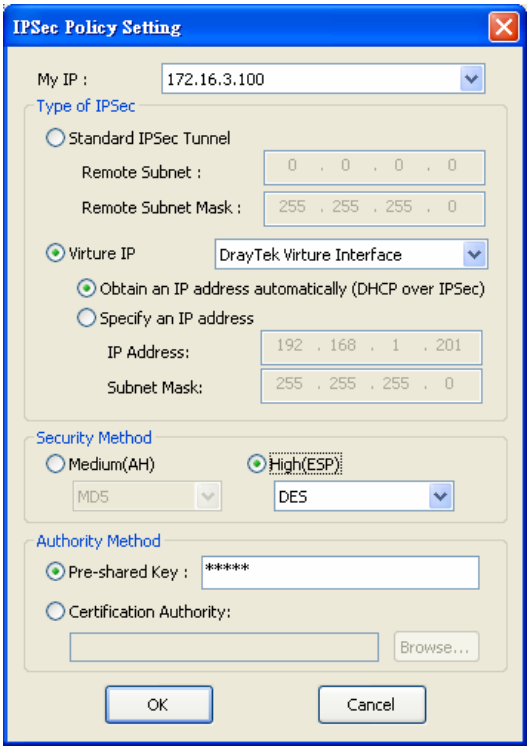


3. In **Step 2. Connect to VPN Server**, click **Insert** button to add a new entry.

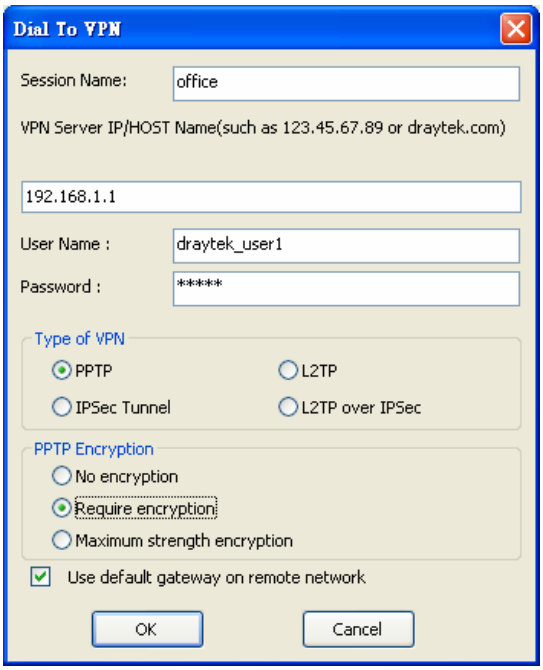
   If an IPSec-based service is selected as shown below,



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.

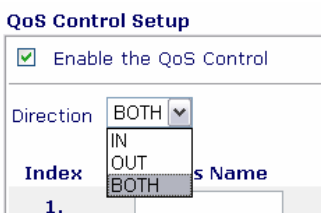


4. Click **Connect** button to build connection. When the connection is successful, you will find a green light on the right down corner.

4.3 QoS Setting Example

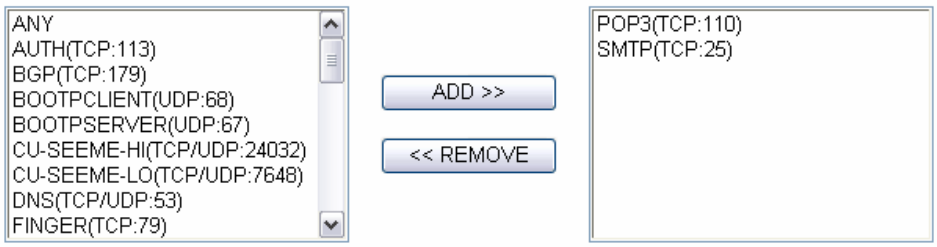
Assume a teleworker sometimes works at home and takes care of children. When working time, he would use Vigor router at home to connect to the server in the headquater office downtown via either HTTPS or VPN to check email and access internal database. Meanwhile, children may chat on VoIP or Skype in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

1. Make sure the QoS Control on the left corner is checked. And select BOTH in **Direction**.



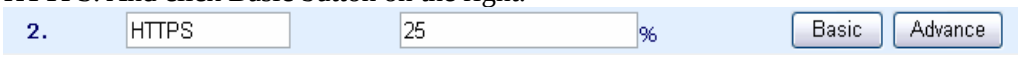
2. Enter the Class Name of Index 1. In this index, she will set reserve bandwidth for Email using protocol POP3 and SMTP. Click Basic button on the right.

3. Select POP3 and SMTP on the left column and add to right column. Click OK to exit.

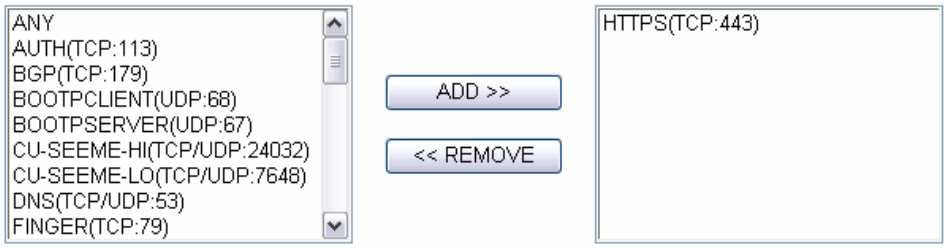


4. Enter the Class Name of Index 2. In this index, she will set reserve bandwidth for

HTTPS. And click Basic button on the right.

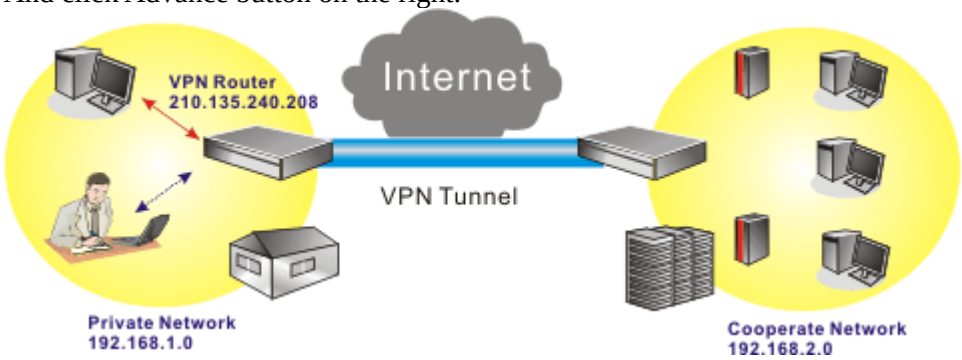


5. Select HTTPS in the list on the left column and click on ADD to add to right column. Click OK to exit.

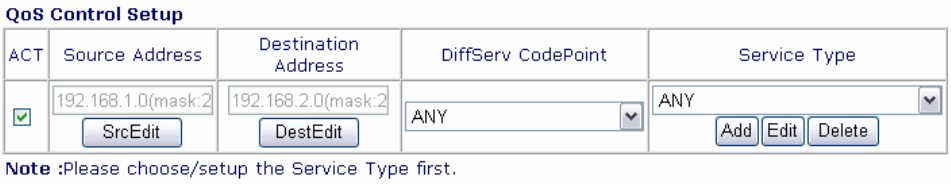


6. Check the Enable UDP Bandwidth Control on the bottom to prevent enormous UDP traffic of VoIP influent other application.

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

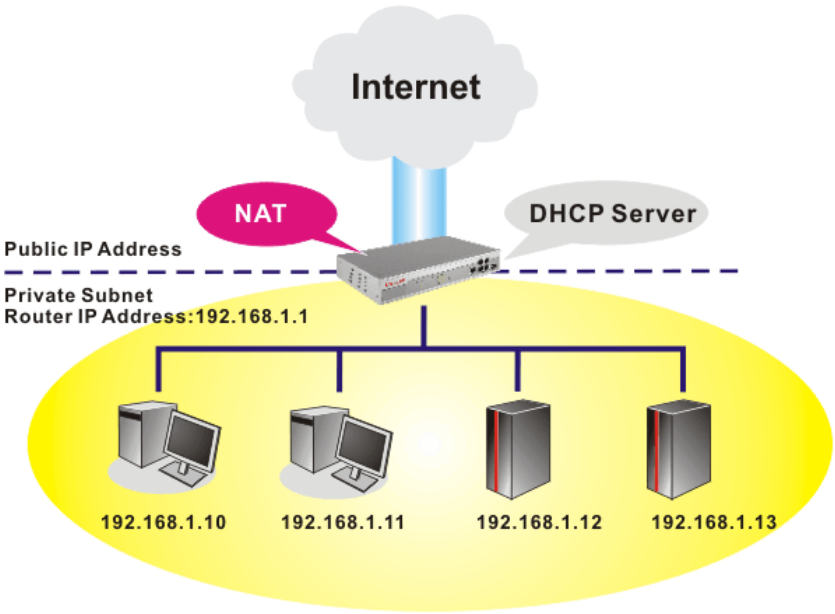


8. Click edit to open a new window. First, check the ACT box. Then click SrcEdit to set a Jane's subnet address. Click DestEdit to set headquarter's subnet address. Leave other fields and click OK.

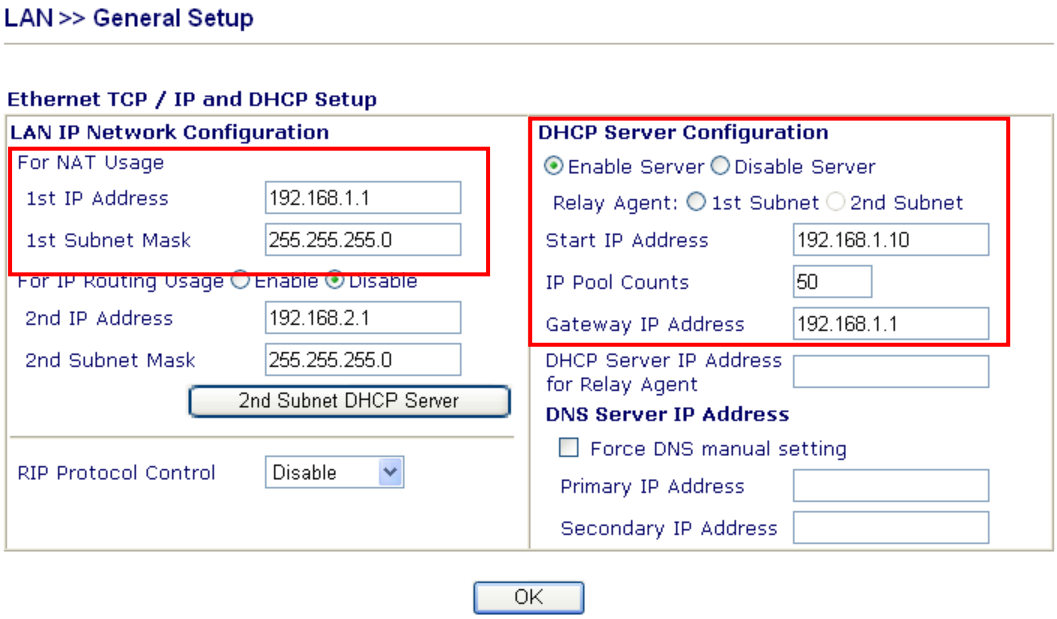


4.4 LAN – Created by Using NAT

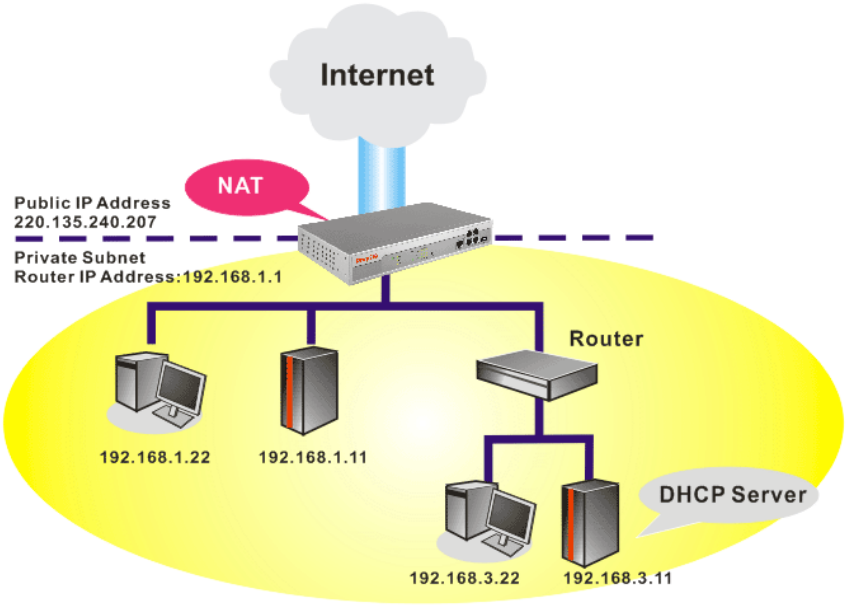
An example of default setting and the corresponding deployment are shown below. The default Vigor router private IP address/Subnet Mask is 192.168.1.1/255.255.255.0. The built-in DHCP server is enabled so it assigns every local NATed host an IP address of 192.168.1.x starting from 192.168.1.10.



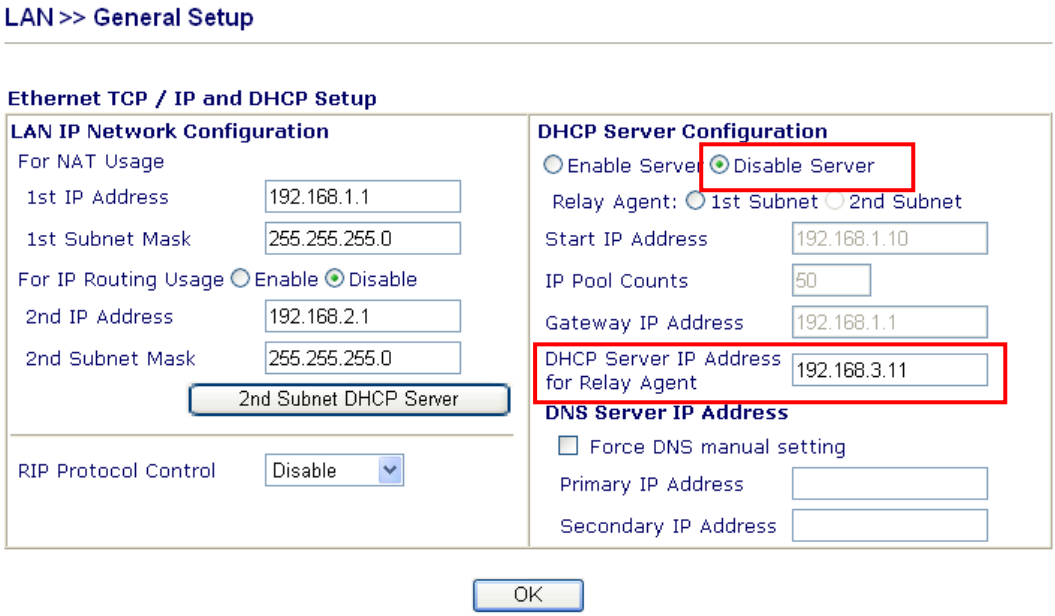
You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.



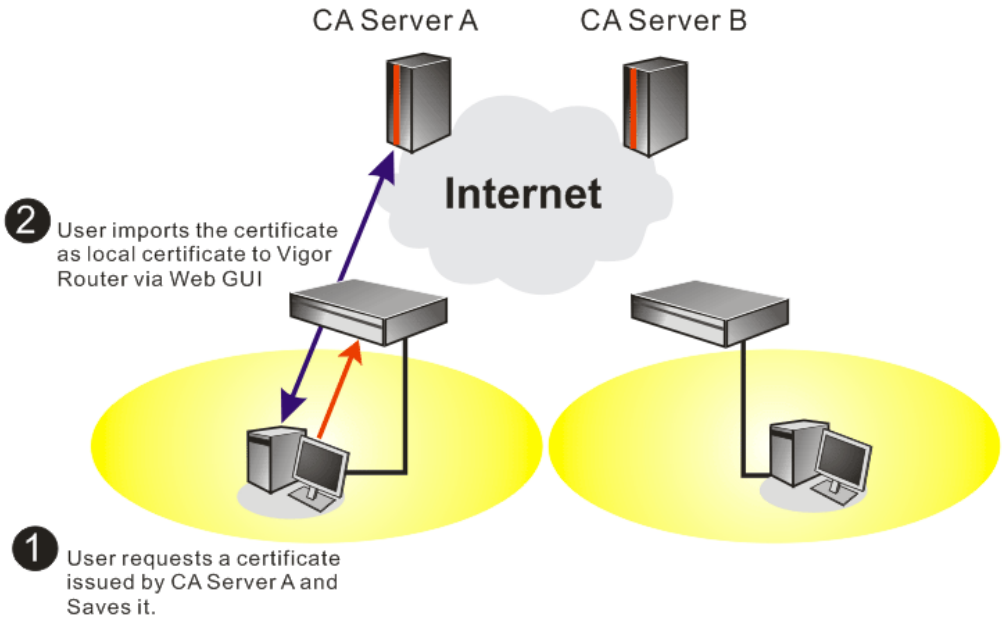
To use another DHCP server in the network rather than the built-in one of Vigor Router, you have to change the settings as show below.



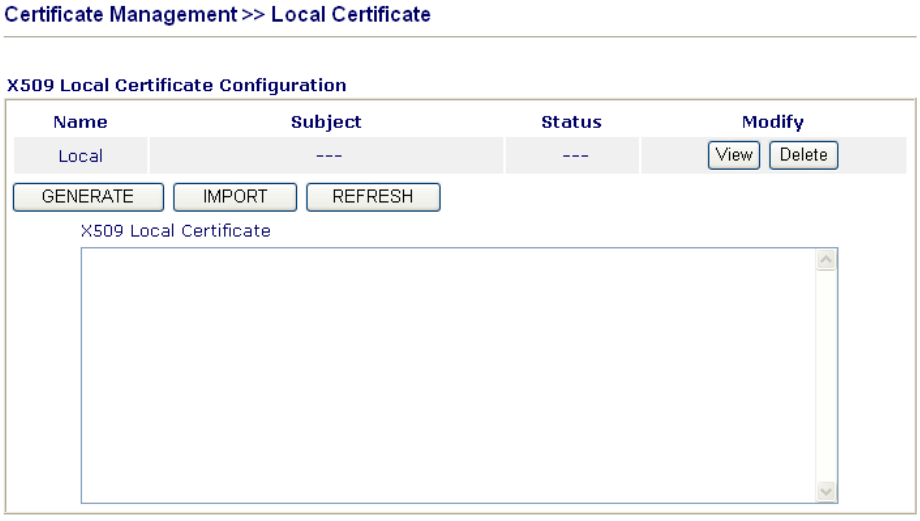
You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.



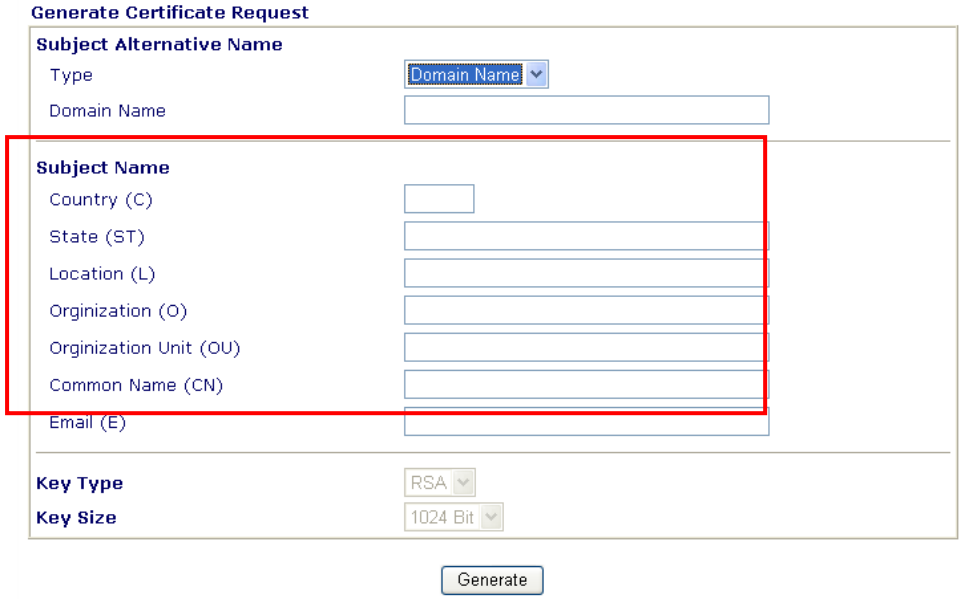
4.5 Request a certificate from a CA server on Windows CA Server



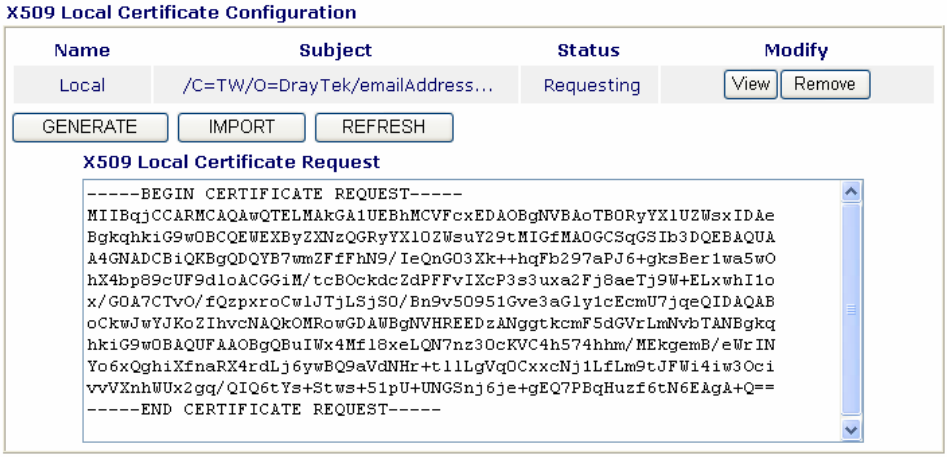
1. Go to **Certificate Management** and choose **Local Certificate**.



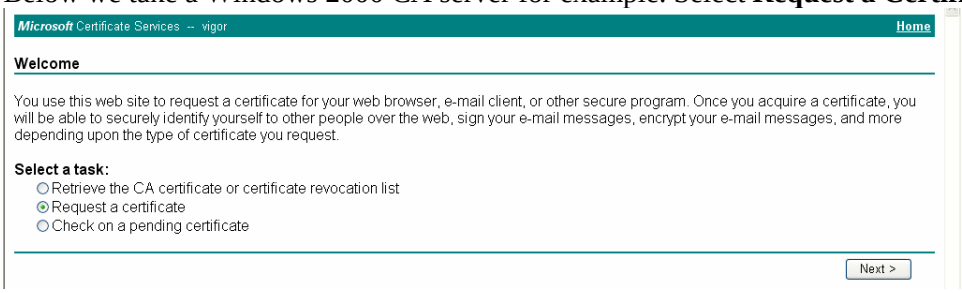
2. You can click **GENERATE** button to start to edit a certificate request. Enter the information in the certificate request.



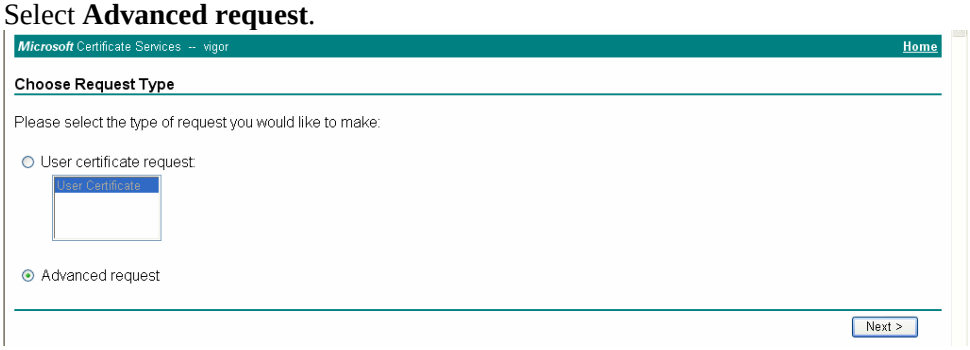
3. Copy and save the X509 Local Certificate Requet as a text file and save it for later use.



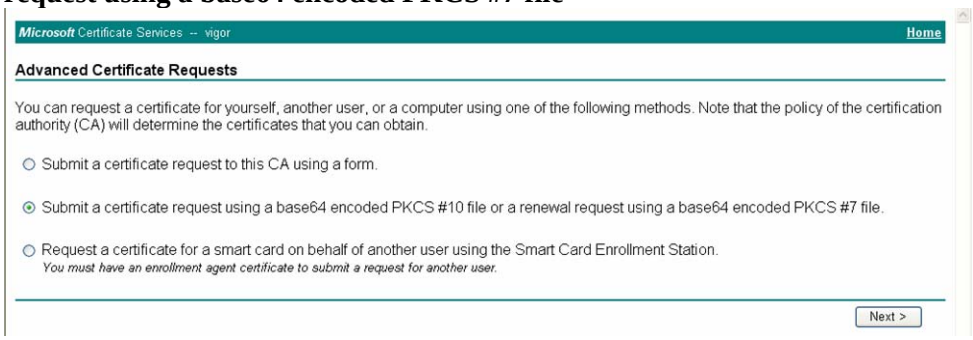
4. Connect to CA server via web browser. Follow the instruction to submit the request. Below we take a Windows 2000 CA server for example. Select **Request a Certificate**.



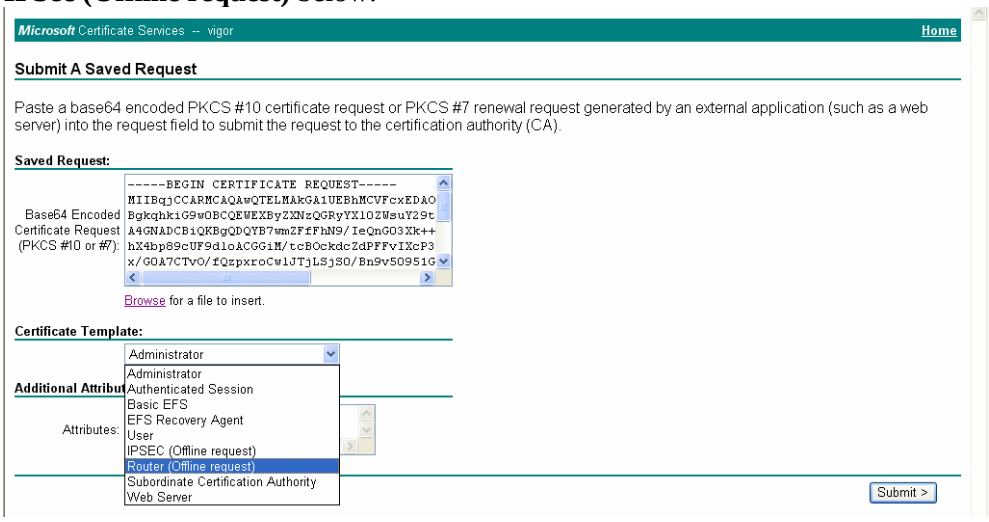
Select **Advanced request**.



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



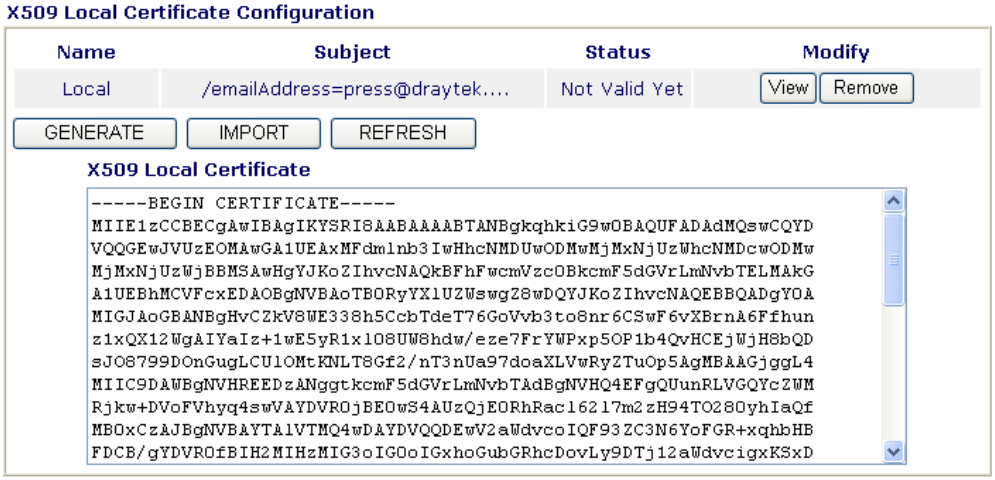
Import the X509 Local Certificate Request text file. Select **Router (Offline request)** or **IPSec (Offline request)** below.



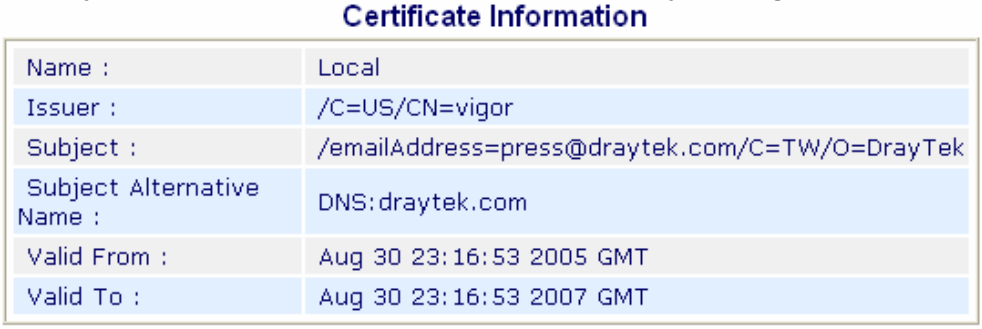
Then you have done the request and the server now issues you a certificate. Select **Base 64 encoded** certificate and **Download CA certificate**. Now you should get a certificate (.cer file) and save it.

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

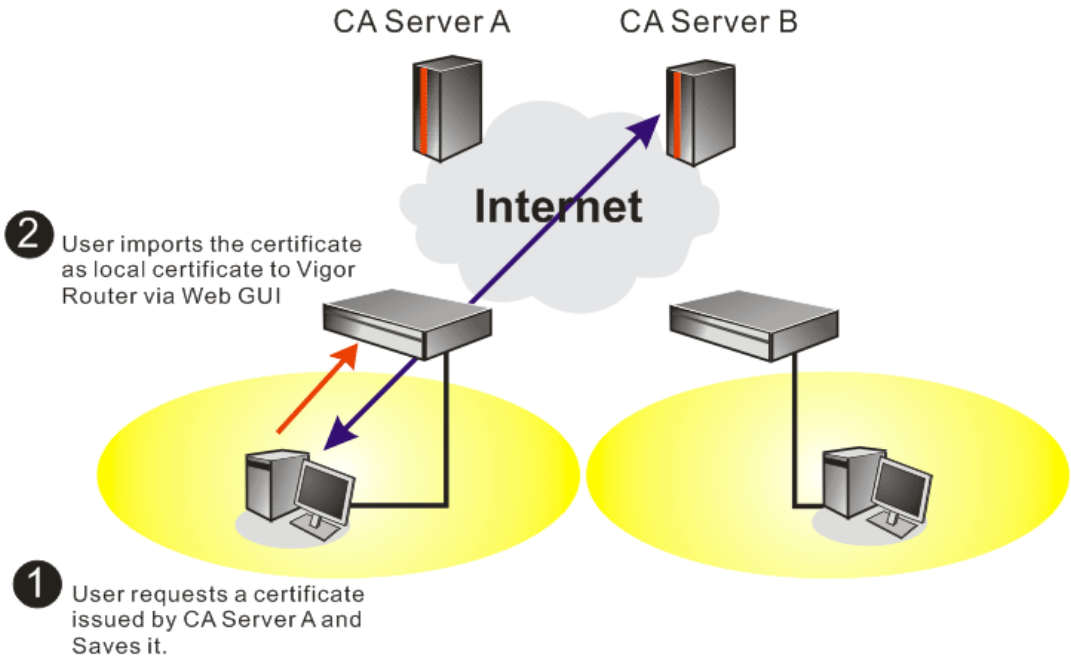
you will find the below window showing "------BEGINE CERTIFICATE------....."



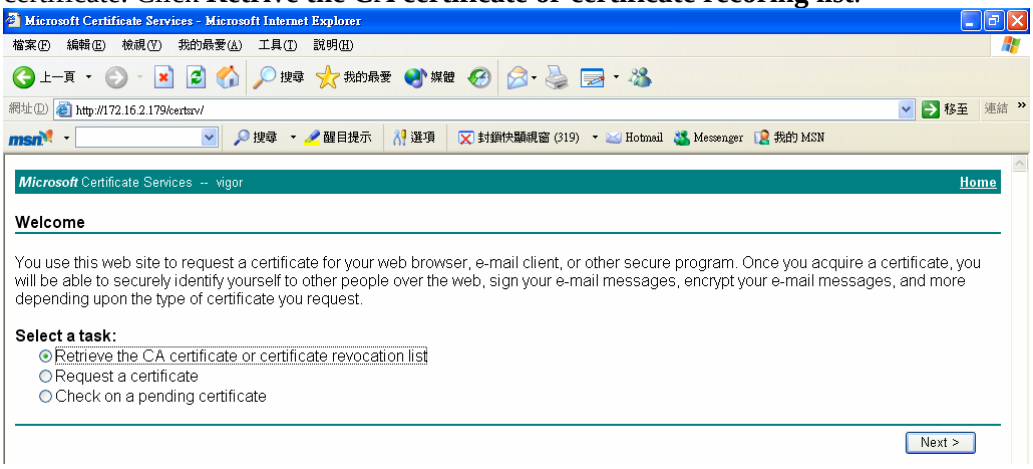
6. You may review the detail information of the certificate by clicking **View** button.



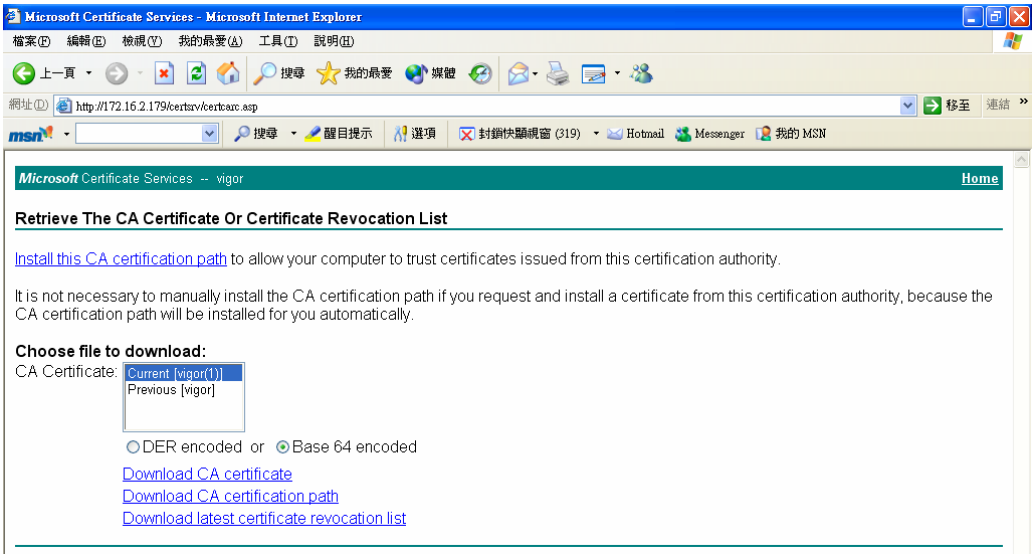
4.6 Request a CA Certificate and Set as Trusted on Windows CA Server



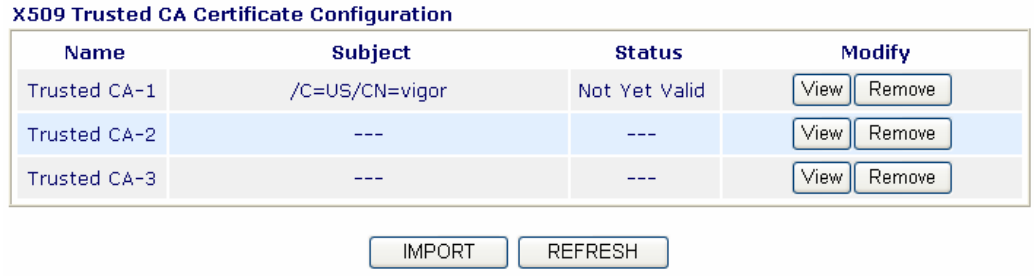
1. Use web browser connecting to the CA server that you would like to retrieve its CA certificate. Click **Retrive the CA certificate or certificate recoring list**.



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.

Certificate Detail Information

Certificate Name:	Trusted CA-1
Issuer:	/C=US/CN=vigor
Subject:	/C=US/CN=vigor
Subject Alternative Name:	
Valid From:	Aug 30 23:08:43 2005 GMT
Valid To:	Aug 30 23:17:47 2007 GMT

5 Trouble Shooting

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

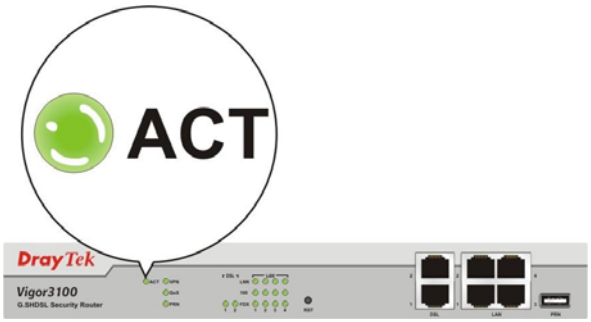
- Checking if the hardware status is OK or not.
- Checking if the Network Connection Settings on your computer is OK or not.
- Pinging the Router from your computer.
- Checking if the ISP Settings are OK or not.
- Backing to factory default setting if necessary.

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

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check the power line and WLAN/LAN cable connections.
   Refer to "**2.1 Hardware Installation"** on quick start guide 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 execute the hardware installation again. And then, try again.

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

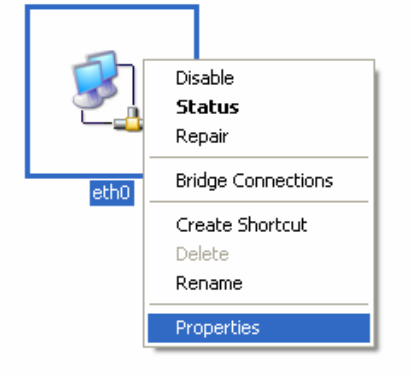
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

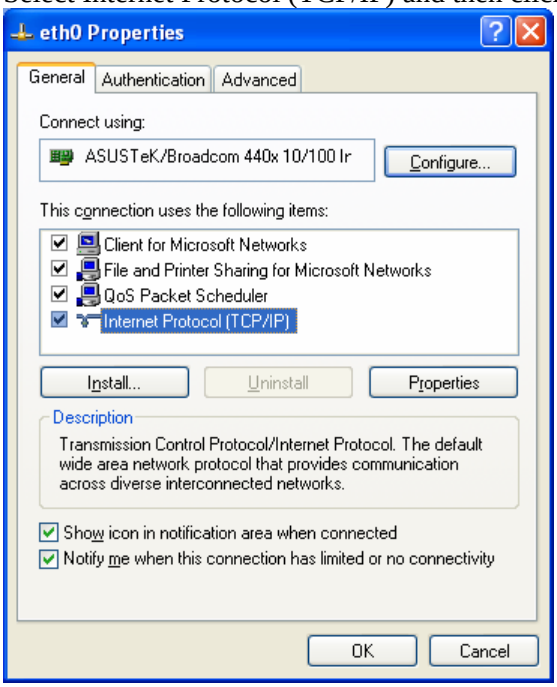
The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

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

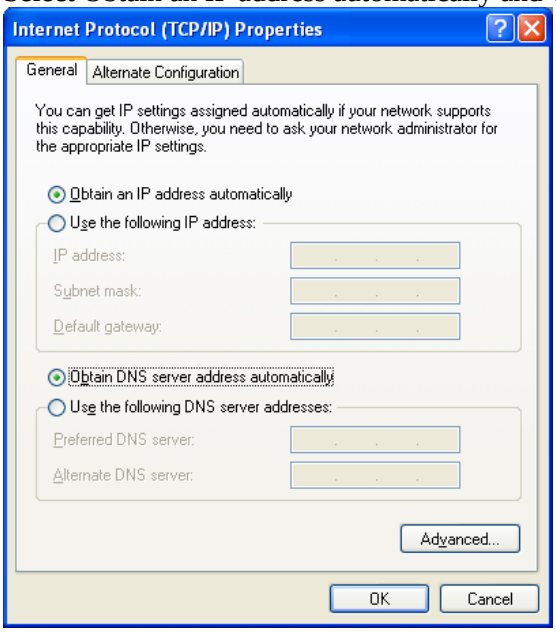
2. Right-click on Local Area Connection and click on Properties.



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

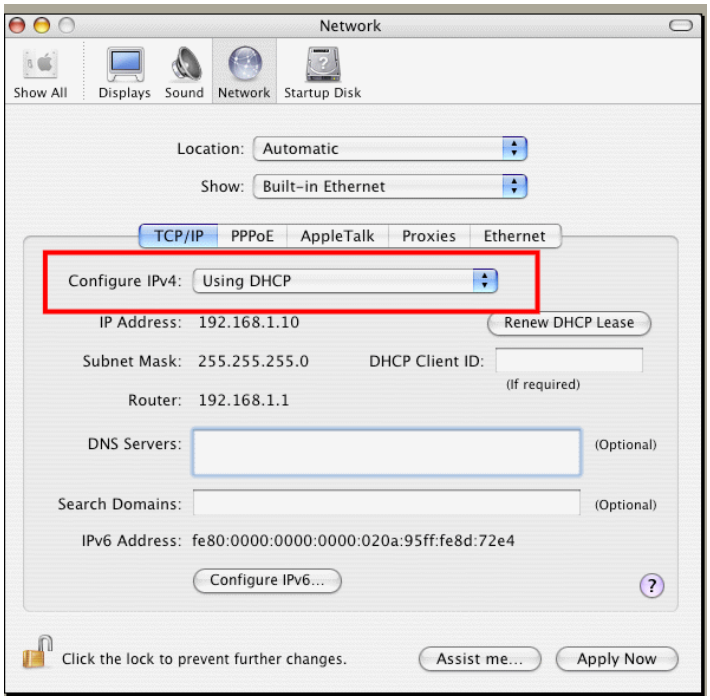


4. Select Obtain an IP address automatically and Obtain DNS server address automatically.



For MacOs

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



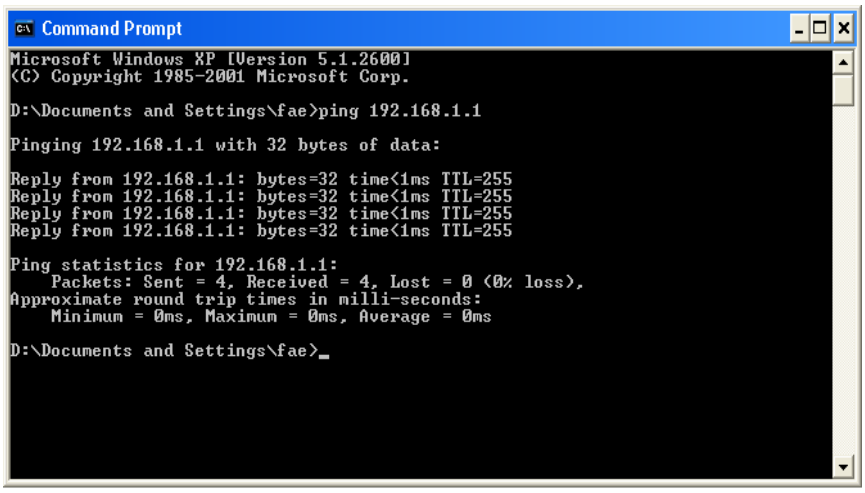
5.3 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use “ping” command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 4.2)

Please follow the steps below to ping the router correctly.

For Windows

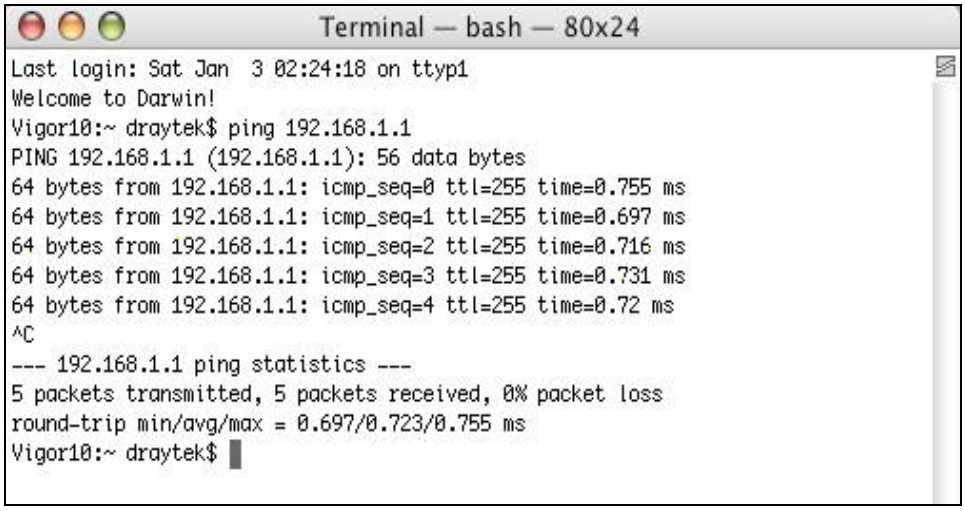
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP). The DOS command dialog will appear.



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.

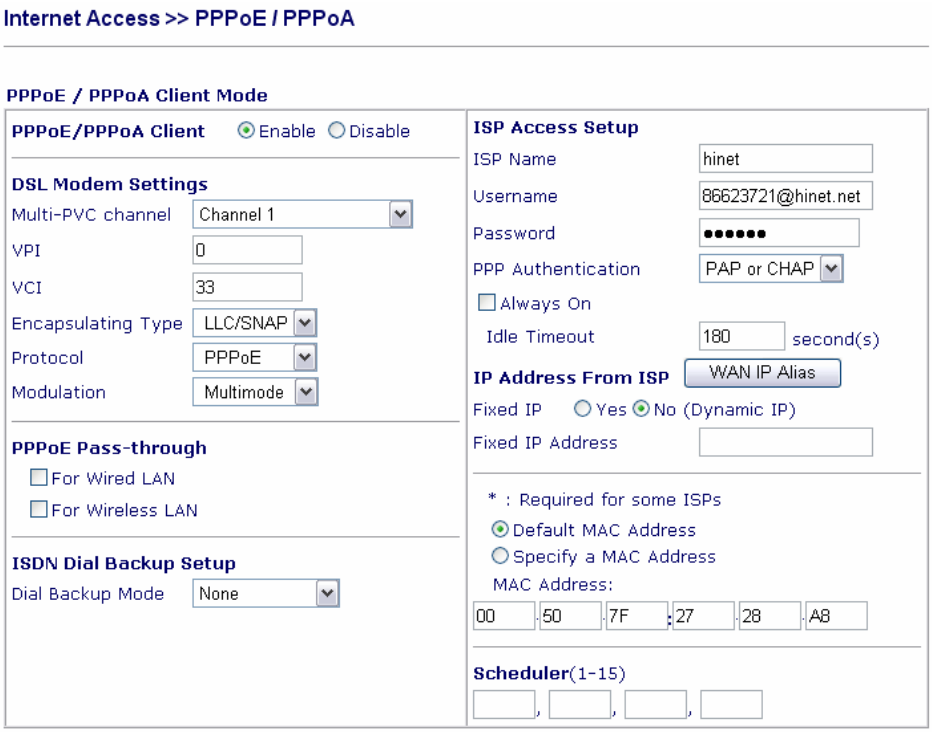


5.4 Checking If the ISP Settings are OK or Not

Click **Internet Access Setup** group and then check whether the ISP settings are set correctly.

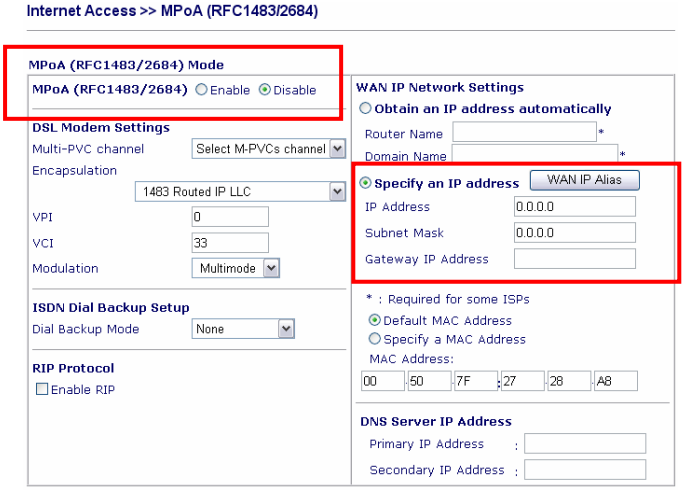
For PPPoE/PPPoA Users

1. Check if the **Enable** option is selected.
2. Check if all parameters of **DSL Modem Settings** are entered with correct values that you got from your ISP.
3. Check if **Username** and **Password** are entered with correct values that you **got from** your **ISP**.



For MPoA (RFC1483/2684) Users

1. Check if the **Enable** option is selected.
2. Check if all parameters of **DSL Modem Settings** are entered with correct values that you got from your **ISP**.
3. Check if **IP Address, Subnet Mask** and **Gateway** are set correctly, or use DHCP server to obtain IP automatically by clicking **Obtain an IP address automatically**.



5.5 Backing to Factory Default Setting If Necessary

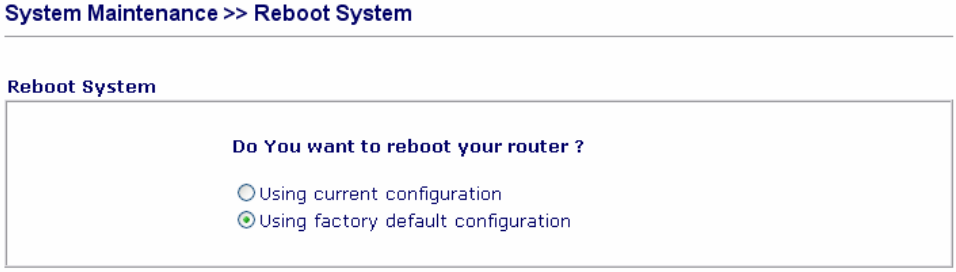
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

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

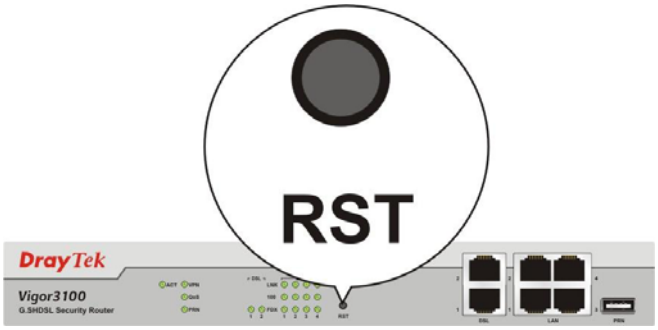
You can reset router to factory default via Web page.

Go to **System Maintenance >> 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.

5.6 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.