DrayTek

Vigor130

VDSL2/ADSL2/2+ Modem

Your reliable networking solutions partner

User's Guide

V1.0

Vigor130 Series
VDSL2/ADSL2/2+ Modem
User's Guide

Version: 1.0

Firmware version: V3.7.1

(For future update, please visit DrayTek web site)

Date: 5/06/2013

Copyright Information

Copyright Declarations

Trademarks

The following trademarks are used in this document:

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

Safety Instructions and Approval

Safety Instructions

- Read the installation guide thoroughly before you set up the modem.
- The modem is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the modem yourself.
- Do not place the modem in a damp or humid place, e.g. a bathroom.
- The modem should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
- Do not expose the modem 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 modem, please follow local regulations on conservation of the environment.

Warranty

We warrant to the original end user (purchaser) that the modem will be free from any defects in workmanship or materials for a period of one (1) year 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 modem via http://www.draytek.com.

Firmware & Tools Updates

Due to the continuous evolution of DrayTek technology, all modems 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 Township, HsinChu Industrial Park, Hsin-Chu, Taiwan 303
Product: Vigor130

DrayTek Corp. declares that Vigor130 is in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

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

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

Federal Communication Commission Interference Statement

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

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

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

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

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

This product is designed for the DSL network throughout the EC region and Switzerland.

Table of Contents

Introduction 1

1.1 Web Configuration Buttons Explanation 1

1.2 LED Indicators and Connectors 2

1.3 Hardware Installation 4

Basic Configuration 5

2.1 Accessing Web Page 5

2.2 Changing Password 6

2.3 Quick Start Wizard 7

2.3.1 Setting PPPoE/PPPoA Connection 7
2.3.2 Setting MPoA/Static or Dynamic Connection 10

2.4 Introducing Dashboard 13

2.4.1 Virtual Panel 13
2.4.2 Name with a Link 14
2.4.3 Quick Access for Common Used Menu 14
2.4.4 GUI Map 15
2.4.5 Web Console 15
2.4.6 Config Backup 16

2.5 Online Status 17

2.5.1 Physical Connection 17
2.5.2 Virtual WAN 19

2.6 Saving Configuration 20

2.7 Registering Vigor Router 20

Advanced Configuration 23

3.1 Internet Access 23

3.1.1 Basics of Internet Protocol (IP) Network 23
3.1.2 General Setup 24
3.1.3 PPPoE/PPPoA 26
3.1.4 MPoA /Static or dynamic IP 28
3.1.5 IPv6 31
3.1.6 Multi-PVCs 36
3.1.7 Multi-VLAN 40

3.2 LAN 42

3.2.1 Basics of LAN 42
3.2.2 General Setup 44
3.2.3 Static Route 49

3.2.4 Bind IP to MAC 53
3.3 NAT 55
3.3.1 Port Redirection 56
3.3.2 DMZ Host 59
3.3.3 Open Ports 62
3.4 Firewall 64
3.4.1 Basics for Firewall 64
3.4.2 General Setup 66
3.4.3 Filter Setup 70
3.4.4 DoS Defense 77
3.5 Objects Settings 81
3.5.1 IP Object 81
3.5.2 IP Group 83
3.5.3 IPv6 Object 85
3.5.4 IPv6 Group 87
3.5.5 Service Type Object 88
3.5.6 Service Type Group 90
3.5.7 Keyword Object 92
3.5.8 Keyword Group 94
3.5.9 File Extension Object 95
3.6 CSM Profile 96
3.6.1 URL Content Filter Profile 97
3.7 Applications 101
3.7.1 Dynamic DNS 101
3.7.2 Schedule 103
3.7.3 UPnP 106
3.7.4 IGMP 108
3.8 System Maintenance 109
3.8.1 System Status 109
3.8.2 TR-069 111
3.8.3 Administrator Password 112
3.8.4 Configuration Backup 113
3.8.5 Syslog/Mail Alert 115
3.8.6 Time and Date 117
3.8.7 Management 118
3.8.8 Reboot System 120
3.8.9 Firmware Upgrade 121
3.9 Diagnostics 122
3.9.1 Dial-out Triggering 122
3.9.2 Routing Table 123
3.9.3 ARP Cache Table 124
3.9.4 IPv6 Neighbour Table 124
3.9.5 DHCP Table 125
3.9.6 NAT Sessions Table 126
3.9.7 Ping Diagnosis 127
3.9.8 Data Flow Monitor 128
3.9.9 Trace Route 130
3.9.10 TSPC Status 131

4 **Application and Examples 132**

4.1 LAN – Created by Using NAT 132

5 **Trouble Shooting 135**

5.1 Checking If the Hardware Status Is OK or Not 135

5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not 136

5.3 Pinging the Modem from Your Computer 138

5.4 Checking If the ISP Settings are OK or Not 139

5.5 Backing to Factory Default Setting If Necessary 139

5.6 Contacting Your Dealer 140

Introduction

Vigor130 Series is a VDSL2/ADSL2/2+ modem.

The object-based design used in SPI (Stateful Packet Inspection) firewall allows users to set firewall policy with ease. It is flexible and makes your network be safe. By the way, DoS/DDoS prevention and URL content filter strengthen the security outside and control inside.

1.1 Web Configuration Buttons Explanation

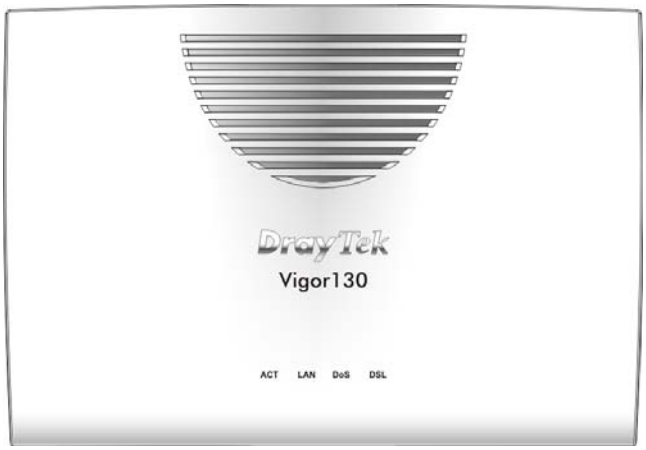
Several main buttons appeared on the web pages are defined as the following:

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

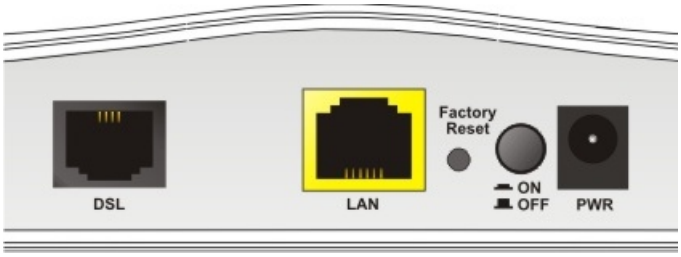
Note: For the other buttons shown on the web pages, please refer to Chapter 4 for detailed explanation.

1.2 LED Indicators and Connectors

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



LED	Status	Explanation
ACT	Off	The system is not ready or is failed.
	Blinking	The system is ready and can work normally.
LAN	On	A normal connection is through its corresponding port.
	Off	LAN is disconnected.
	Blinking	Data is transmitting (sending/receiving).
DoS	On	The DoS/DDoS function is active.
	Blinking	It will blink while detecting an attack.
DSL	On	DSL connection synchronized.
	Blinking	DSL connection is synchronizing.



Interface	Description
DSL	Connecter for accessing the Internet through VDSL2/ADSL2/2+.
LAN	Connecter for local networked devices.
Factory Reset	Restore the default settings. Usage: Turn on the modem. Press the button and keep for more than 10 seconds. Then the modem will restart with the factory default configuration.
	ON/OFF: Power switch.
	Connecter for a power adapter.

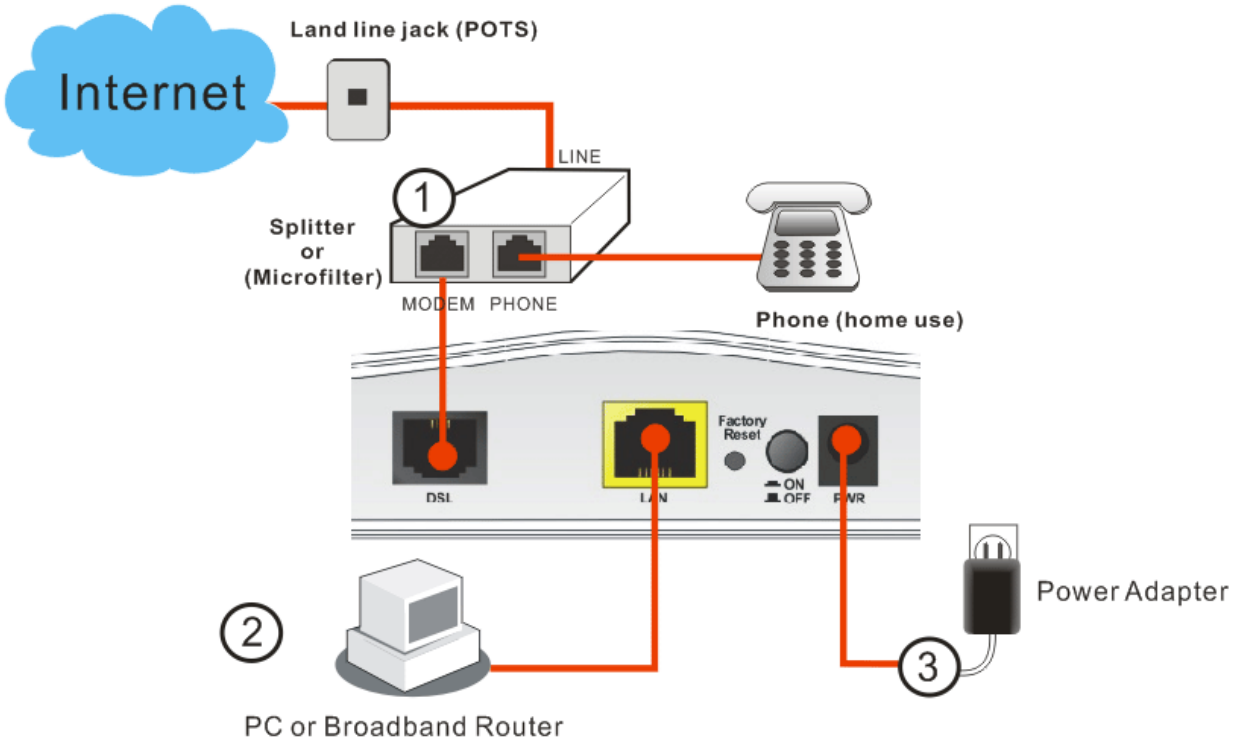
1.3 Hardware Installation

This section will guide you to install the modem through hardware connection and configure the modem's settings through web browser.

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

1. Connect the DSL interface to the MODEM port of external splitter with a DSL line cable.
2. Connect the LAN port to your computer with a RJ-45 cable.
3. Connect one end of the power adapter to the Power port of this device. Connect the other end to the wall outlet of electricity.
4. Power on the modem.
5. Check the **POWER, ACT, LAN, DSL** and **INTERNET** LEDs to assure network connections.

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



2 Basic Configuration

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

2.1 Accessing Web Page

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

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

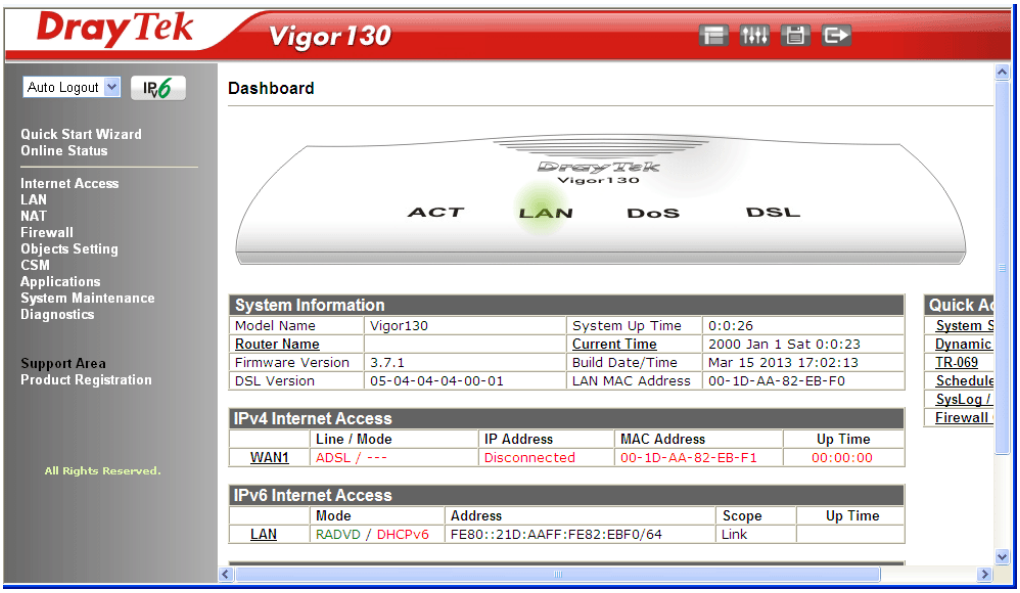
2. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for username and password. Please type “admin/admin” as the username and password. Then click **Login**.

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

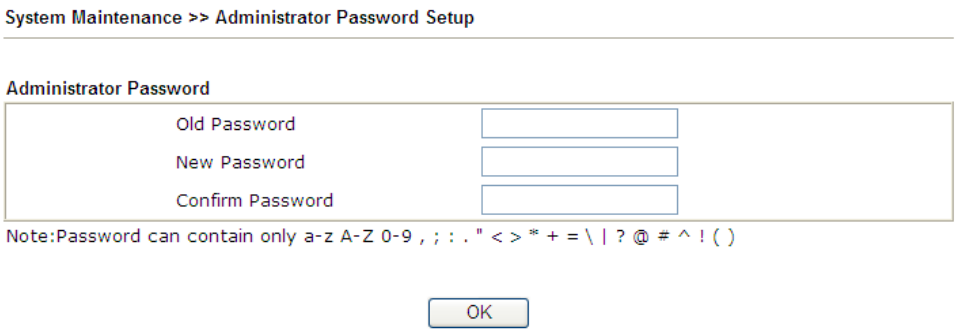
2.2 Changing Password

Please change the password for the original security of the modem.

1. Access into the web user interface of Vigor130. The **Main Screen** will appear as below.



2. Go to **System Maintenance** page and choose **Administrator Password/User Password**.



3. Enter the login password (the default is blank) on the field of **Old Password**. Type **New Password**. Then click **OK** to continue.

4. Now, the password has been changed. Next time, use the new password to access the Web User Interface for this modem.

2.3 Quick Start Wizard

Notice: Quick Start Wizard for user operation is the same as for administrator's operation.

The configuration provide here can help you to deploy and use the modem quickly.

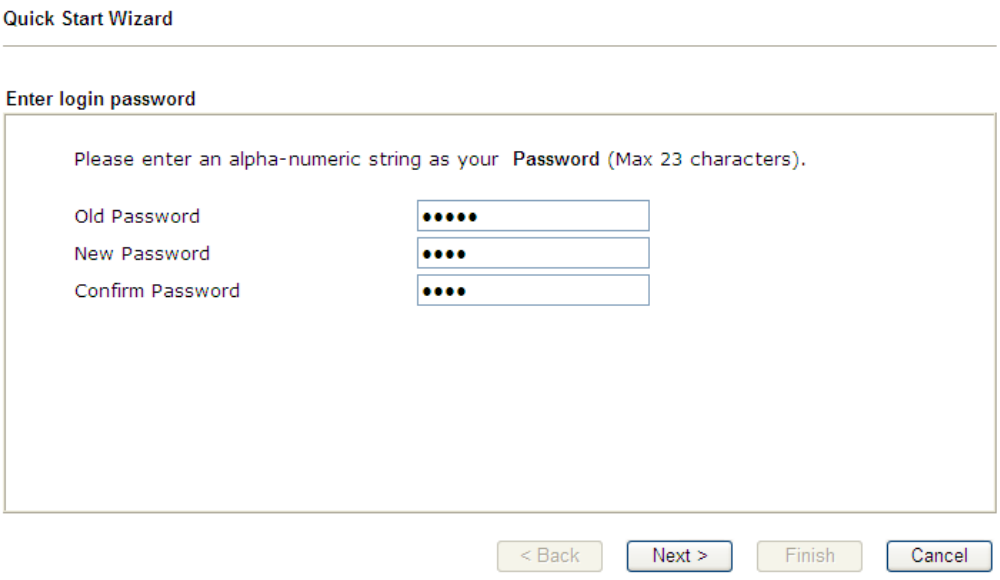
2.3.1 Setting PPPoE/PPPoA Connection

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

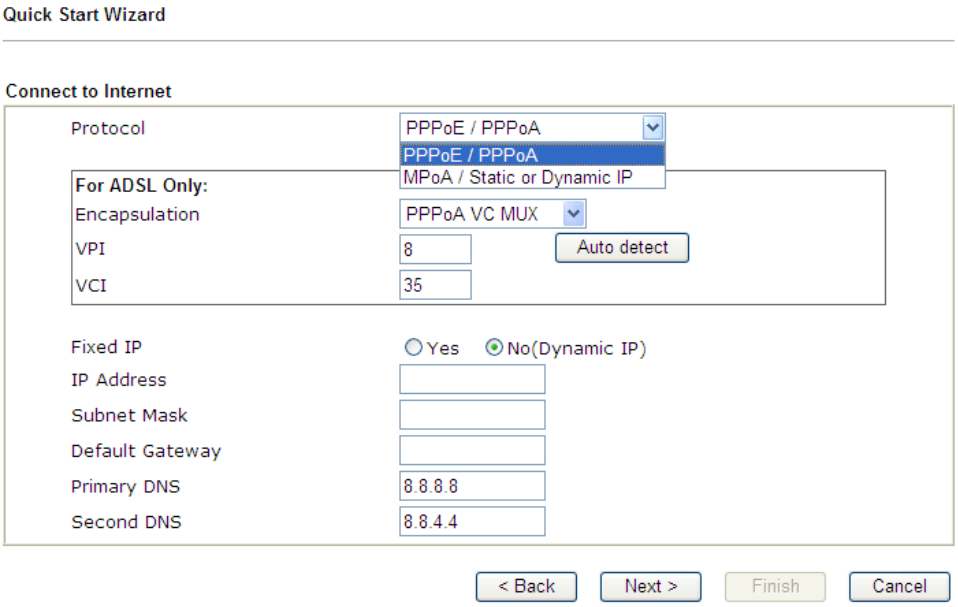
PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.

If your ISP provides you the **PPPoE** connection, please select **PPPoE** for this modem.

1. Click **Quick Start wizard**.
2. The first screen of **Quick Start Wizard** is entering login password of the web user interface. After typing the password, please click **Next**.



3. You can configure the modem to access the Internet with different protocol/modes such as **PPPoE/PPPoA** or **MPoA/Static or Dynamic IP**. The modem supports the ADSL WAN interface for Internet access. In this case, choose **PPPoE/PPPoA**.

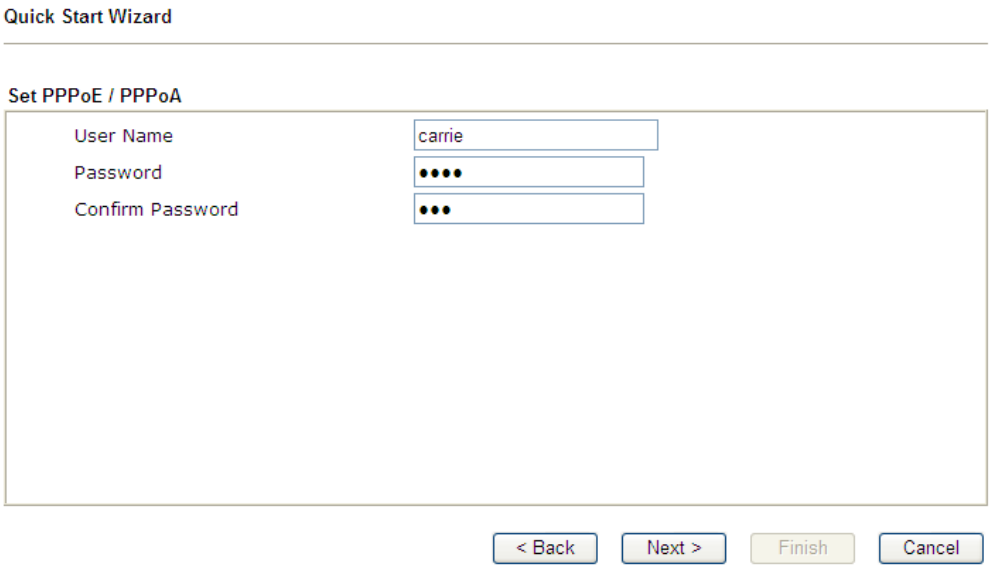


Available parameters are listed below:

Item	Description
For ADSL Only	You have to select an appropriate WAN connection type for connecting to the Internet through this modem according to the settings that your ISP provided. **Auto detect** – Click it to detect suitable values below by the modem automatically.
Encapsulation	Select an IP mode for this WAN interface. There are several available modes for Internet access such as **PPPoE**, **PPPoA.**
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.
Fixed IP	Click **Yes** to specify a fixed IP for the modem. Otherwise, click **No (Dynamic IP)** to allow the modem choosing a dynamic IP. If you choose **No**, the following IP Address, Subnet Mask and Default Gateway will not be changed.
IP Address	Assign an IP address for the protocol that you select.
Subnet Mask	Assign a subnet mask value for the protocol of

Item	Description
	MPoA/Static or Dynamic IP.
Default Gateway	Assign an IP address to the gateway for the protocol of **MPoA/Static or Dynamic IP**.
Primary DNS	Assign an IP address to the primary DNS.
Second DNS	Assign an IP address to the secondary DNS.

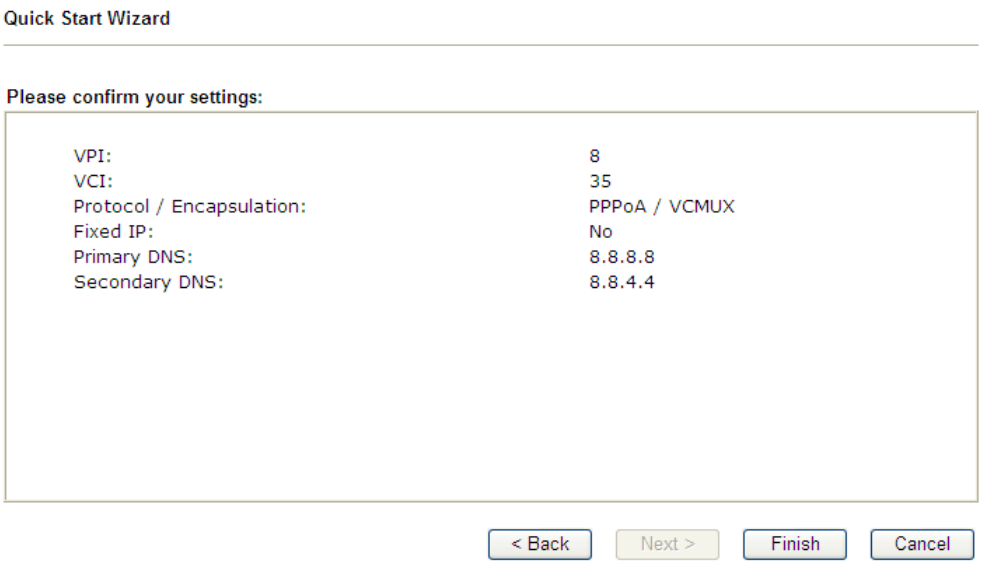
4. After finished the above settings, click **Next** to access into next page.



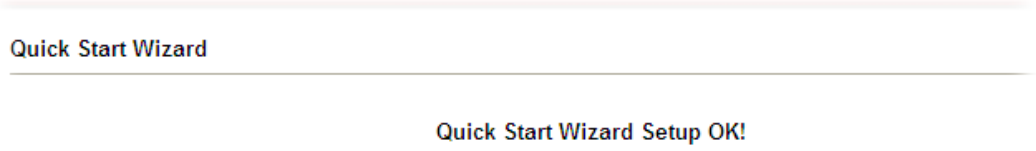
Available parameters are listed below:

Item	Description
User Name	Assign a specific valid user name provided by the ISP. It will be used to access Internet.
Password	Assign a valid password provided by the ISP. It will be used to access Internet.
Confirm Password	Retype the password.

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

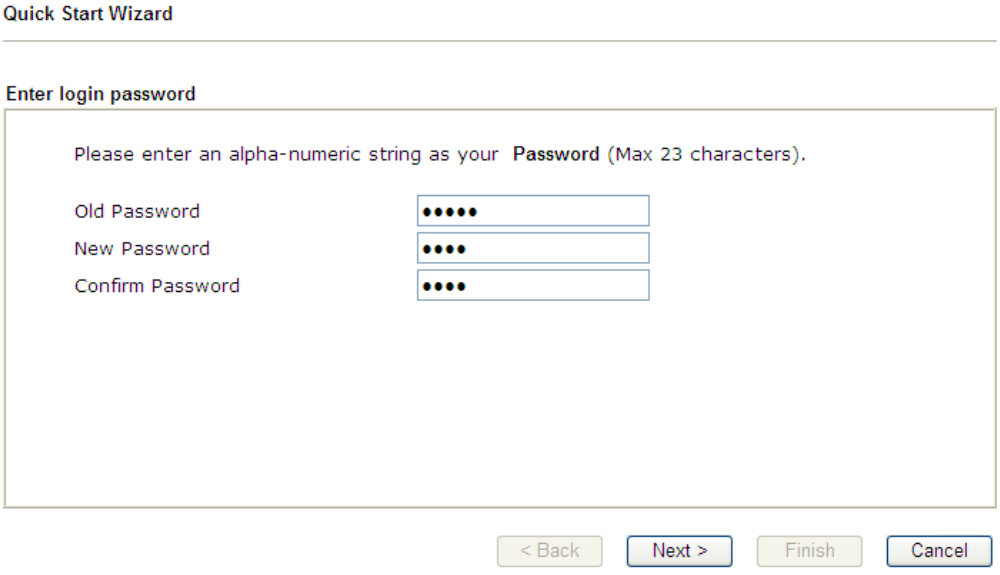


6. Click **Finish.** The Quick Start Wizard Setup OK page will be displayed.

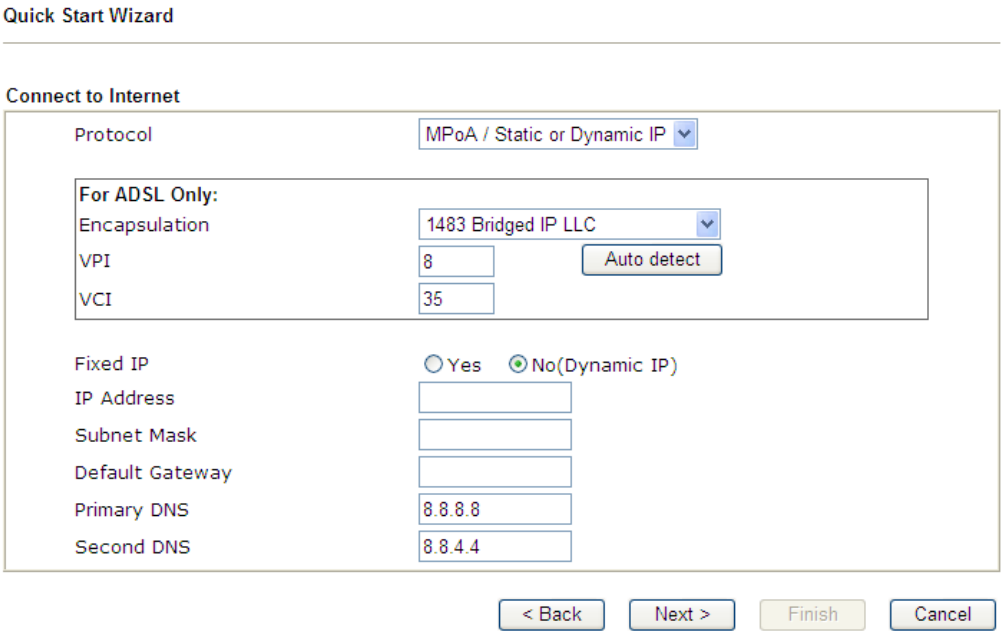


2.3.2 Setting MPoA/Static or Dynamic Connection

1. Click **Quick Start wizard**.
2. The first screen of **Quick Start Wizard** is entering login password of the web user interface. After typing the password, please click **Next**.



3. You can configure the modem to access the Internet with different protocol/modes such as **PPPoE/PPPoA** or **MPoA/Static or Dynamic IP**. The modem supports the ADSL WAN interface for Internet access. In this case, choose MPoA/Static or Dynamic.

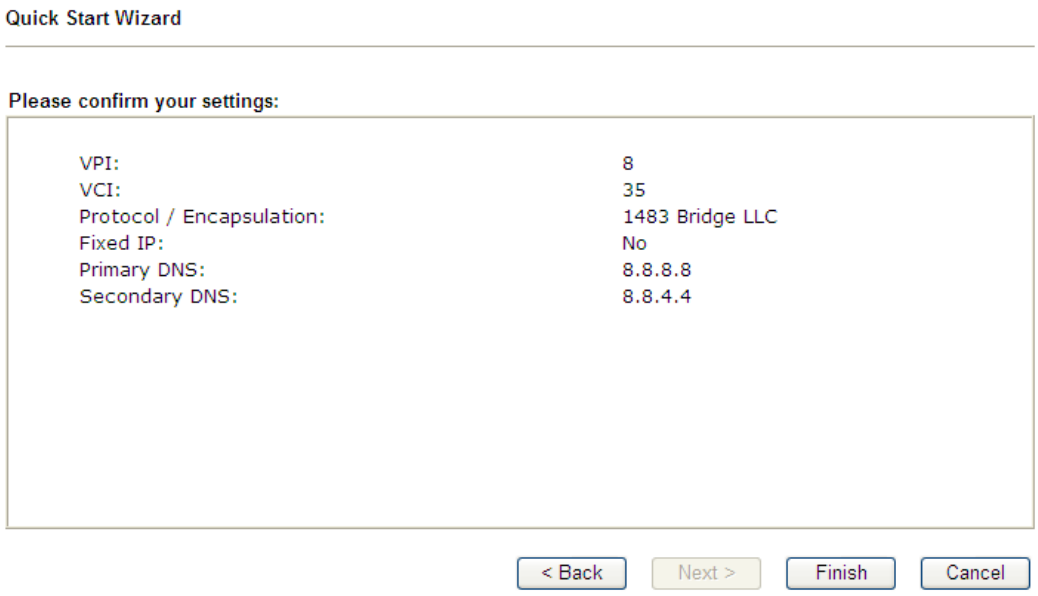


Available parameters are listed below:

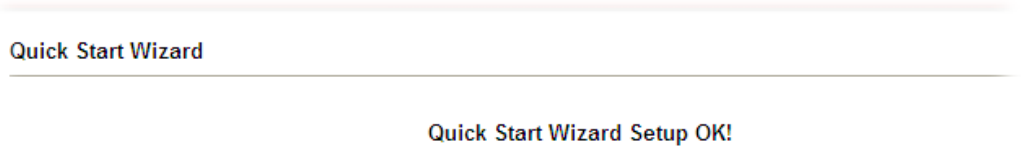
Item	Description
For ADSL Only	You have to select an appropriate WAN connection type for connecting to the Internet through this modem according to the settings that your ISP provided. **Auto detect** – Click it to detect suitable values below by the modem automatically.
Encapsulation	Select an IP mode for this WAN interface. There are several available modes for Internet access such as **PPPoE**, **PPPoA.**
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.
Fixed IP	Click **Yes** to specify a fixed IP for the modem. Otherwise, click **No (Dynamic IP)** to allow the modem choosing a dynamic IP. If you choose **No**, the following IP Address, Subnet Mask and Default Gateway will not be changed.
IP Address	Assign an IP address for the protocol that you select.
Subnet Mask	Assign a subnet mask value for the protocol of

Item	Description
	MPoA/Static or Dynamic IP.
Default Gateway	Assign an IP address to the gateway for the protocol of **MPoA/Static or Dynamic IP**.
Primary DNS	Assign an IP address to the primary DNS.
Second DNS	Assign an IP address to the secondary DNS.

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

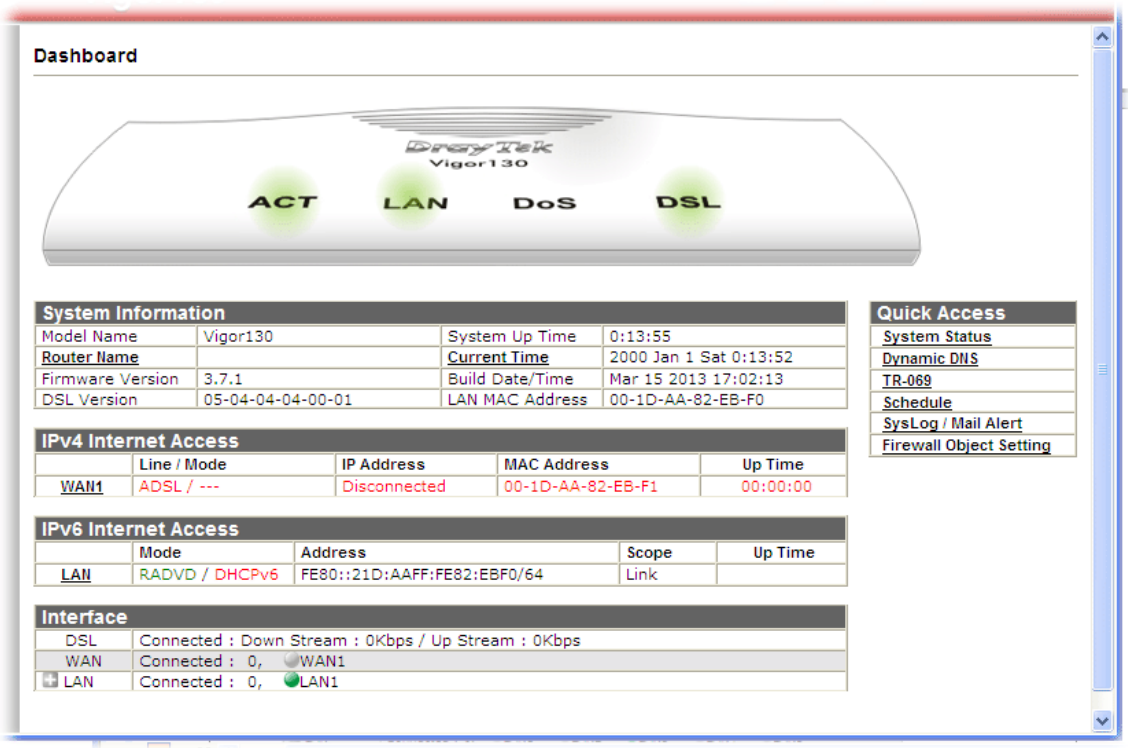


5. Click **Finish.** The Quick Start Wizard Setup OK page will be displayed.



2.4 Introducing Dashboard

The Dashboard (home page) shows the connection status including System Information, IPv4 Internet Access, IPv6 Internet Access, Interface (physical connection), Security and Quick Access.



2.4.1 Virtual Panel

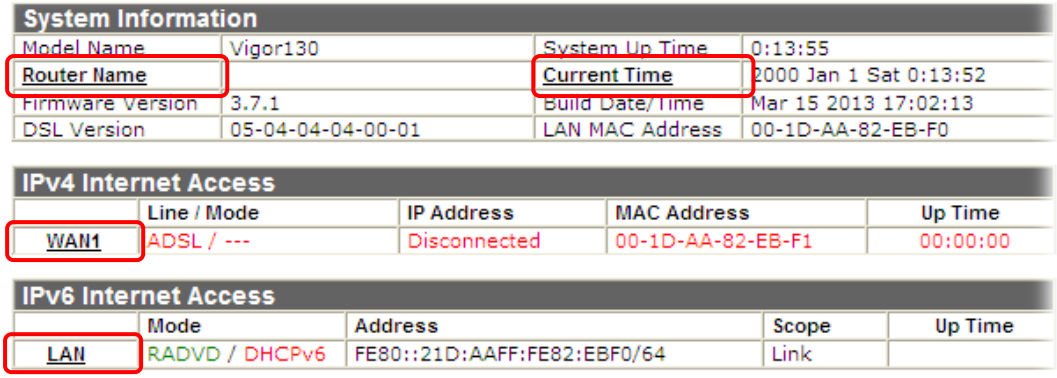
On the top of the Dashboard, a virtual panel (simulating the physical panel of the modem) displays the physical interface connection. It will be refreshed every five seconds.

Port	Color Displayed	Explanation
LED (left side)	Black	It means the modem or the function is not working.
	Green	It means the modem or the function is working.

For detailed information about the LED display, refer to **1.2 LED Indicators and Connectors**.

2.4.2 Name with a Link

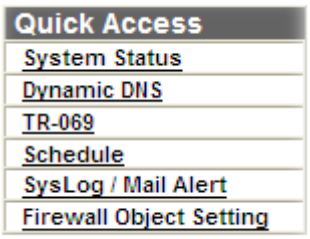
A name with a link (e.g., Router Name, Current Time, WAN1/LAN and etc.) below means you can click it to open the configuration page for modification.



2.4.3 Quick Access for Common Used Menu

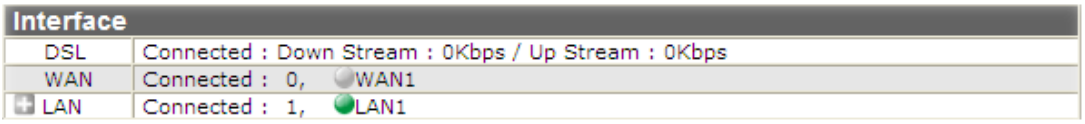
All the menu items can be accessed and arranged orderly on the left side of the main page for your request. However, some **important** and **common** used menu items which can be accessed in a quick way just for convenience.

Look at the right side of the Dashboard. You will find a group of common used functions grouped under **Quick Access**.

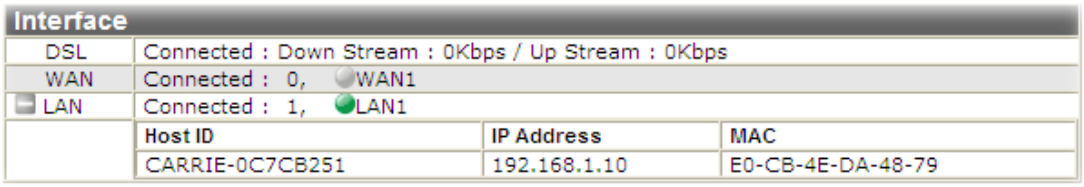


The function links of System Status, Dynamic DNS, TR-069, Schedule, Syslog/Mail Alert, and Firewall Object Setting are displayed here. Move your mouse cursor on any one of the links and click on it. The corresponding setting page will be open immediately.

Note that there is a plus ( ) icon located on the left side of LAN. Click it to review the LAN connection(s) used presently.



Host connected physically to the modem via LAN port(s) will be displayed with green circles in the field of Connected.



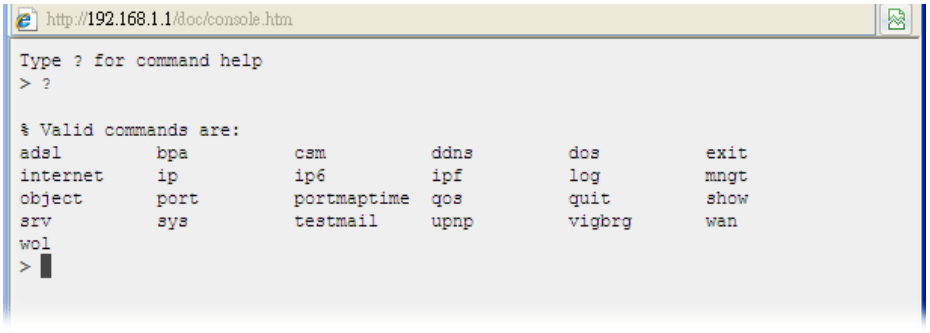
2.4.4 GUI Map

All the functions the modem supports are listed with table clearly in this page. Users can click the function link to access into the setting page of the function for detailed configuration. Click the icon on the top of the main screen to display all the functions.

2.4.5 Web Console

It is not necessary to use the telnet command via DOS prompt. The changes made by using web console have the same effects as modified through web user interface. The functions/settings modified under Web Console also can be reviewed on the web user interface.

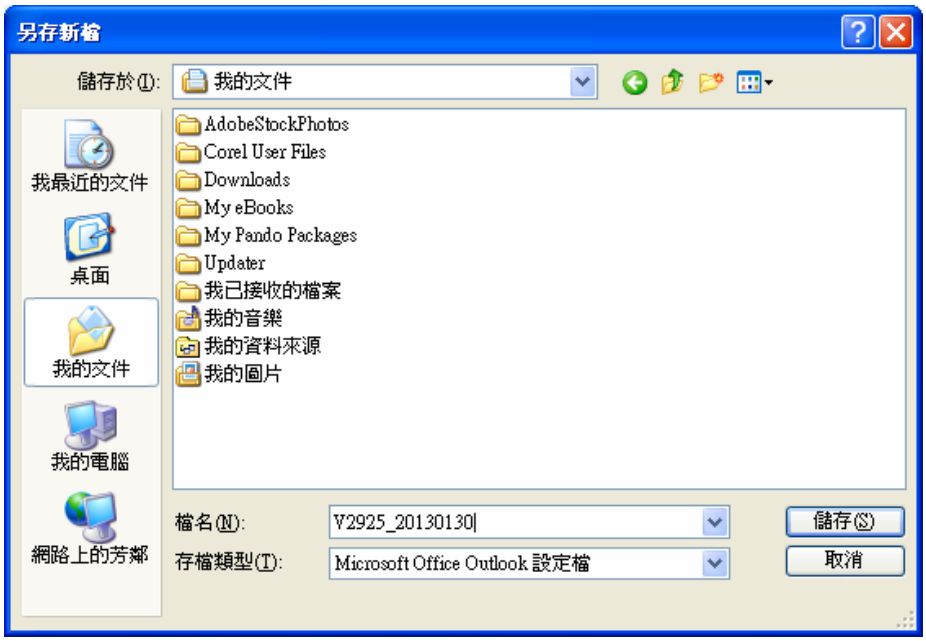
Click the **Web Console** icon on the top of the main screen to open the following screen.



2.4.6 Config Backup

There is one way to store current used settings quickly by clicking the **Config Backup** icon. It allows you to backup current settings as a file. Such configuration file can be restored by using **System Maintenance>>Configuration Backup**.

Simply click the icon on the top of the main screen and a pop up dialog will appear.



Click **Save** to store the setting.

2.4.7 Logout

Click the **Logout** icon to exit the web user interface.

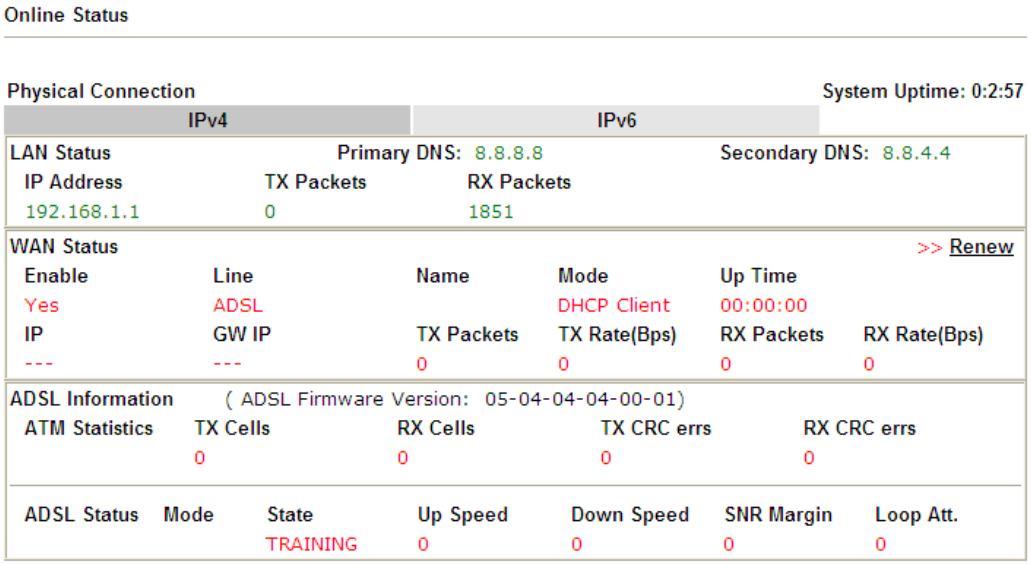
2.5 Online Status

2.5.1 Physical Connection

Such page displays the physical connection status such as LAN connection status, WAN connection status, ADSL information, and so on.

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

Physical Connection for IPv4 Protocol

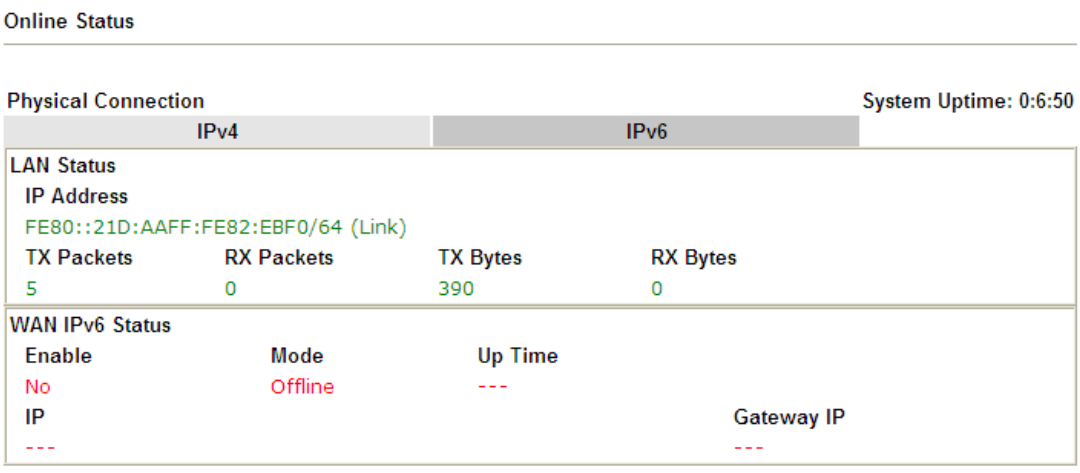


Detailed explanation is shown below:

Item	Description
LAN Status	**Primary DNS**-Display the primary DNS server address for WAN interface. **Secondary DNS** -Display the secondary DNS server address for WAN interface. **IP Address**-Display the IP address of the LAN interface. **TX Packets**-Display the total transmitted packets at the LAN interface. **RX Packets**-Display the total received packets at the LAN interface.
WAN Status	**Enable – Yes** in red means such interface is available but not connected. **Yes** in green means such interface is connected.

Item	Description
	Line – Display the physical connection of this interface. **Name** – Display the name of the modem. **Mode** - Display the type of WAN connection (e.g., PPPoE). **Up Time** - Display the total uptime of the interface. **IP** - Display the IP address of the WAN interface. **GW IP** - Display the IP address of the default gateway. **TX Packets** - Display the total transmitted packets at the WAN interface. **TX Rate** - Display the speed of transmitted octets at the WAN interface. **RX Packets** - Display the total number of received packets at the WAN interface. **RX Rate** - Display the speed of received octets at the WAN interface.
ADSL Information	**ATM Statistics –** Display the ATM layer information. **TX Cells –**Display the total number of ATM transmission cells. **RX Cells –**Display the total number of ATM received cells. **TX CRC errs –** Display the total number of transmission CRC errors. **RX CRC errs –**Display the total number of CRC errors received. **ADSL Status –**Display the ADSL layer information. **Mode –** Display the type of ADSL mode, such as T1.413, G.DMT, ADSL2+(G.992.5), and so on. **State –** Display the ADSL connection status, such as Ready, HANDSHAKING, SHOWTIME and so on. **Up Speed –** Display the upstream rate. **Down Speed –** Display the downstream rate. **SNR Margin –** Display number of SRR Margin. **Loop Att .-** Display the number of Loop Attenuation.

Physical Connection for IPv6 Protocol



Detailed explanation (for IPv6) is shown below:

Item	Description
LAN Status	**IP Address**- Displays the IPv6 address of the LAN interface.. **TX Packets**-Displays the total transmitted packets at the LAN interface. **RX Packets**-Displays the total received packets at the LAN interface. **TX Bytes** - Displays the speed of transmitted octets at the LAN interface. **RX Bytes** - Displays the speed of received octets at the LAN interface.
WAN IPv6 Status	**Enable – No** in red means such interface is available but not enabled. **Yes** in green means such interface is enabled. No in red means such interface is not available. **Mode** - Displays the type of WAN connection (e.g., TSPC). **Up Time** - Displays the total uptime of the interface. **IP** - Displays the IP address of the WAN interface. **Gateway IP** - Displays the IP address of the default gateway.

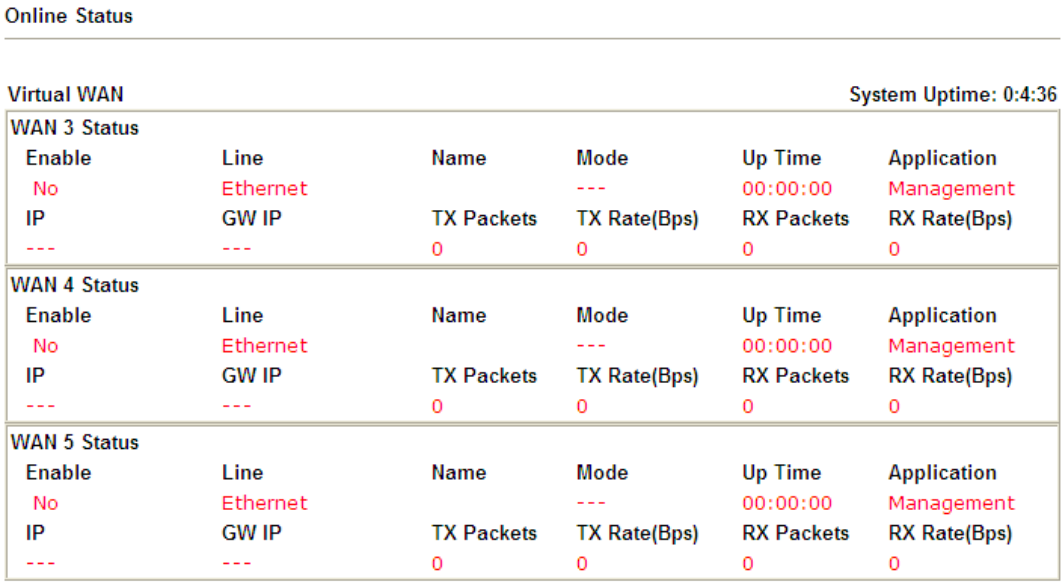
Note: The words in green mean that the WAN connection of that interface (WAN1) is ready for accessing Internet; the words in red mean that the WAN connection of that interface (WAN1) is not ready for accessing Internet.

2.5.2 Virtual WAN

Such page displays the virtual WAN connection information.

Virtual WAN are used by TR-069 management, VoIP service and so on.

The Application field will list the purpose of such WAN connection.



Detailed explanation is shown below:

Item	Description
WAN Status	**Enable – Yes** in red means such interface is available but not enabled. **Yes** in green means such interface is enabled. **Line** – Display the physical connection (Ethernet, or USB) of this interface. **Name** – Display the name of the modem. **Mode** - Display the type of WAN connection (e.g., PPPoE). **Up Time** - Display the total uptime of the interface. **IP** - Displays the IP address of the WAN interface. **GW IP** - Display the IP address of the default gateway. **TX Packets** - Display the total transmitted packets at the WAN interface. **TX Rate** - Display the speed of transmitted octets at the WAN interface. **RX Packets** - Display the total number of received packets at the WAN interface. **RX Rate** - Display the speed of received octets at the WAN interface.

2.6 Saving Configuration

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

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

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

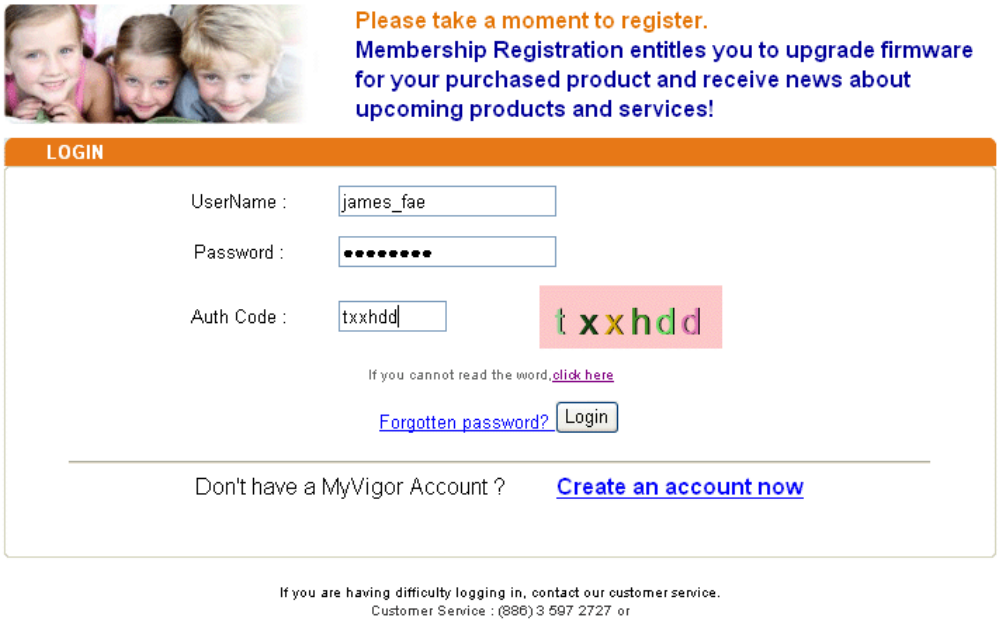
2.7 Registering Vigor Router

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

1 Again, login the web configuration interface of Vigor modem by typing "**admin/admin**" as User Name / Password.

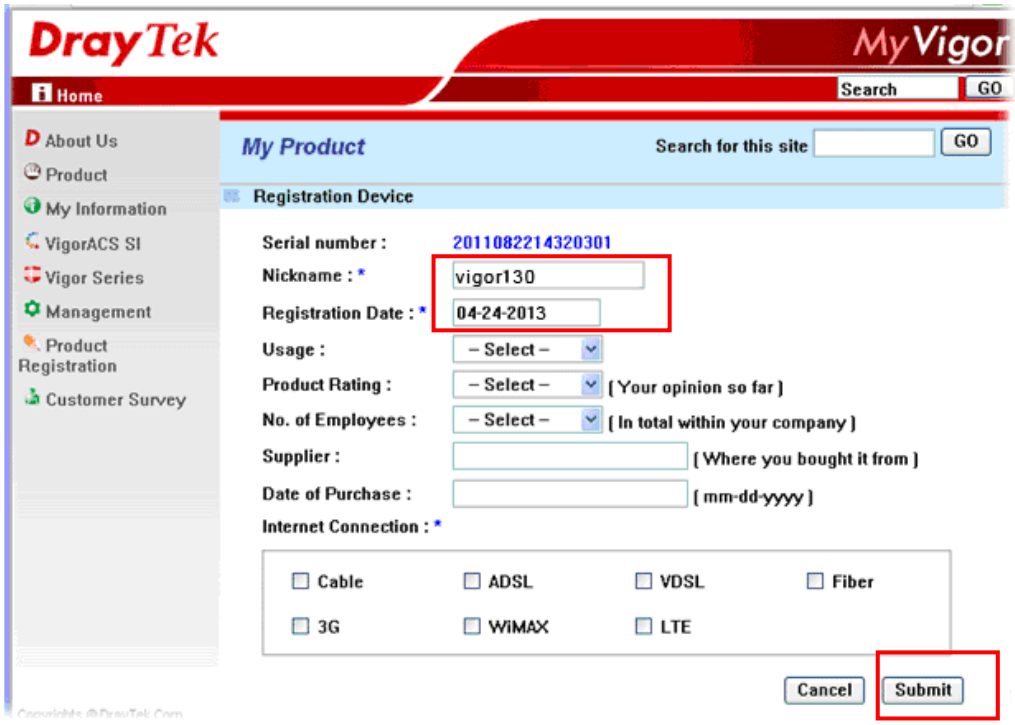
2 Click **Support Area>>Production Registration** from the home page.

3 A **Login** page will be shown on the screen. Please type the account and password that you created previously. And click **Login**. If not, please click **Create an account now link** first to create a new account. Then, back to this setting page.

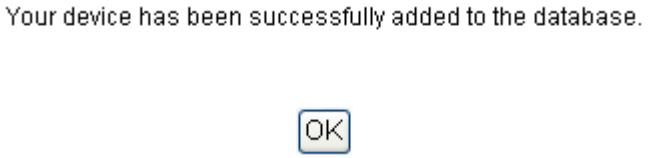


4 The following page will be displayed after you logging in MyVigor. From this page, please click **Add** or **Product Registration**.

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



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



7 Now, you have finished the product registration.

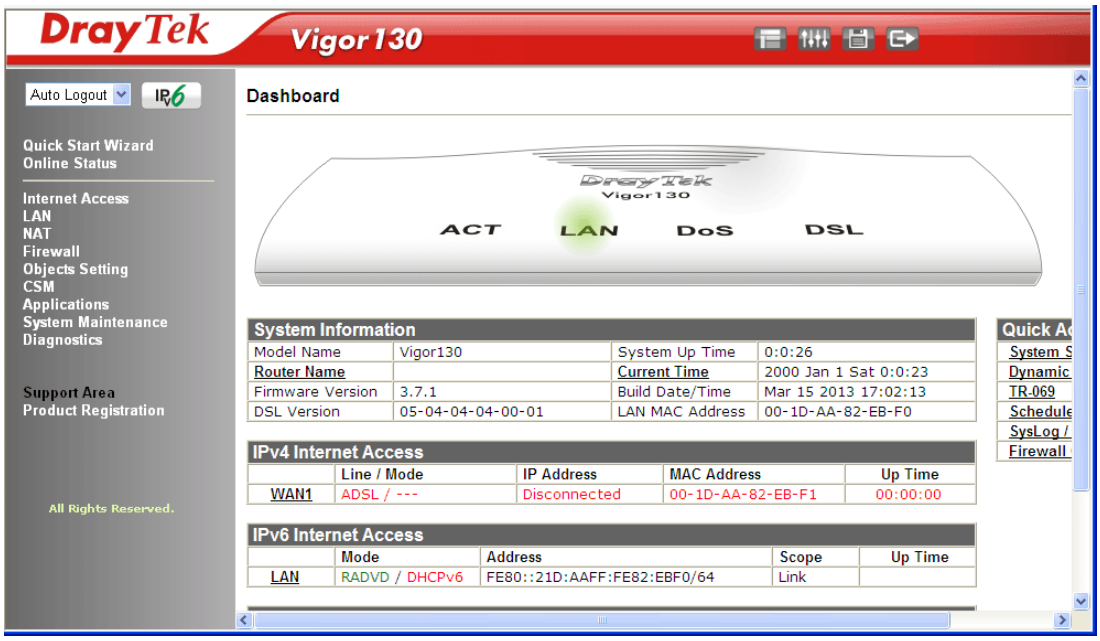
8 After clicking **OK**, you will see the following page. Your modem has been registered to *myvigor* website successfully.

3 Advanced Configuration

This chapter will guide users to execute advanced (full) configuration. As for other examples of application, please refer to chapter 5.

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

Now, the **Main Screen** will appear. Note that “Admin mode” will be displayed on the bottom left side.



3.1 Internet Access

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

3.1.1 Basics of Internet Protocol (IP) Network

IP means Internet Protocol. Every device in an IP-based Network including modems, 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 modem since they do not need to be accessed by the public. Hence, the NIC has reserved certain addresses that will never be registered publicly. These are known as ***private*** IP addresses, and are listed in the following ranges:

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

What are Public IP Address and Private IP Address

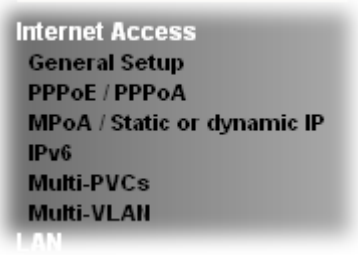
As the modem plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor modem. The modem itself will also use the default **private IP** address: 192.168.1.1 to communicate with the local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

Get Your Public IP Address from ISP

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

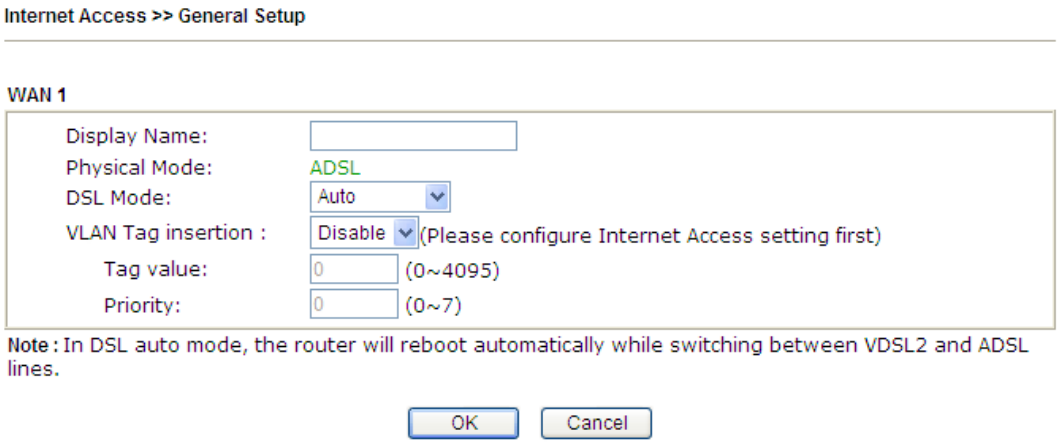
When a modem begins to connect to your ISP, a serial of discovery process will occur to ask for a connection. Then a session will be created. Your user ID and password is authenticated via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information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

Below shows the menu items for Internet Access.



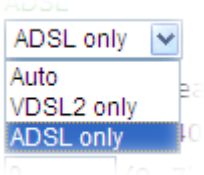
3.1.2 General Setup

This section will introduce some general settings of Internet.



Available settings are explained as follows:

Item	Description
Display Name	Type the description for such WAN interface.

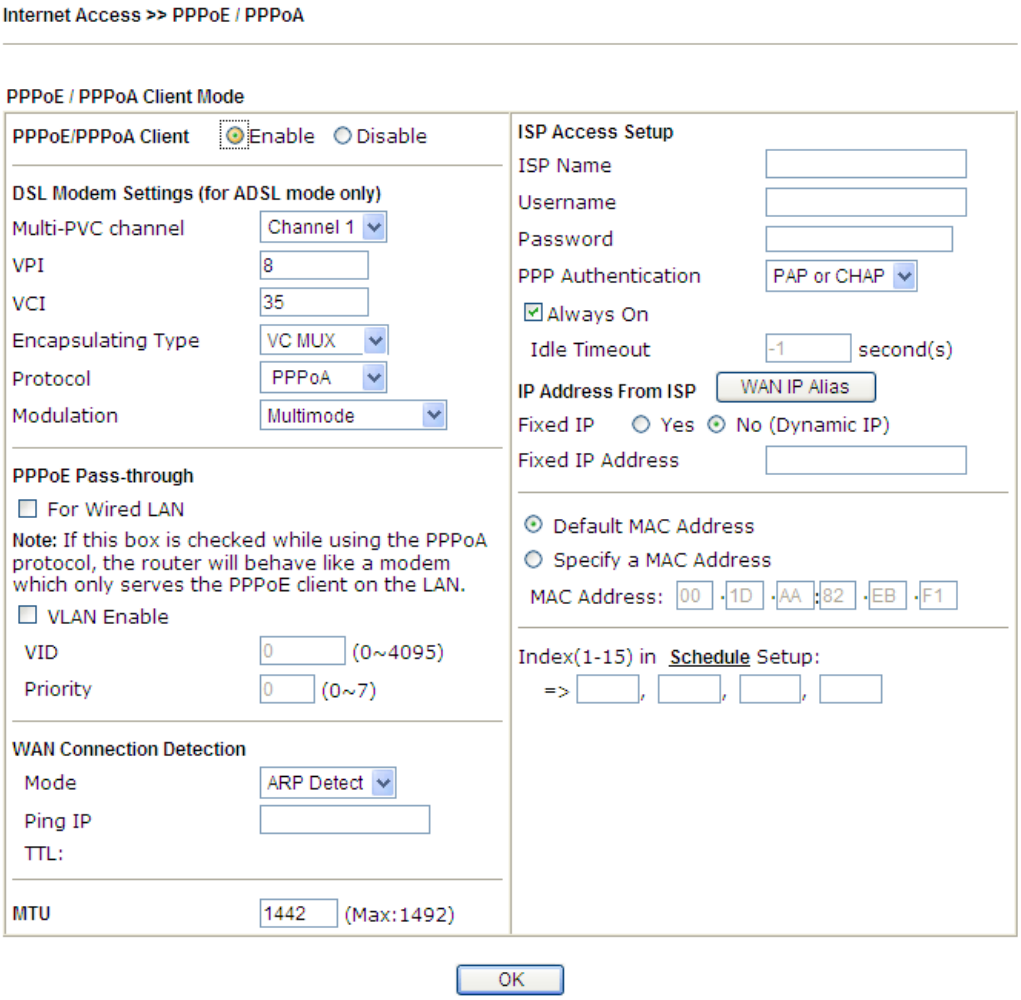
Physical Mode	Display the physical mode of such WAN interface.
DSL Mode	Specify which DSL mode can be used for such WAN connection. **Auto** – The system will choose the suitable one automatically. 
VLAN Tag insertion	**Enable** – Enable the function of VLAN with tag. The modem will add specific VLAN number to all packets on the WAN while sending them out. Please type the tag value and specify the priority for the packets sending by WAN1. **Disable** – Disable the function of VLAN with tag. **Tag value** – Type the value as the VLAN ID number. The range is form 0 to 4095. **Priority** – Type the packet priority number for such VLAN. The range is from 0 to 7.

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

3.1.3 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 modem encapsulates the PPP session based for transport across the ADSL loop and your ISP's Digital Subscriber Line Access Multiplexer (SDLAM).

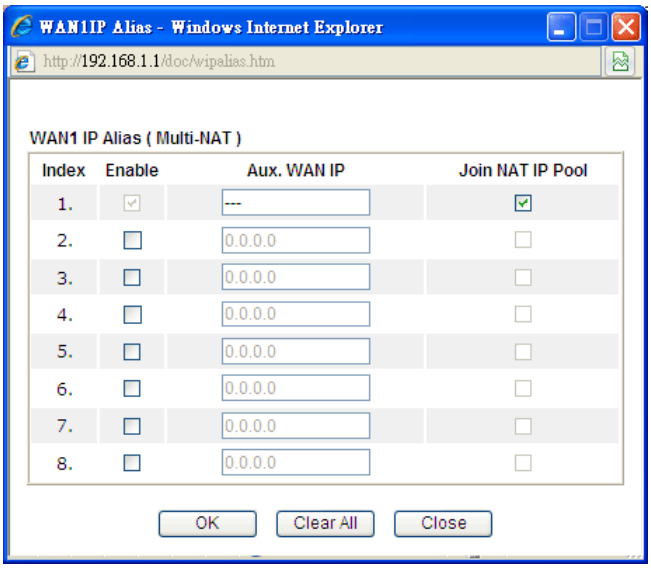
To choose PPPoE or PPPoA as the accessing protocol of the internet, please select **PPPoE/PPPoA** from the **Internet Access** menu. The following web page will be shown.



Available settings are explained as follows:

Item	Description
Enable/Disable	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**. **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 protocol, PPPoE or PPPoA. **Modulation** – Choose a suitable method for PPPoE/PPoA connection.
PPPoE Pass-through	The modem offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor modem. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction. **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. However, if this box is checked in PPPoA protocol, only PPPoE clients on the LAN will be served and only one session is allowed. **VLAN Enable** - Enable the function of VLAN with tag. The modem will add specific VLAN number to all packets while sending them out. Please type the tag value and specify the priority for the packets sent by the modem. **VLAN ID** –Type the value as the VLAN ID number. The range is form 1 to 4095. **Priority (802.1p)** - Type the packet priority number for such VLAN. The range is from 0 to 7.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. **Mode** – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection. **Ping IP** – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. **TTL (Time to Live)** – Displays value for your reference. TTL value is set by telnet command.
MTU	It means Max Transmit Unit for packet. The default setting will be 1442.
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 the name of the ISP if required. **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** - If you want to connect to Internet all the time, check the **Always On** box. **Idle Timeout** – Set the timeout for breaking down the Internet after passing through the time without any action. This setting

	is active only when the **Active on demand** option for Active Mode is selected in **WAN>> General Setup** page.
IP Address 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. **WAN IP Alias -** If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.  **Fixed IP** – Click **Yes** to use this function and type in a fixed IP address in the box of **Fixed IP Address**. **Default MAC Address** – You can use **Default MAC Address** or specify another MAC address by typing on the boxes of MAC Address for the modem. **Specify a MAC Address –** Type the MAC address for the modem 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 **Applications >> 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.

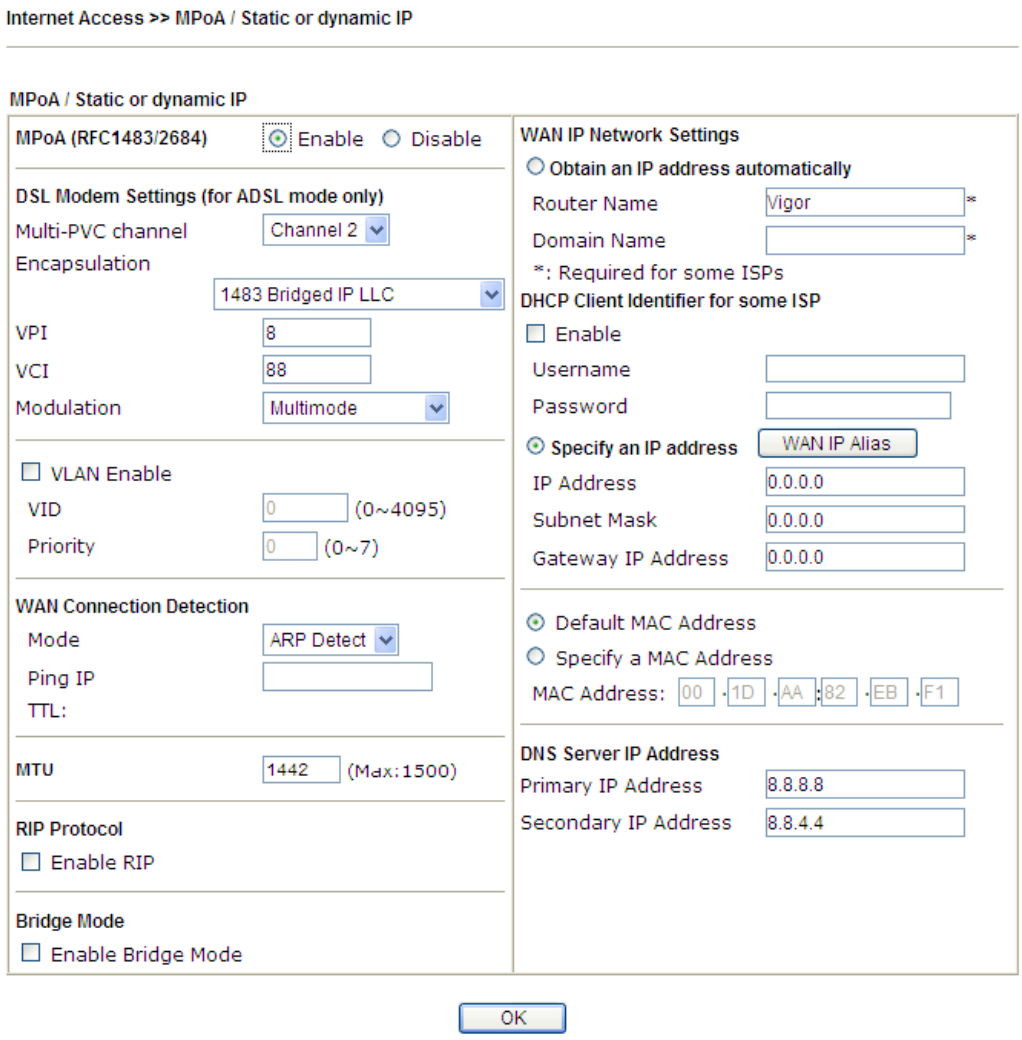
3.1.4 MPoA /Static or dynamic IP

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.

For static IP mode, you usually receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your DSL or Cable ISP service providers. In most cases, a

Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you have a public subnet, you could assign an IP address or many IP address to the WAN interface.

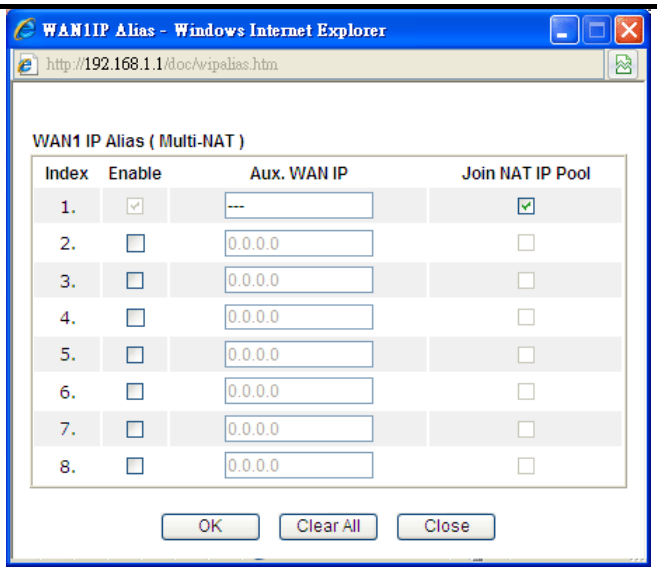
To use **MPoA /Static or dynamic IP** as the accessing protocol of the Internet, select **MPoA** mode. The following web page will appear.



Available settings are explained as follows:

Item	Description
Enable/Disable	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**. **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 protocol, PPPoE or

	PPPoA. **Modulation** – Choose a suitable method for PPPoE/PPoA connection.
VLAN Enable	Enable the function of VLAN with tag. The modem will add specific VLAN number to all packets while sending them out. Please type the tag value and specify the priority for the packets sending by the modem. **VLAN ID** –Type the value as the VLAN ID number. The range is form 1 to 4095. **Priority (802.1p)** - Type the packet priority number for such VLAN. The range is from 0 to 7.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. **Mode** – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection. **Ping IP** – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. **TTL (Time to Live)** – Displays value for your reference. TTL value is set by telnet command.
MTU	It means Max Transmit Unit for packet. The default setting will be 1442.
RIP Protocol	Routing Information Protocol is abbreviated as RIP （RFC1058）specifying how modems 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. The modem will work as a bridge modem.
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. **Modem Name** – Type in the modem name provided by ISP. **Domain Name** – Type in the domain name that you have assigned.
DHCP Client Identifier for some ISP	This feature is offered for certain ISP with special request. **Enable** – Check this box to enable the function of DHCP client identifier for some ISP. **Username** – Type a username used for such function. **Password** – Type a password used for such function.
Specify an IP address	Click this radio button to specify some data. **WAN IP Alias** - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.

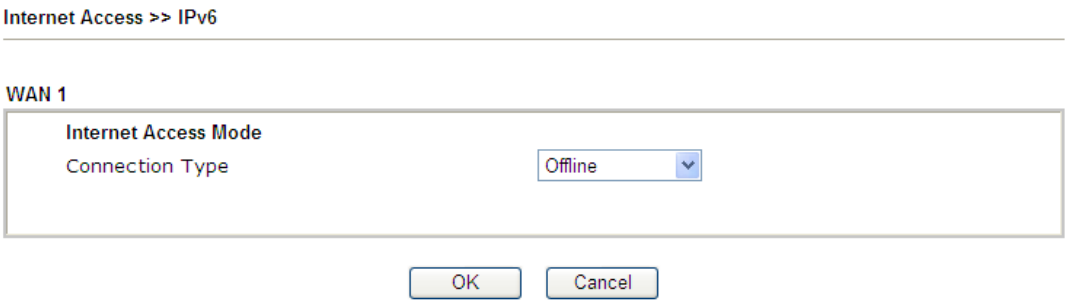
	 **IP Address** – Type in the private IP address. **Subnet Mask** – Type in the subnet mask. **Gateway IP Address** – Type in gateway IP address.
Default MAC Address	Type in MAC address for the modem. You can use **Default MAC Address** or specify another MAC address for your necessity. **MAC Address** – Type in the MAC address for the modem manually.
DNS Server IP Address	Type in the primary IP address for the modem. If necessary, type in secondary IP address for necessity in the future.

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

3.1.5 IPv6

Offline

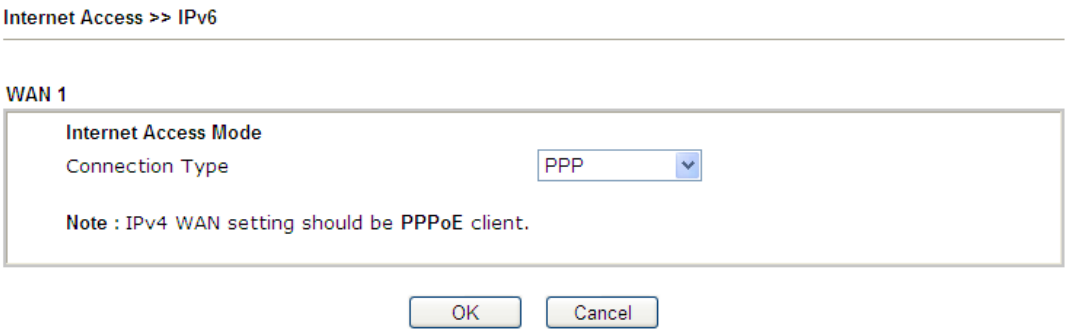
When **Offline** is selected, the IPv6 connection will be disabled.



PPP

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

No need to type any other information for PPP mode.



Below shows an example for successful IPv6 connection based on PPPoE mode.

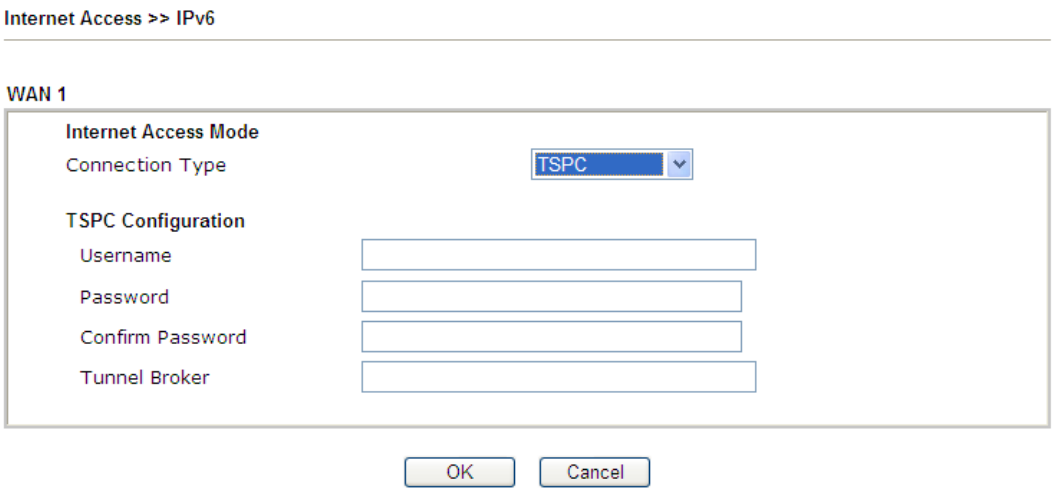
Note: At present, the **IPv6 prefix** can be acquired via the PPPoE mode connection which is available for the areas such as Taiwan (hinet), the Netherlands, Australia and UK.

TSPC

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

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

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

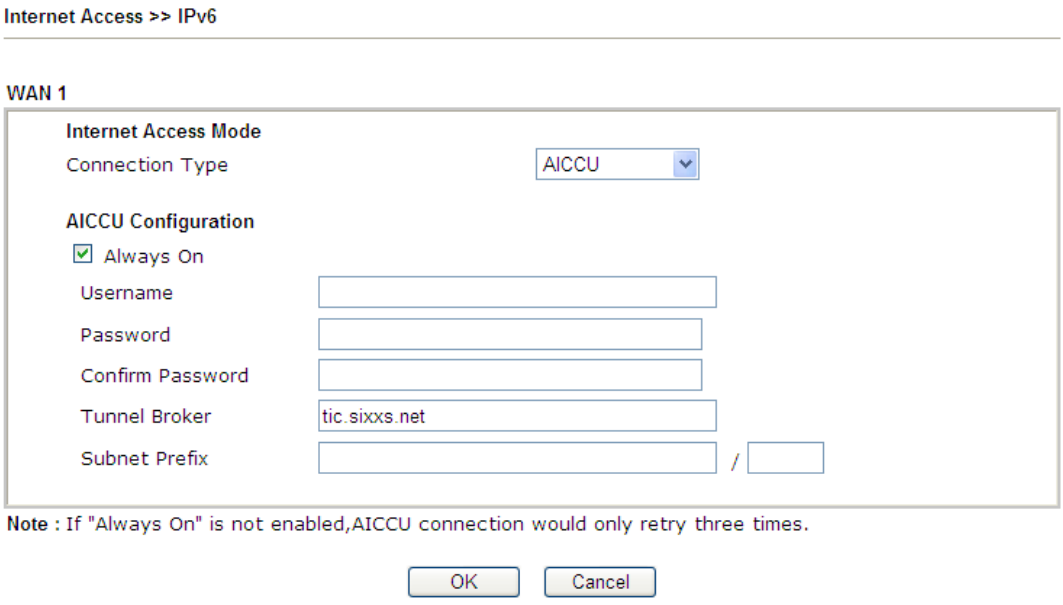


Available settings are explained as follows:

Item	Description
Username	Type the name obtained from the broker. It is suggested for you to apply another username and password for http://gogonet.gogo6.com/page/freenet6-account.
Password	Type the password assigned with the user name.
Confirm Password	Type the password again to make the confirmation.
Tunnel Broker	Type the address for the tunnel broker IP, FQDN or an optional port number.

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

AICCU



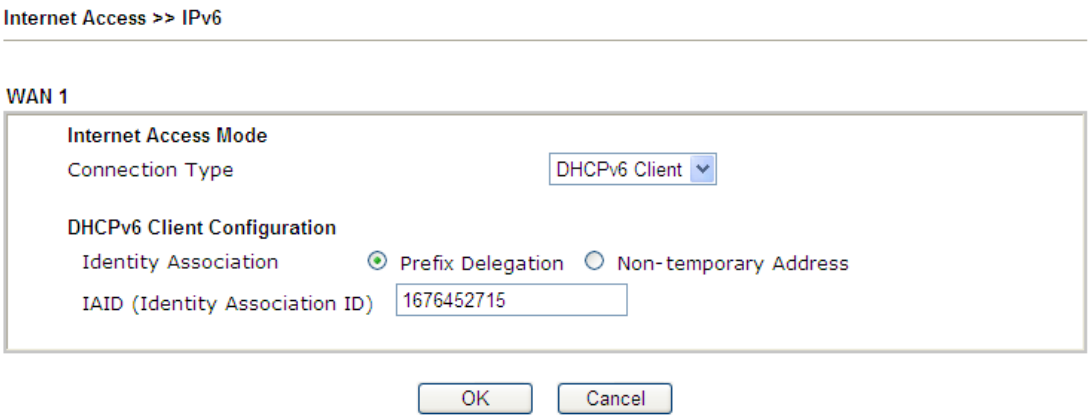
Available settings are explained as follows:

Item	Description
Always	The IPv6 network connection will be always on when this box is checked.
Username	Type the name obtained from the broker. Please apply new account at http://www.sixxs.net/. It is suggested for you to apply another username and password.
Password	Type the password assigned with the user name.
Confirm Password	Type the password again to make the confirmation.
Tunnel Broker	Type the address for the tunnel broker IP, FQDN or an optional port number.
Subnet Prefix	Type the subnet prefix address getting from service provider

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

DHCPv6 Client

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



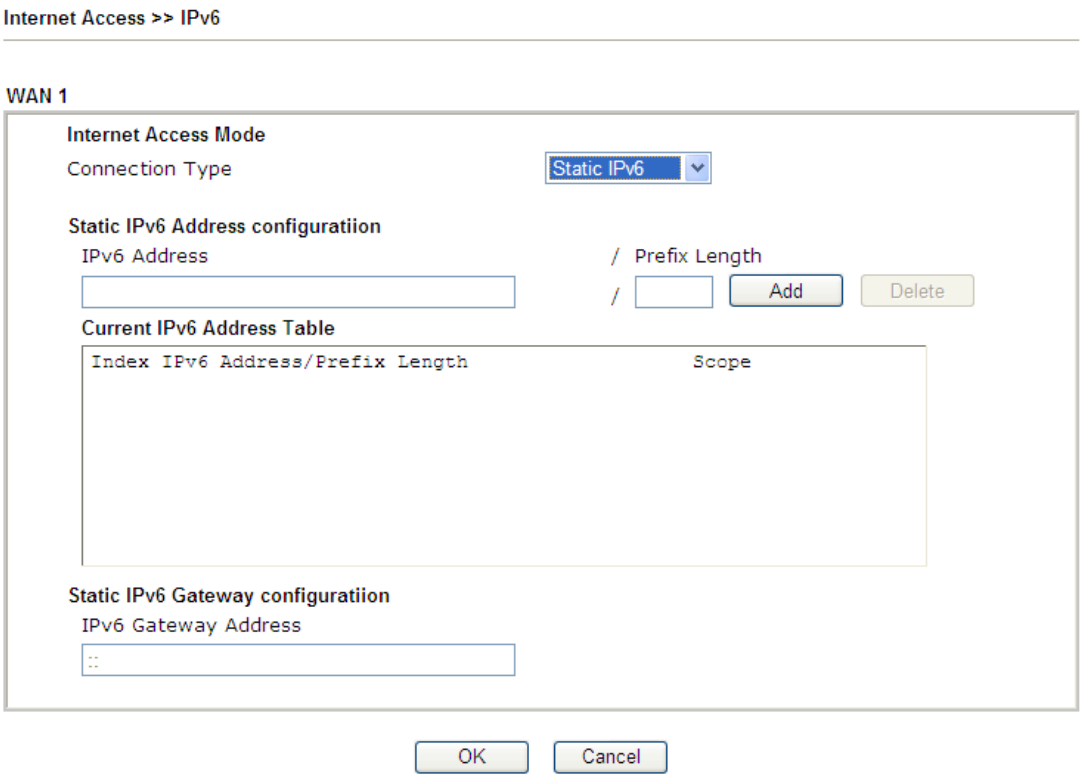
Available settings are explained as follows:

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

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

Static IPv6

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



Available settings are explained as follows:

Item	Description
Static IPv6 Address configuration	**IPv6 Address –** Type the IPv6 Static IP Address. **Prefix Length –** Type the fixed value for prefix length. **Add –** Click it to add a new entry. **Delete –** Click it to remove an existed entry.
Current IPv6 Address Table	Display current interface IPv6 address.
Static IPv6 Gateway Configuration	**IPv6 Gateway Address -** Type your IPv6 gateway address here.

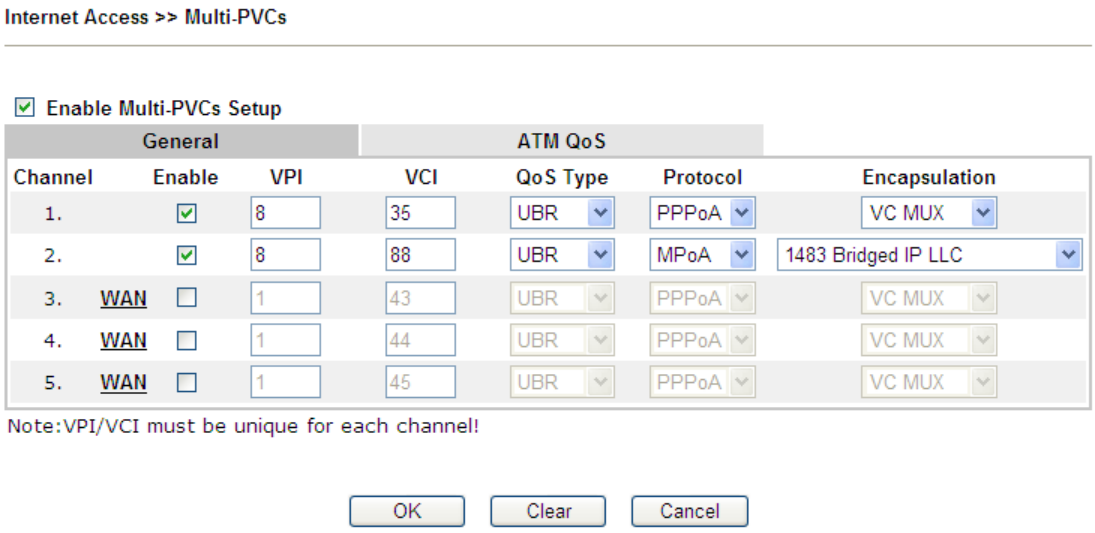
After finishing all the settings here, please click **OK** to save the configuration.

3.1.6 Multi-PVCs

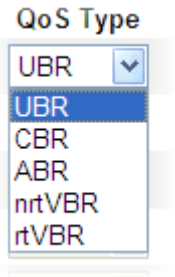
This modem allows you to create multi-PVCs for different data transferring for using. Simply go to **Internet Access** and select **Multi-PVC Setup** page.

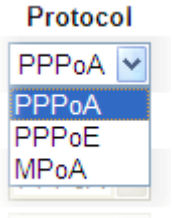
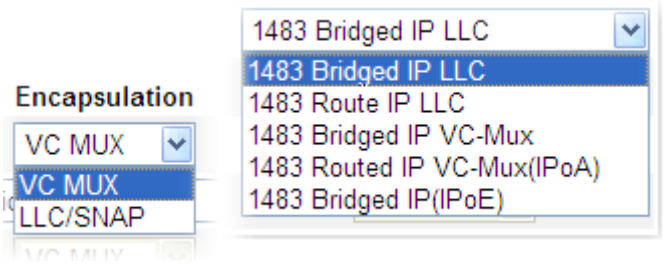
General

The system allows you to set up to eight channels which are ready for choosing as the first PVC line that will be used as multi-PVCs.

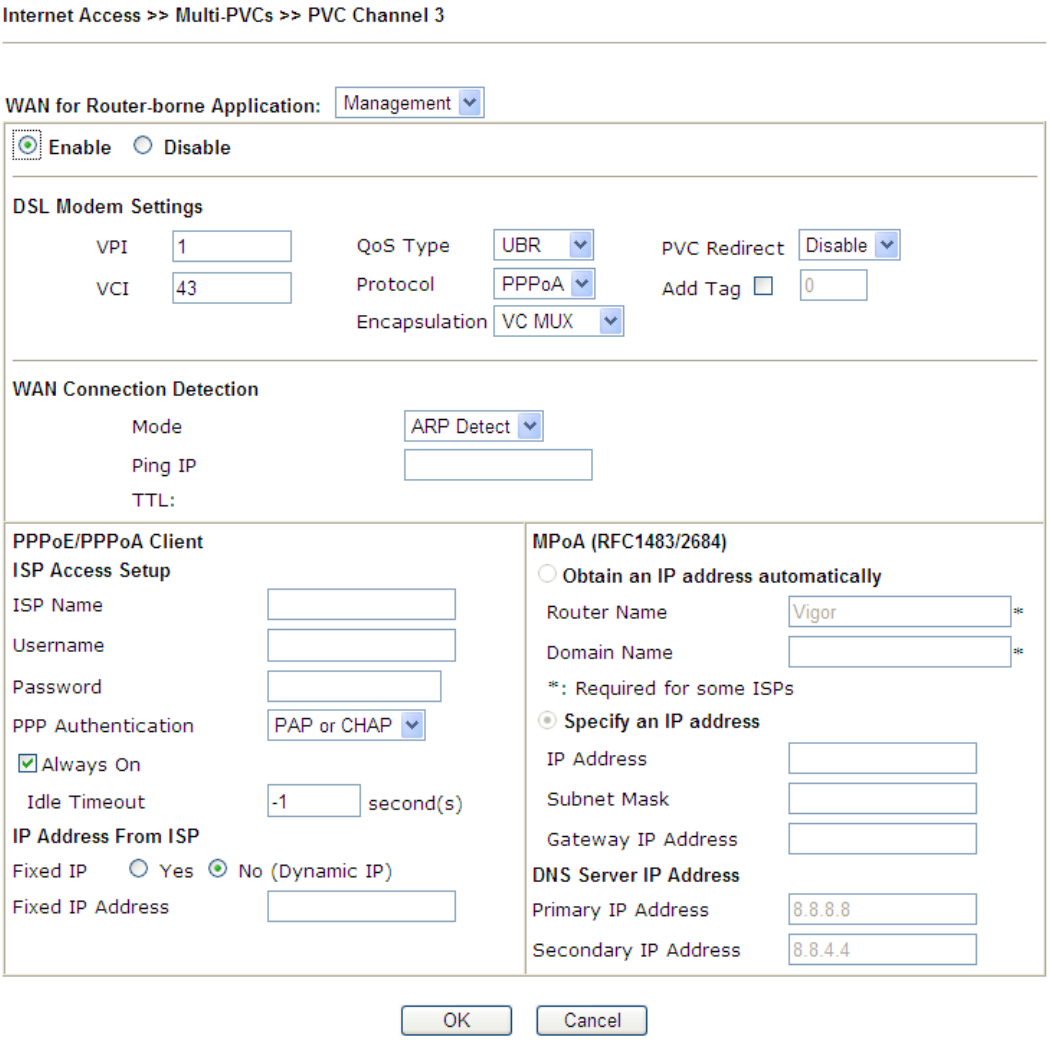


Available settings are explained as follows:

Item	Description
Enable Multi-PVCs Setup	Check it to enable the multi-PVCs function.
Enable	Check this box to enable that channel. The channels that you enabled here will be shown in the **Multi-PVC channel** drop down list on the web page of **Internet Access**. Though you can enable eight channels in this page, yet only one channel can be chosen on the web page of **Internet Access**.
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. 

WAN link for Channel 3, 4 and 5 are provided for modem-borne application such as TR-069 and VoIP. The settings must be applied and obtained from your ISP. For your special request, please contact with your ISP and then click WAN link of Channel 3 or 4 to configure your modem.



Available settings are explained as follows:

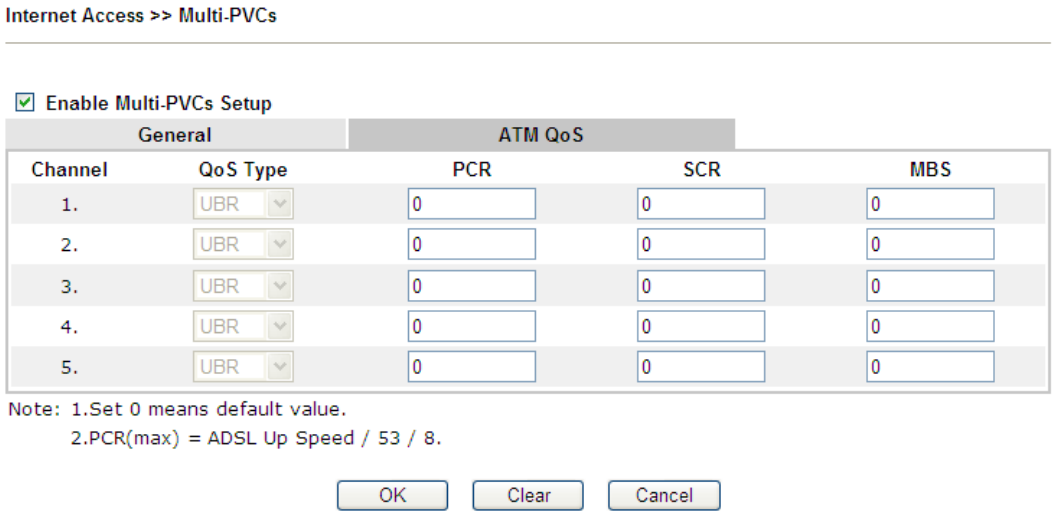
Item	Description
WAN for Router-borne Application	Choose the modem service for channel 5, 6 or 7. **Management** - It can be specified for general management (Web configuration/telnet/TR-069). If you choose Management, the configuration for this PVC will be effective for Web configuration/telnet/TR-069. **IPTV** - It can be specified for IPTV only. If you choose IPTV, the configuration for this PVC will be effective for IPTV data transmitting and receiving.

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

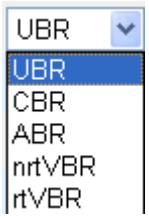
For other settings, refer to **3.1.3 PPPoE/PPPoA.**

ATM QoS

Such configuration is applied to upstream packets. Such information will be provided by ISP. Please contact with your ISP for detailed information.

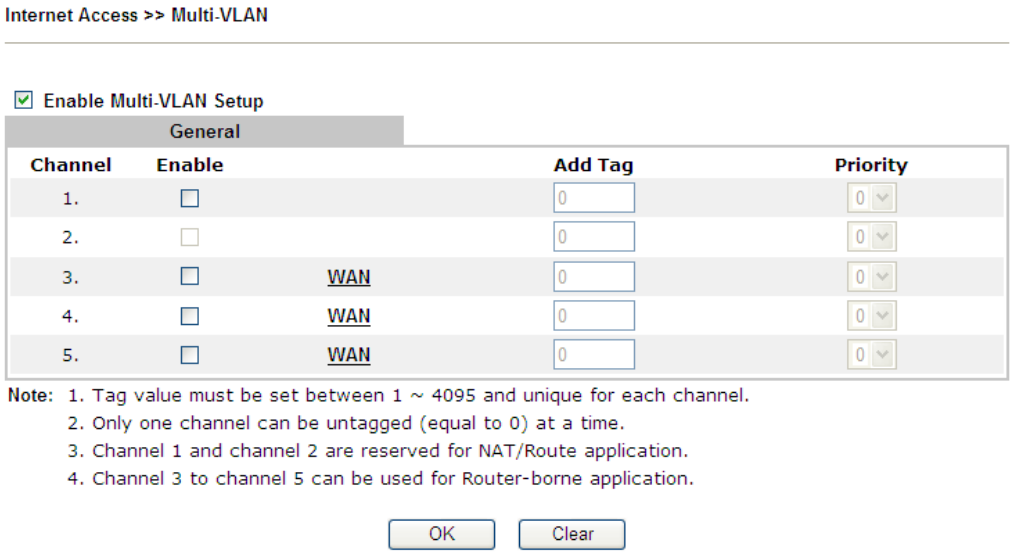


Available settings are explained as follows:

Item QoS Type	Description
	Select a proper QoS type for the channel according to the information that your ISP provides. 
PCR	It represents Peak Cell Rate. The default setting is “0”.
SCR	It represents Sustainable Cell Rate. The value of SCR must be smaller than PCR.
MBS	It represents Maximum Burst Size. The range of the value is 10 to 50.

3.1.7 Multi-VLAN

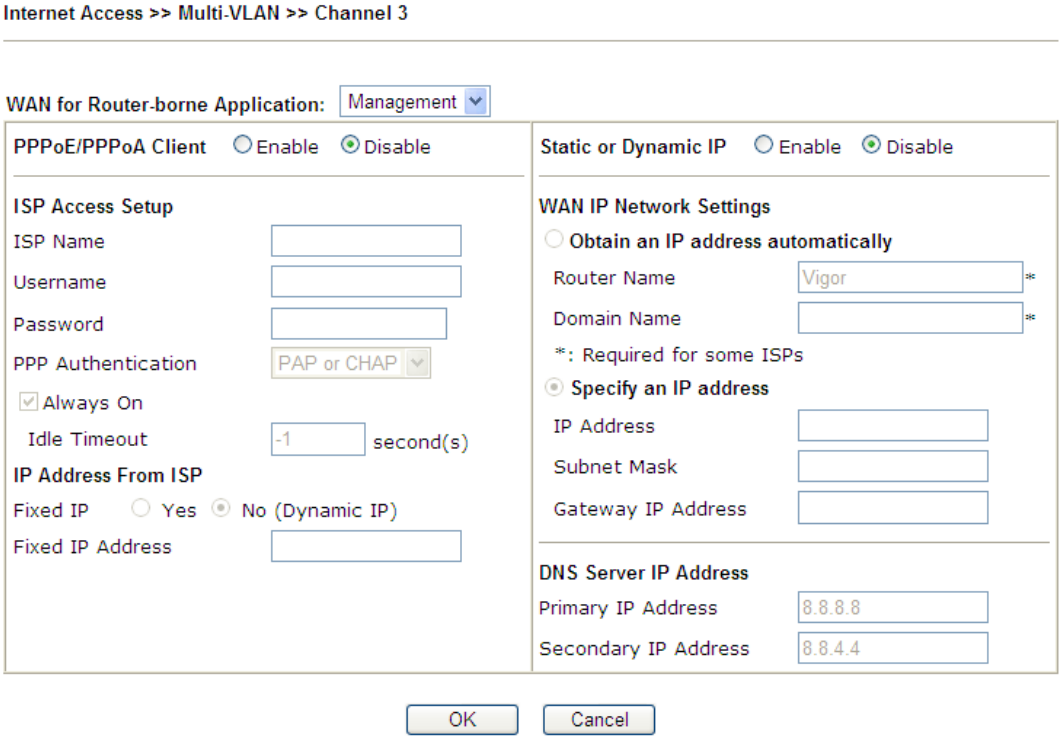
This modem allows you to create multi-VLAN for different purposes of data transferring. Simply go to **WAN** and select **Multi-VLAN**.



Available settings are explained as follows:

Item	Description
Enable	Check it to enable such function.
Channel	Display the number of each channel.
Enable	Check this box to enable that channel. The channels that you enabled here will be shown in the **Multi-VLAN** channel drop down list on the web page of **Internet Access**. Though you can enable eight channels in this page, yet only one channel can be chosen on the web page of **Internet Access**.
Add Tag	To identify the usage of VLAN, check this box to invoke this setting. And type the number for VLAN ID (number).
Priority	To add the packet priority number for such VLAN. The range is from 0 to 7.

WAN link for Channel 3, 4 and 5 are provided for router-borne application such as **TR-069**. The settings must be applied and obtained from your ISP. For your special request, please contact with your ISP and then click **WAN** link of Channel 3, 4 or 5 to configure your modem.



Available settings are explained as follows:

Item	Description
WAN for Router-borne Application	Choose the modem service for channel 3, 4 or 5. **Management** - It can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this VLAN will be effective for Web configuration/telnet/TR069. **IPTV** - It can be specified for IPTV only. If you choose IPTV, the configuration for this VLAN will be effective for IPTV data transmitting and receiving.

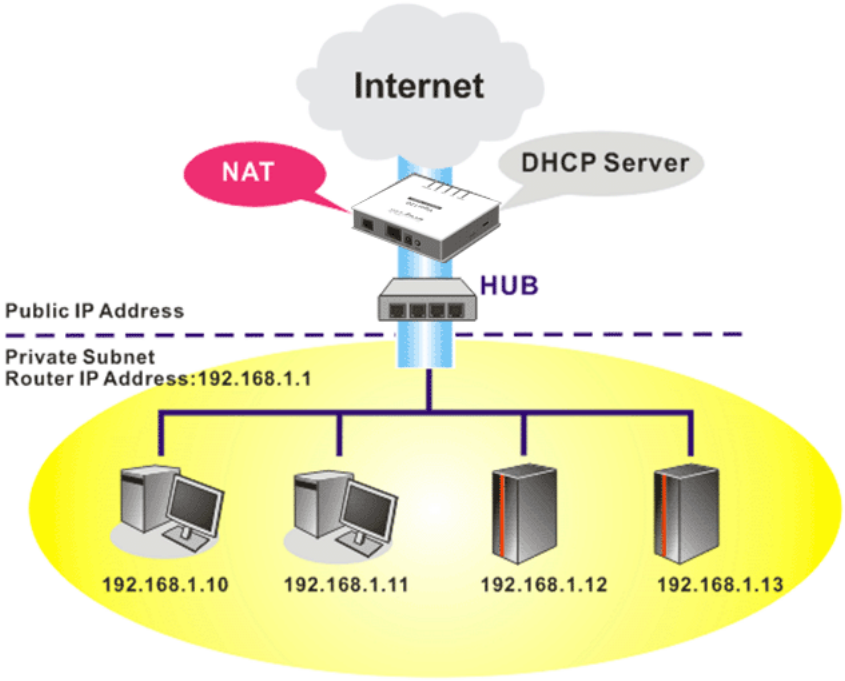
For other settings, refer to **3.3.3 PPPoE/PPPoA.**

3.2 LAN

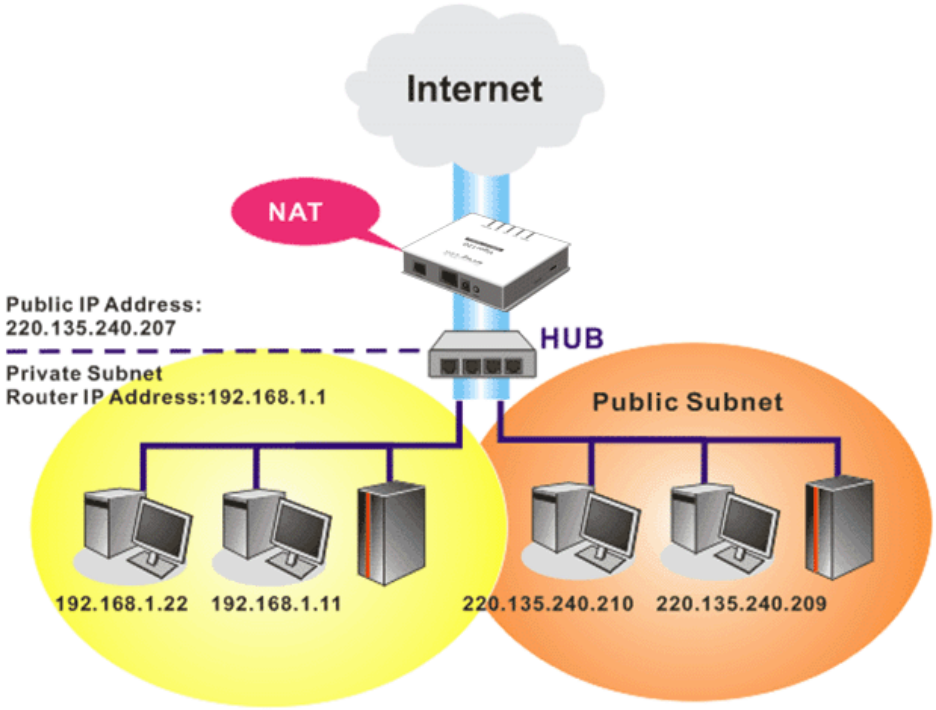
Local Area Network (LAN) is a group of subnets regulated and ruled by modem. The design of network structure is related to what type of public IP addresses coming from your ISP.

3.2.1 Basics of LAN

The most generic function of Vigor modem is NAT. It creates a private subnet of your own. As mentioned previously, the modem 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 modem 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 modem will serve for IP routing to help hosts in the public subnet to communicate with other public hosts or servers outside. Therefore, the modem should be set as the gateway for public hosts.

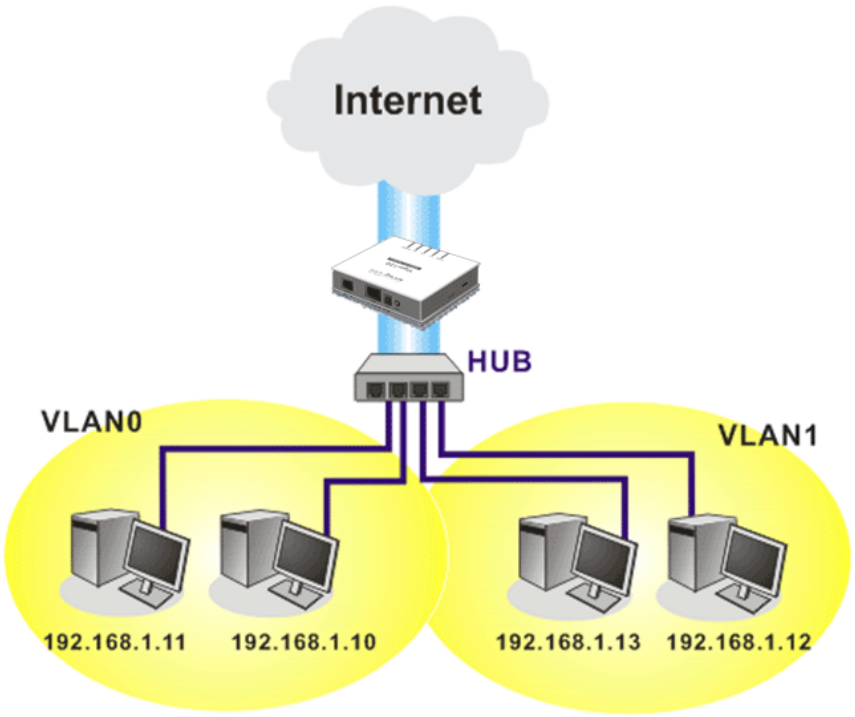


What is Routing Information Protocol (RIP)

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

What is Static Route

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

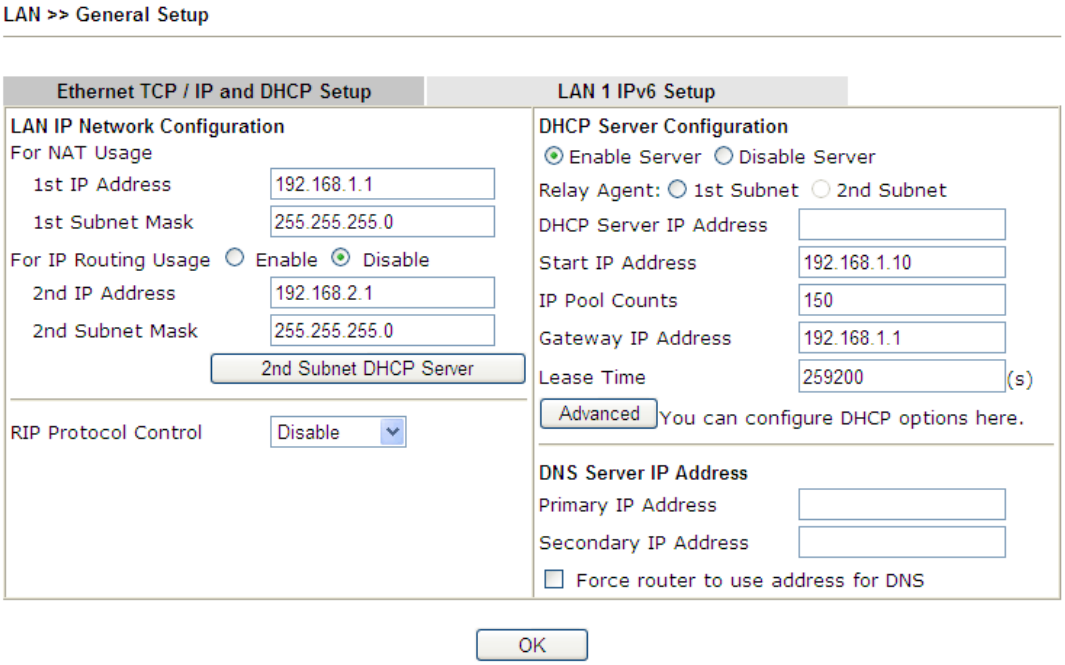


3.2.2 General Setup

This page provides you the general settings for LAN. Open **LAN>>General Setup**.

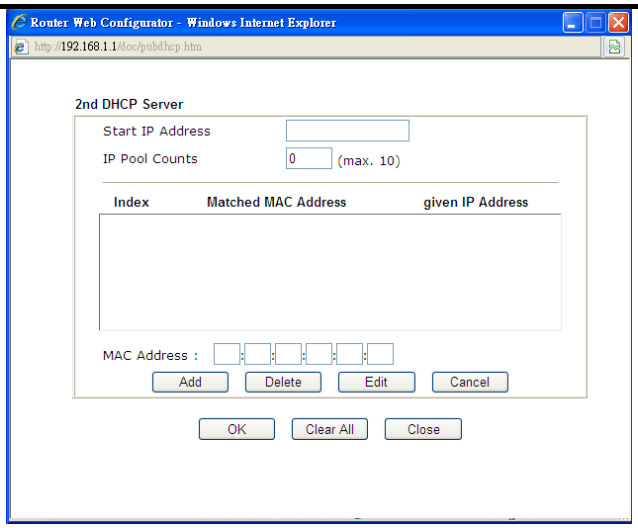
Details Page for LAN1 – Ethernet TCP/IP and DHCP Setup

There are two configuration pages for LAN1, Ethernet TCP/IP and DHCP Setup (based on IPv4) and IPv6 Setup. Click the tab for each type and refer to the following explanations for detailed information.



Available settings are explained as follows:

Item	Description
LAN IP Network Configuration	**For NAT Usage,** **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 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 Subnet DHCP Server** - You can configure the modem 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 modem 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 modem 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 modem 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,

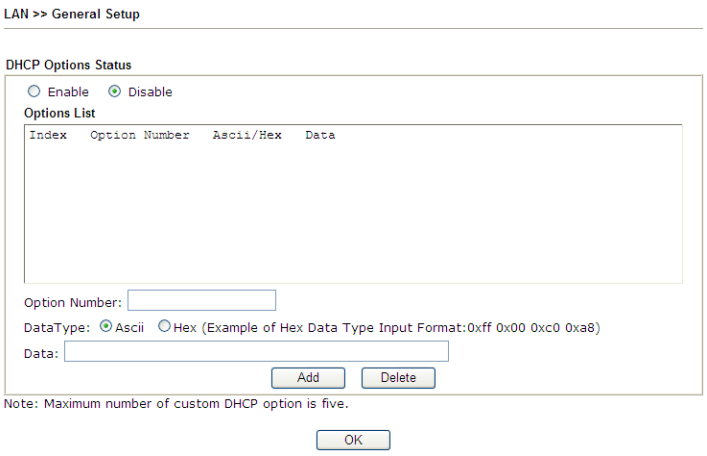
Disable - deactivate the RIP protocol. It will lead to a stoppage of the exchange of routing information between modems. (Default)

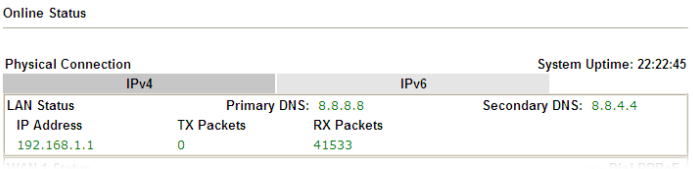
- **1st Subnet -** Select the modem to change the RIP information of the 1st subnet with neighboring modems.
- **2nd Subnet -** Select the modem to change the RIP information of the 2nd subnet with neighboring modems.

DHCP Server Configuration

DHCP stands for Dynamic Host Configuration Protocol. The modem 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 modem 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

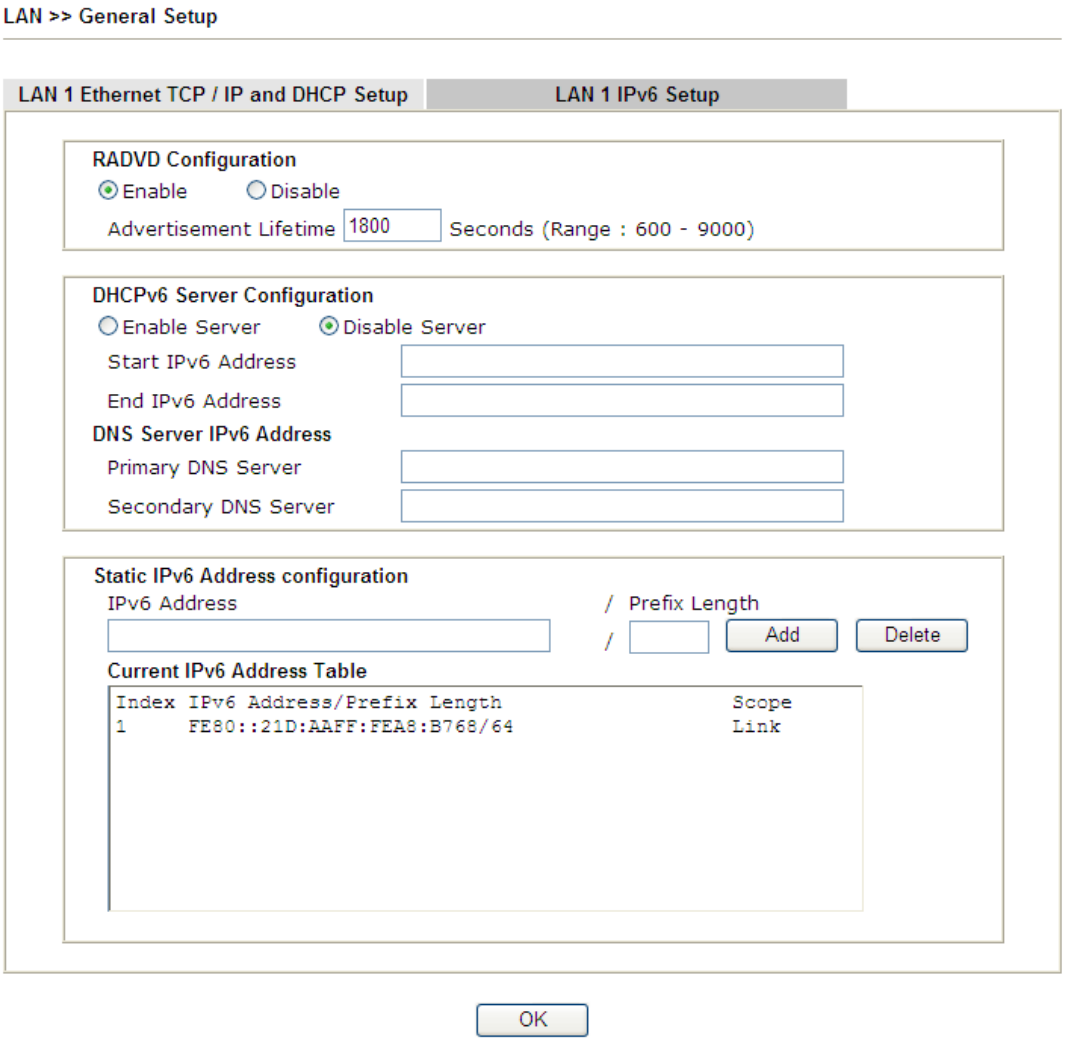
	you to redirect the DHCP request to the specified location. **Enable Server -** Let the modem assign IP address to every host in the LAN. **Disable Server –** Let you manually assign IP address to every host in the LAN. **Relay Agent – (1st subnet/2nd subnet)** Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to. **DHCP Server IP Address –**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. **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 modem 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 modem, which means the modem is the default gateway. **Lease Time –** Enter the time to determine how long the IP address assigned by DHCP server can be used. – If required, click it to set option number for DHCP.
Advanced	DHCP packets can be processed by adding option number and data information when such function is enabled.  **Enable/Disable** – Enable/Disable the function of DHCP Option. This modem allows you to add up to five Option Numbers. Each DHCP option is composed by an option number with data. For example, Option number:100 Data: abcd When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets. **Option Number** – Type a number for such function.

	Different number means different meaning. Please contact with your ISP for obtaining the correct number value. **DataType** – Choose the type (ASCII or Hex) for the data to be calculated. **Data** – Type the content of the data to be processed by the function of DHCP option.
DNS Server IP Address	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. **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 modem 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 modem 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 modem 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 modem will resolve the domain name immediately. Otherwise, the modem forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection. **Force router to use address for DNS**- Force Vigor modem to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).

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

Details Page for LAN1 – IPv6 Setup

There are two configuration pages for LAN1, Ethernet TCP/IP and DHCP Setup (based on IPv4) and IPv6 Setup. Click the tab for each type and refer to the following explanations for detailed information. Below shows the settings page for IPv6.



It provides 2 daemons for LAN side IPv6 address configuration. One is **RADVD**(stateless) and the other is **DHCPv6 Server** (Stateful).

Available settings are explained as follows:

Item	Description
RADVD Configuration	**Enable** – Click it to enable RADVD server. The modem advertisement daemon (radvd) sends Router Advertisement messages, specified by RFC 2461, to a local Ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless auto-configuration. **Disable** – Click it to disable RADVD server. **Advertisement Lifetime** - The lifetime associated with the default modem in units of seconds. It's used to control the lifetime of the prefix. The maximum value corresponds to 18.2 hours. A lifetime of 0 indicates that the modem is not a default modem and should not appear on the default modem list.
DHCPv6 Server Configuration	**Enable Server** –Click it to enable DHCPv6 server. DHCPv6 Server could assign IPv6 address to PC according to the Start/End IPv6 address configuration.

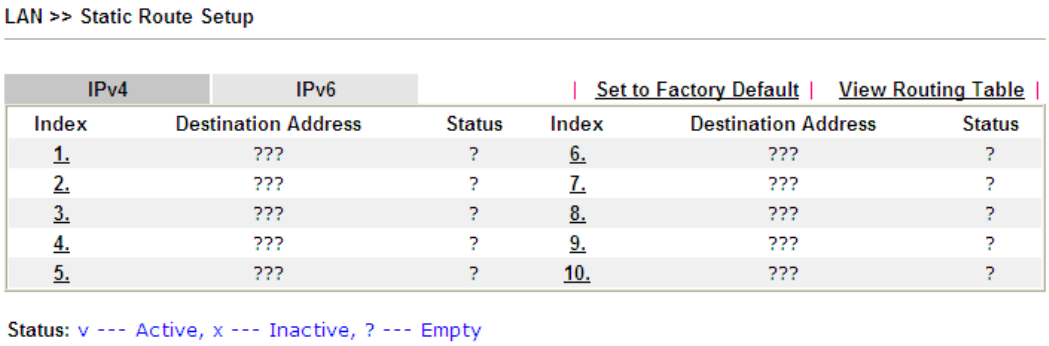
	Disable Server –Click it to disable DHCPv6 server. **Start IPv6 Address** / **End IPv6 Address** –Type the start and end address for IPv6 server.
DNS Server IPv6 Address	**Primary DNS Sever** – Type the IPv6 address for Primary DNS server. **Secondary DNS Server** –Type another IPv6 address for DNS server if required.
Static IPv6 Address configuration	**IPv6 Address** –Type static IPv6 address for LAN. **Prefix Length –** Type the fixed value for prefix length. **Add –** Click it to add a new entry. **Delete –** Click it to remove an existed entry.
Current IPv6 Address Table	Display current used IPv6 addresses.

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

3.2.3 Static Route

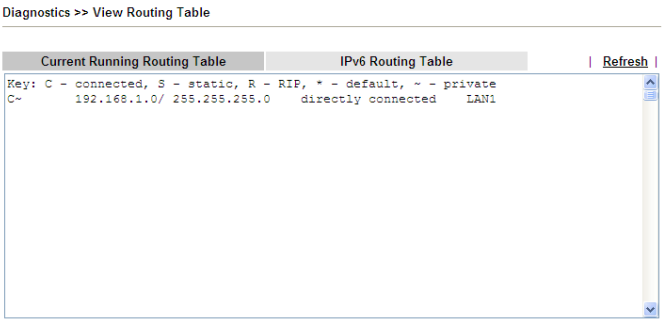
Go to **LAN** to open setting page and choose **Static Route**. The modem offers IPv4 and IPv6 for you to configure the static route. Both protocols bring different web pages.

Static Route for IPv4



Available settings are explained as follows:

Item	Description
Index	The number (1 to 10) under Index allows you to open next page to set up static route.
Destination Address	Displays the destination address of the static route.
Status	Displays the status of the static route.
Set to Factory Default	Clear all of the settings and return to factory default settings.

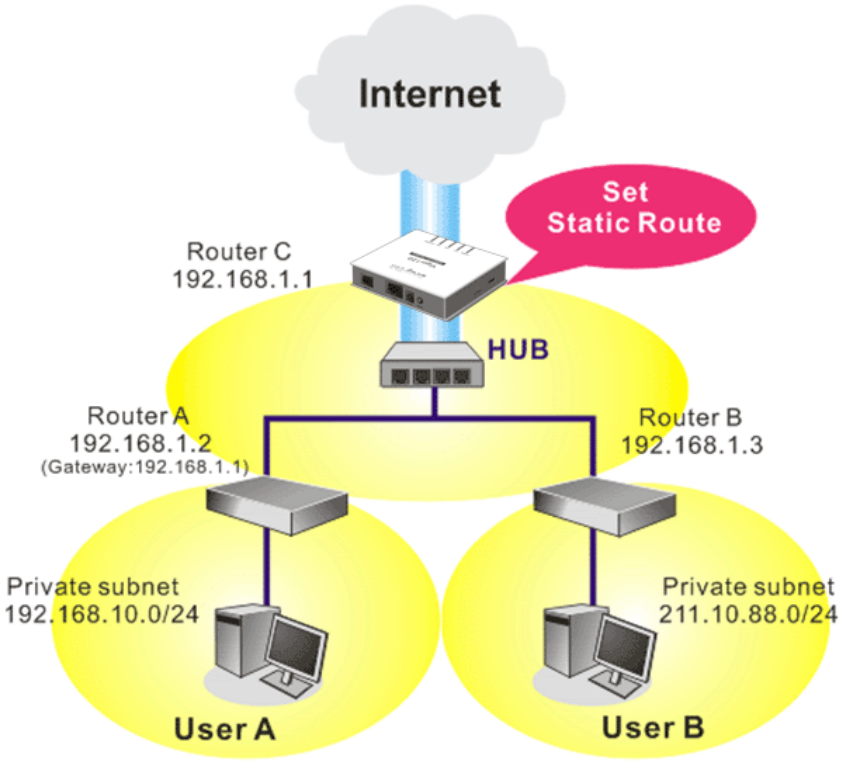
Viewing Routing Table	Displays the routing table for your reference. 

Add Static Routes to Private and Public Networks (based on IPv4)

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

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

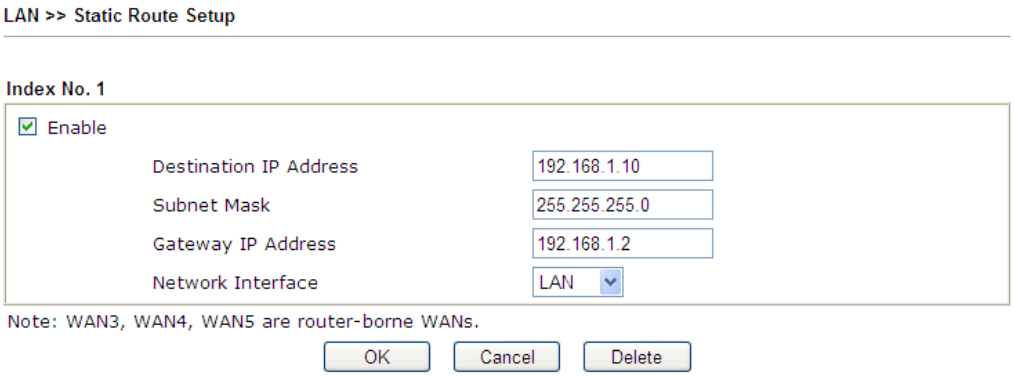
Before setting Static Route, user A cannot talk to user B for Modem A can only forward recognized packets to its default gateway Main Modem.



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 modems 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 modem, and continuously exchange of IP routing information with different subnets.

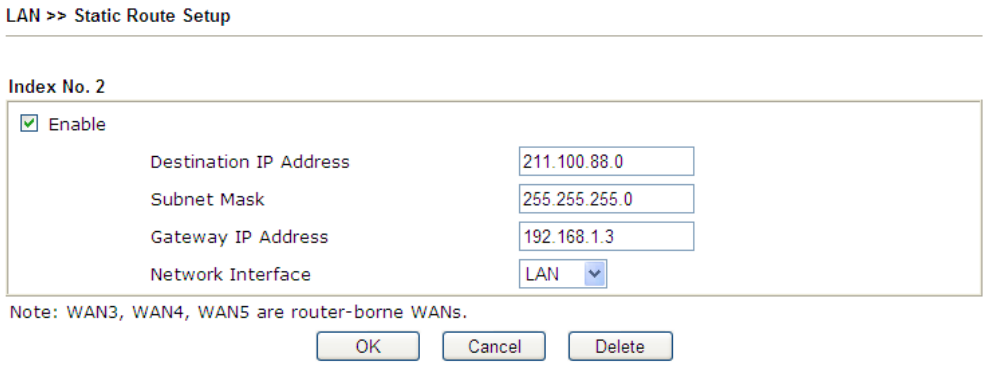
2. Click the **LAN - Static Route** and click on the **Index Number 1.** Check the **Enable** box. Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click **OK**.



Available settings are explained as follows:

Item	Description
Enable	Click it to enable this profile.
Destination IP Address	Type an IP address as the destination of such static route.
Subnet Mask	Type the subnet mask for such static route.
Network Interface	Use the drop down list to specify an interface for such static route.

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.

Diagnostics >> View Routing Table

Current Running Routing Table | IPv6 Routing Table | Refresh |

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
S~      192.168.10.0/ 255.255.255.0    via 192.168.1.2       LAN1
C~       192.168.1.0/ 255.255.255.0    directly connected    LAN1
S~      211.100.88.0/ 255.255.255.0    via 192.168.1.3       LAN1
```

Static Route for IPv6

You can set up to 40 profiles for IPv6 static route. Click the IPv6 tab to open the following page:

LAN >> Static Route Setup

IPv4 | IPv6 | Set to Factory Default | View IPv6 Routing Table |

Index	Destination Address	Status	Index	Destination Address	Status
1.	::/0	x	11.	::/0	x
2.	::/0	x	12.	::/0	x
3.	::/0	x	13.	::/0	x
4.	::/0	x	14.	::/0	x
5.	::/0	x	15.	::/0	x
6.	::/0	x	16.	::/0	x
7.	::/0	x	17.	::/0	x
8.	::/0	x	18.	::/0	x
9.	::/0	x	19.	::/0	x
10.	::/0	x	20.	::/0	x

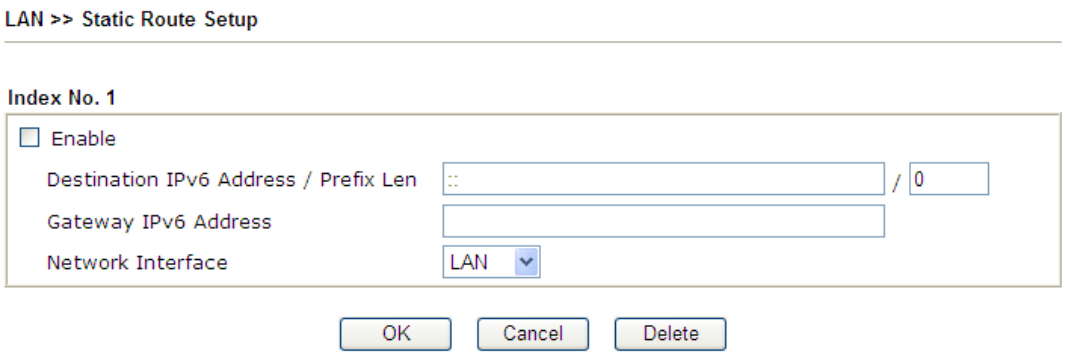
<< 1 - 20 | 21 - 40 >> Next >>

Status: v --- Active, x --- Inactive, ? --- Empty

Available settings are explained as follows:

Item	Description
Index	The number (1 to 40) under Index allows you to open next page to set up static route.
Destination Address	Displays the destination address of the static route.
Status	Displays the status of the static route.
Set to Factory Default	Clear all of the settings and return to factory default settings.
Viewing IPv6 Routing Table	Displays the routing table for your reference.

Click any underline of index number to get the following page.



Available settings are explained as follows:

Item	Description
Enable	Click it to enable this profile.
Destination IPv6 Address / Prefix Len	Type the IP address with the prefix length for this entry.
Gateway IPv6 Address	Type the gateway address for this entry.
Network Interface	Use the drop down list to specify an interface for this static route. 

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

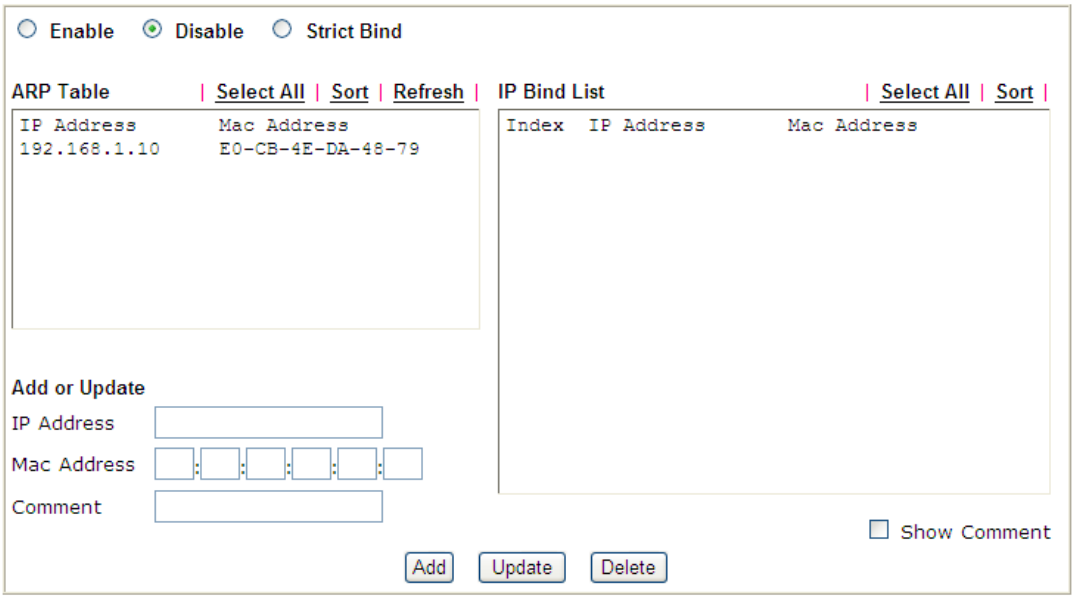
3.2.4 Bind IP to MAC

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

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

LAN >> Bind IP to MAC

Bind IP to MAC



Note: IP-MAC binding presets DHCP Allocations.
If you select Strict Bind, unspecified LAN clients cannot access the Internet.

OK

Available settings are explained as follows:

Item	Description
Enable	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
Disable	Click this radio button to disable this function. All the settings on this page will be invalid.
Strict Bind	Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List.
ARP Table	This table is the LAN ARP table of this modem. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking **Add** below.
Select All	Click this link to select all the items in the ARP table.
Sort	Reorder the table based on the IP address.
Refresh	Refresh the ARP table listed below to obtain the newest ARP table information.
Add 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. **Comment** – Type a brief description for the entry. **Show Comment** – Check this box to display the comment on IP Bind List box.
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 or Update** to the table of **IP Bind List**.
Update	It allows you to edit and modify the selected IP address and MAC address that you create before.
Delete	You can remove any item listed in **IP Bind List**. Simply click and select the one, and click **Delete**. The selected item will be removed from the **IP Bind List**.

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

When you finish the configuration, click **OK** to save the settings.

3.3 NAT

Usually, the modem serves as an NAT (Network Address Translation) modem. 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 modem, the modem will change its source address into the public IP address of the modem, select the available public port, and then forward it. At the same time, the modem 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 modem's public IP address and the modem will do the inversion based on its table. Therefore, the internal host can communicate with external host smoothly.

The benefit of the NAT includes:

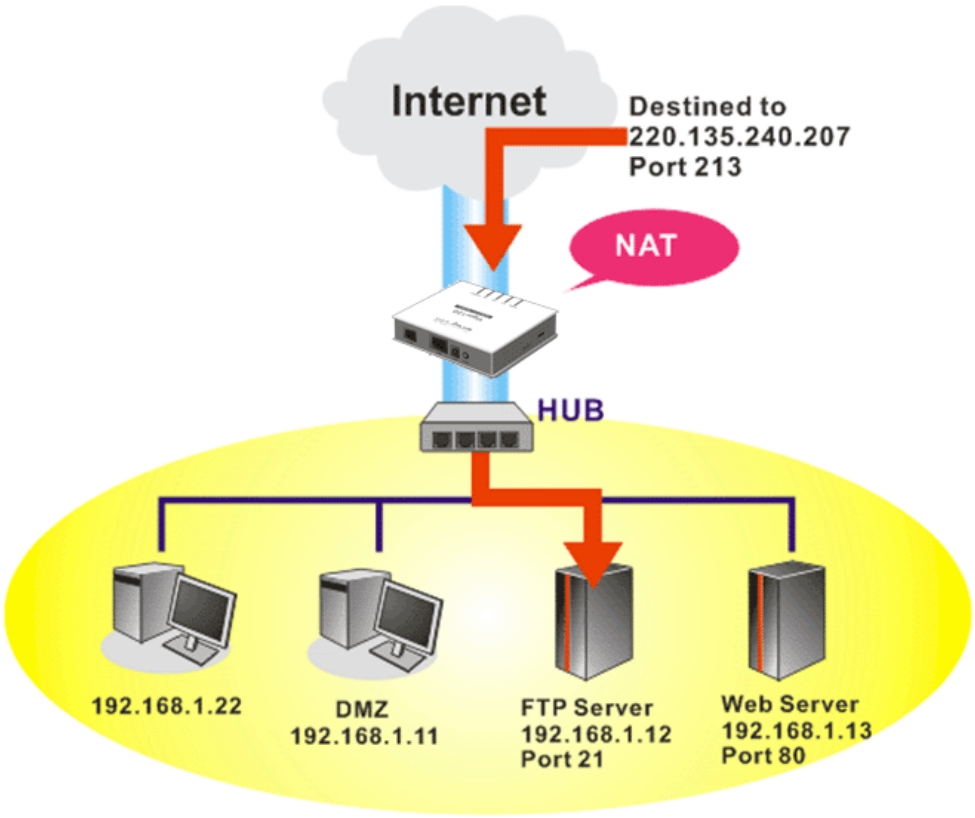
- **Save cost on applying public IP address and apply efficient usage of IP address.** NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- **Enhance security of the internal network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

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

Below shows the menu items for NAT.

3.3.1 Port Redirection

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



The port redirection can only apply to incoming traffic.

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

NAT >> Port Redirection

Port Redirection | Set to Factory Default |

Index	Service Name	WAN Interface	Protocol	Public Port	Private IP	Status
1.		All				x
2.		All				x
3.		All				x
4.		All				x
5.		All				x
6.		All				x
7.		All				x
8.		All				x
9.		All				x
10.		All				x

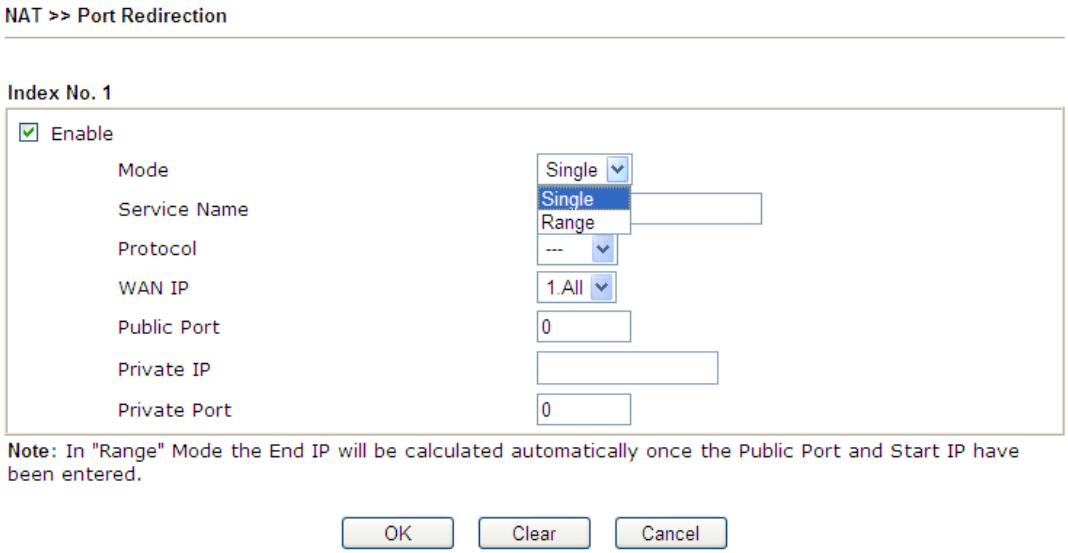
<< 1-10 | 11-20 >> Next >>

Each item is explained as follows:

Item	Description
Index	Display the number of the profile.
Service Name	Display the description of the specific network service.
WAN Interface	Display the WAN IP address or interface used by the profile.

Protocol	Display the transport layer protocol (TCP or UDP).
Public Port	Display the port number which will be redirected to the specified **Private IP and Port** of the internal host.
Private IP	Display the IP address of the internal host providing the service.
Status	Display if the profile is enabled (v) or not (x).

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



Available settings are explained as follows:

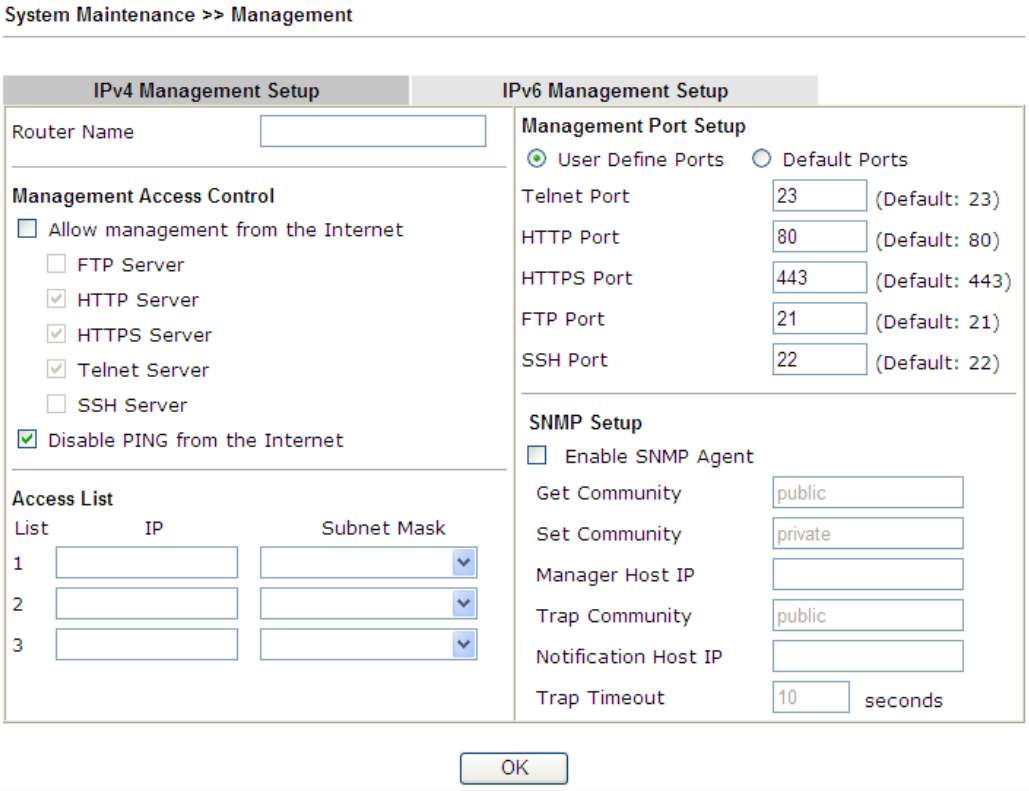
Item	Description
Enable	Check this box to enable such port redirection setting.
Mode	Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select **Range**. In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.
Service Name	Enter the description of the specific network service.
Protocol	Select the transport layer protocol (TCP or UDP).
WAN IP	Select the WAN IP used for port redirection. There are eight WAN IP alias that can be selected and used for port redirection. The default setting is **All** which means all the incoming data from any port will be redirected to specified range of IP address and port.
Public Port	Specify which port can be redirected to the specified **Private IP and Port** of the internal host. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Simply type the required number on the first box. The second one will be assigned automatically later.

Private IP	Specify the private IP address of the internal host providing the service. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point) and the fourth digits in the second box (as the end point).
Private Port	Specify the private port number of the service offered by the internal host.

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

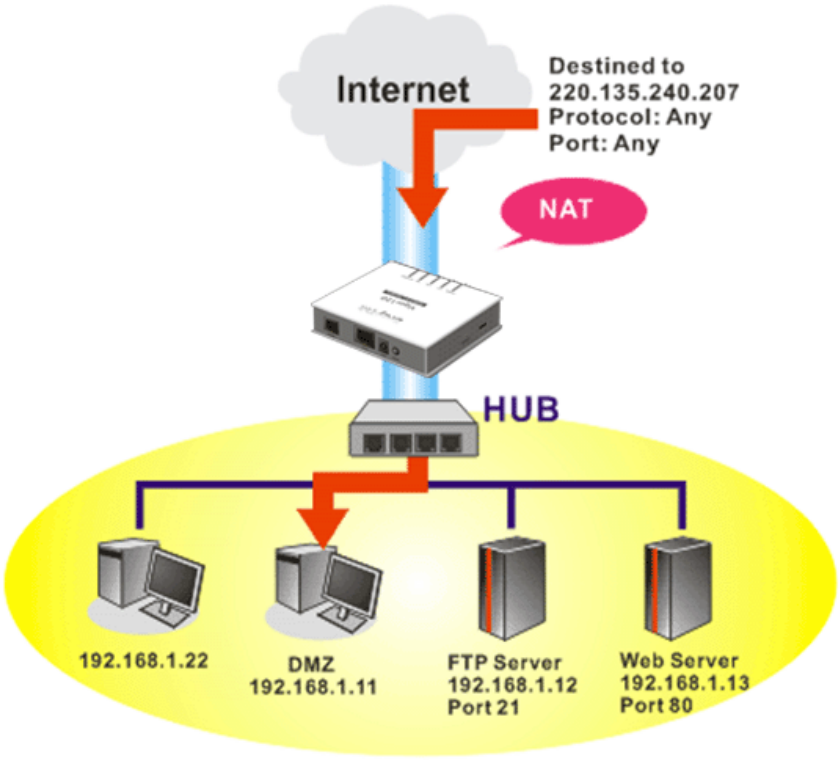
Note that the modem has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the modem in order to avoid confliction.

For example, the built-in Web User Interface in the modem 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 modem's http port to any one other than the default port 80** to avoid conflict, such as 8080. This can be set in the **System Maintenance >>Management Setup**. You then will access the admin screen of by suffixing the IP address with 8080, e.g., http://192.168.1.1:8080 instead of port 80.



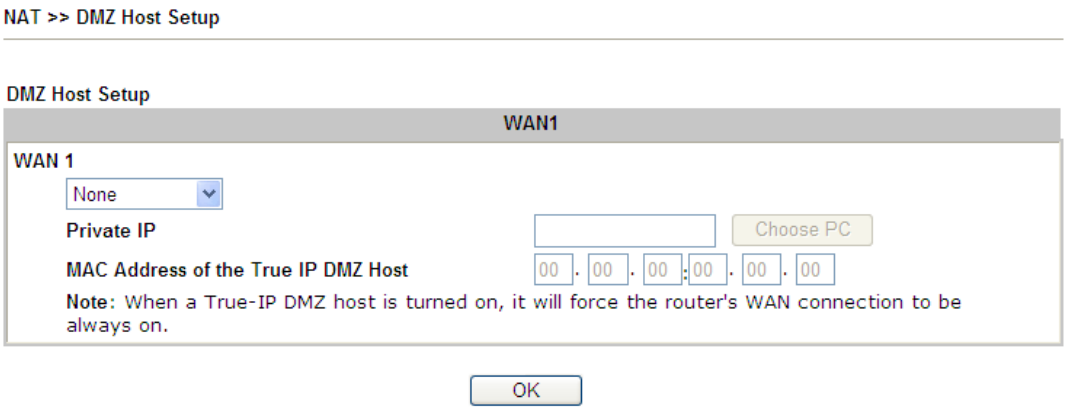
3.3.2 DMZ Host

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



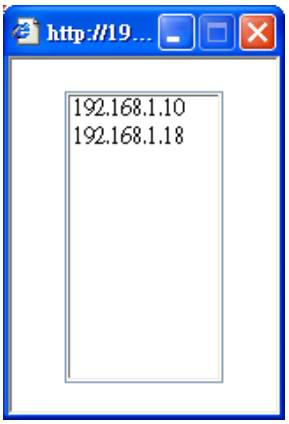
The inherent security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

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



Available settings are explained as follows:

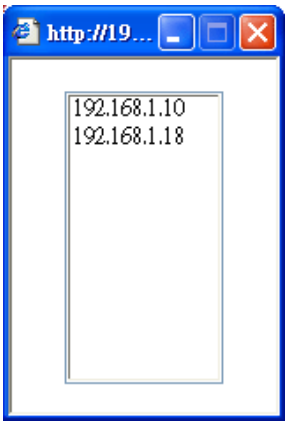
Item	Description
WAN 1 None None Private IP Active True IP	Choose **Private IP** or **Active True IP** first. **Active True IP** selection is available for WAN1 only.
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.
Choose PC	Click this button and then a window will automatically pop

	up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.  When you have selected one private IP from the above dialog, the IP address will be shown on the following screen. Click **OK** to save the setting.

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

Available settings are explained as follows:

Item	Description
Enable	Check to enable the DMZ Host function.
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.

Choose PC	Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.  When you have selected one private IP from the above dialog, the IP address will be shown on the following screen. Click **OK** to save the setting.

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

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:

NAT >> Open Ports

Open Ports Setup | Set to Factory Default |

Index	Comment	WAN Interface	Aux. WAN IP	Local IP Address	Status
1.					x
2.					x
3.					x
4.					x
5.					x
6.					x
7.					x
8.					x
9.					x
10.					x

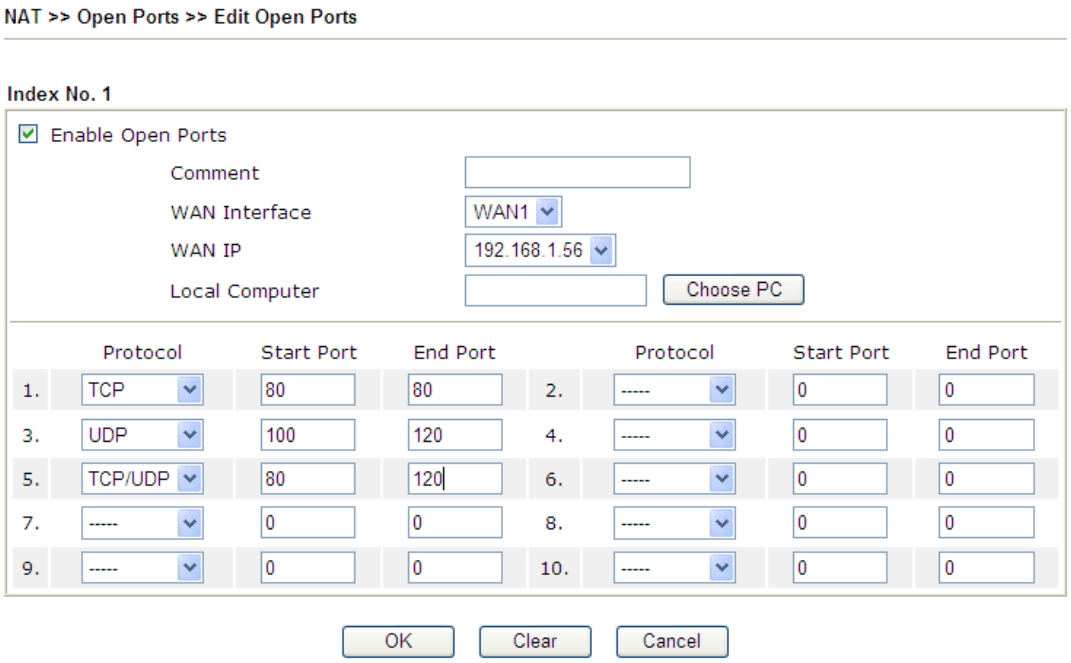
<< 1-10 | 11-20 >> Next >>

Available settings are explained as follows:

Item	Description
Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.

Comment	Specify the name for the defined network service.
WAN Interface	Display the WAN interface used by such index.
Aux. WAN IP	Display the IP address defined in **WAN Alias** for **PPPoE/PPPoA** or **MPoA** mode.
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.



Available settings are explained as follows:

Item	Description
Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
WAN Interface	Specify the WAN interface that will be used for this entry.
WAN IP	Specify the WAN IP address that will be used for this entry. This setting is available when WAN IP Alias is configured.
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.

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

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 modem 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 modem to build an unwanted outgoing connection.

Firewall Facilities

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

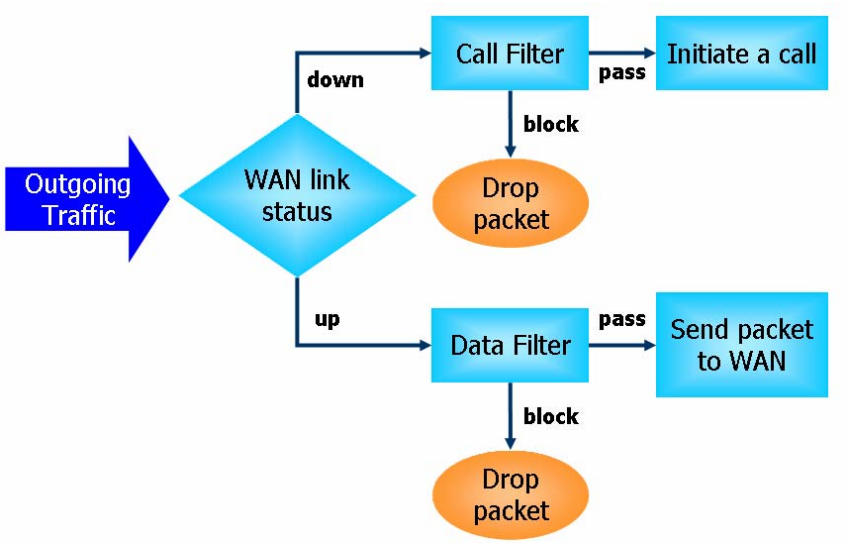
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

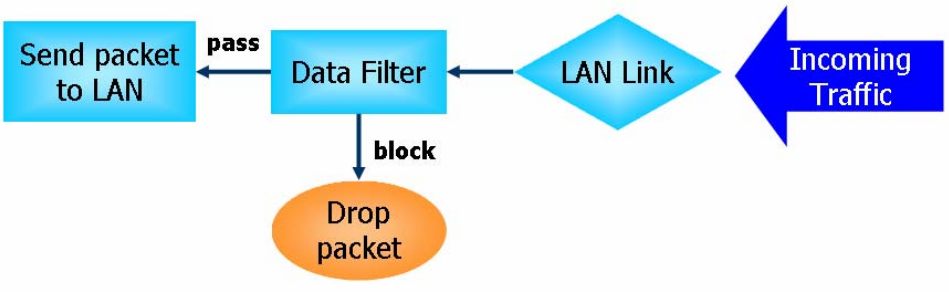
IP Filters

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 modem 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 modem.

The following illustrations are flow charts explaining how modem 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 modem not just examine the header information also monitor the state of the connection.

URL Content Filter

To provide an appropriate cyberspace to users, Vigor modem 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 modem 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.

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.

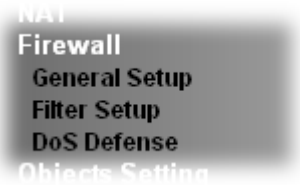
The **DoS Defense** function enables the Vigor modem to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog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

Also the Vigor modem 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 modem 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. Port Scan attack
5. IP options
6. Land attack
7. Smurf attack
8. Trace route
9. SYN fragment
10. Fraggle attack
11. TCP flag scan
12. Tear drop attack
13. Ping of Death attack
14. ICMP fragment
15. Unknown protocol

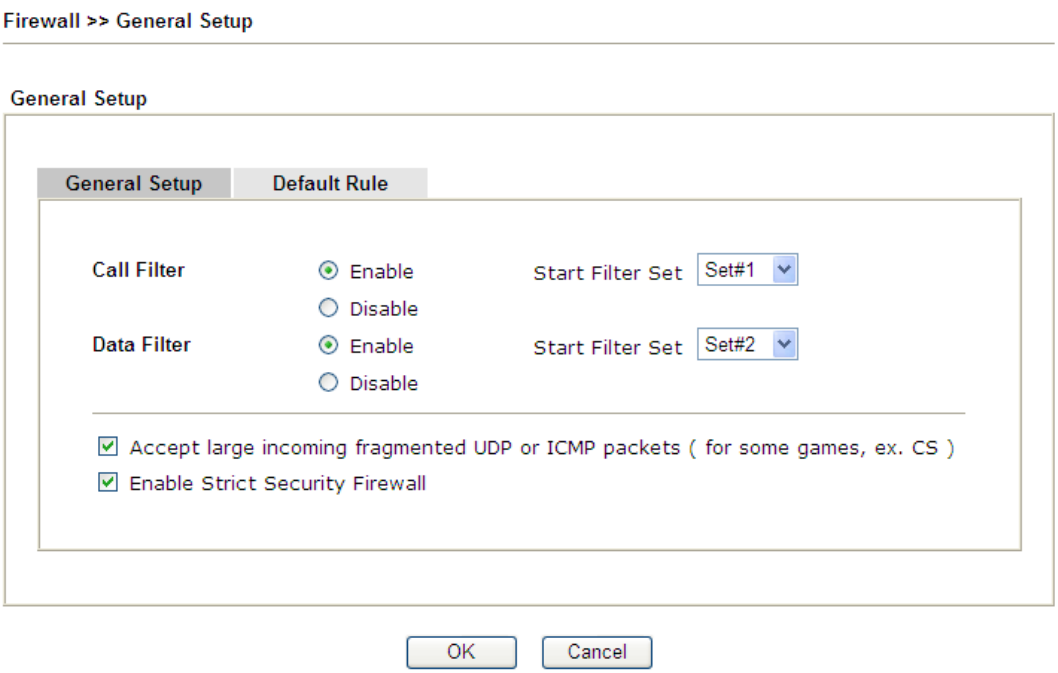
Below shows the menu items for Firewall.



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, **Apply IP filter to VPN incoming packets**, and **Accept incoming fragmented UDP packets**.

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

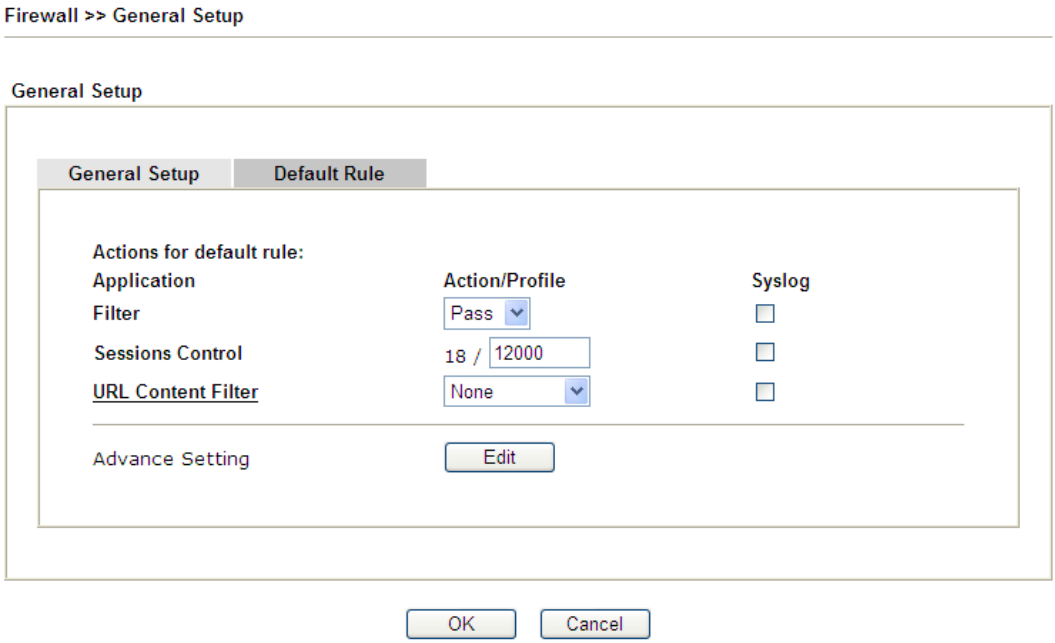


Available settings are explained as follows:

Item	Description
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.
Accept large incoming…	Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor modem will reject these fragmented packets to prevent attack unless you enable "**Accept large incoming fragmented UDP or ICMP Packets**". By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable "**Accept large incoming fragmented UDP or ICMP Packets**".
Enable Strict Security Firewall	For the sake of security, the modem will execute strict security checking for data transmission. Such feature is enabled in default. All the packets, while transmitting through Vigor modem, will be filtered by firewall. If the firewall system (e.g., content filter server) does not make any response (pass or block) for these packets, then the modem's firewall will block the packets directly.

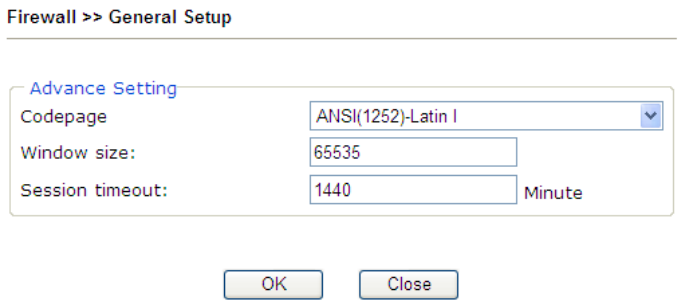
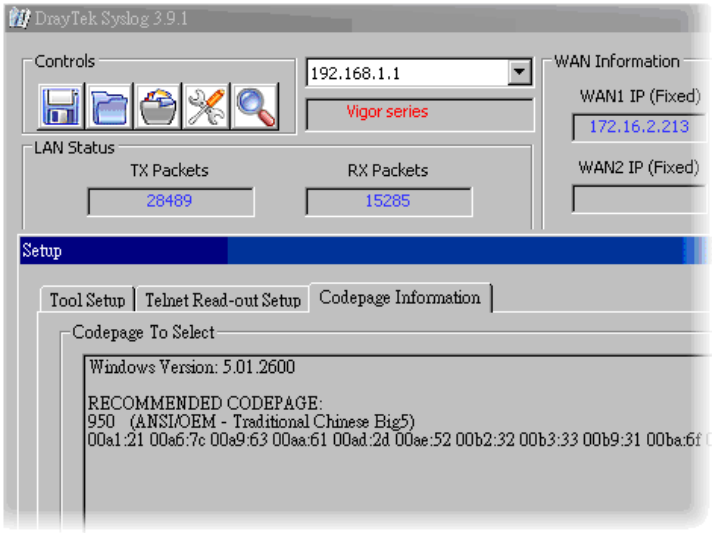
Default Rule Page

Such page allows you to choose filtering profiles including QoS, Load-Balance policy, WCF, APP Enforcement, URL Content Filter, for data transmission via Vigor modem.



Available settings are explained as follows:

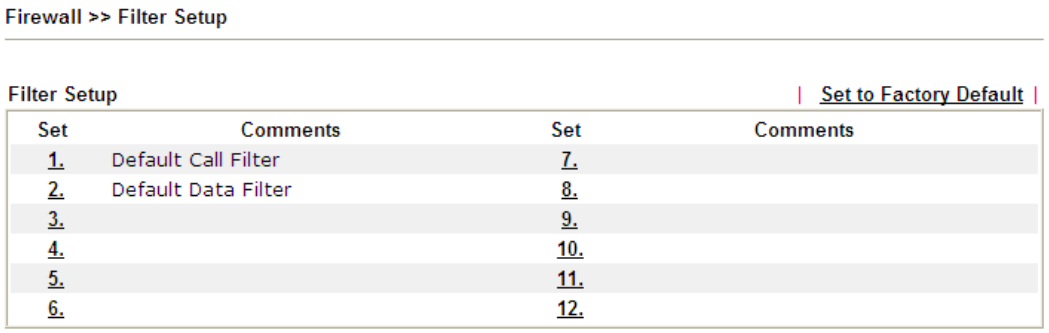
Item	Description
Filter	Select **Pass** or **Block** for the packets that do not match with the filter rules. Filter Pass (Pass / Block)
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.
URL Content Filter	Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this modem. Please set at least one profile for choosing in **CSM>> URL Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.

Advance Setting	Click **Edit** to open the following window. However, it is **strongly recommended** to use the default settings here.  **Codepage** - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage. If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.  **Window size** – It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper. **Session timeout** – Setting timeout for sessions can make the best utilization of network resources.

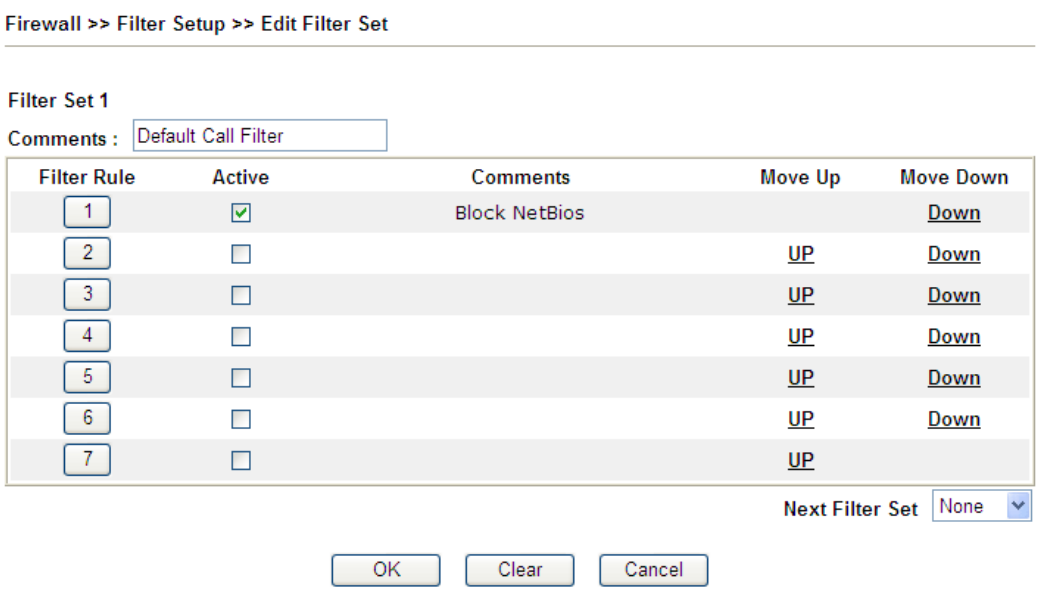
After finishing all the settings here, please click **OK** to save the configuration.

3.4.3 Filter Setup

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



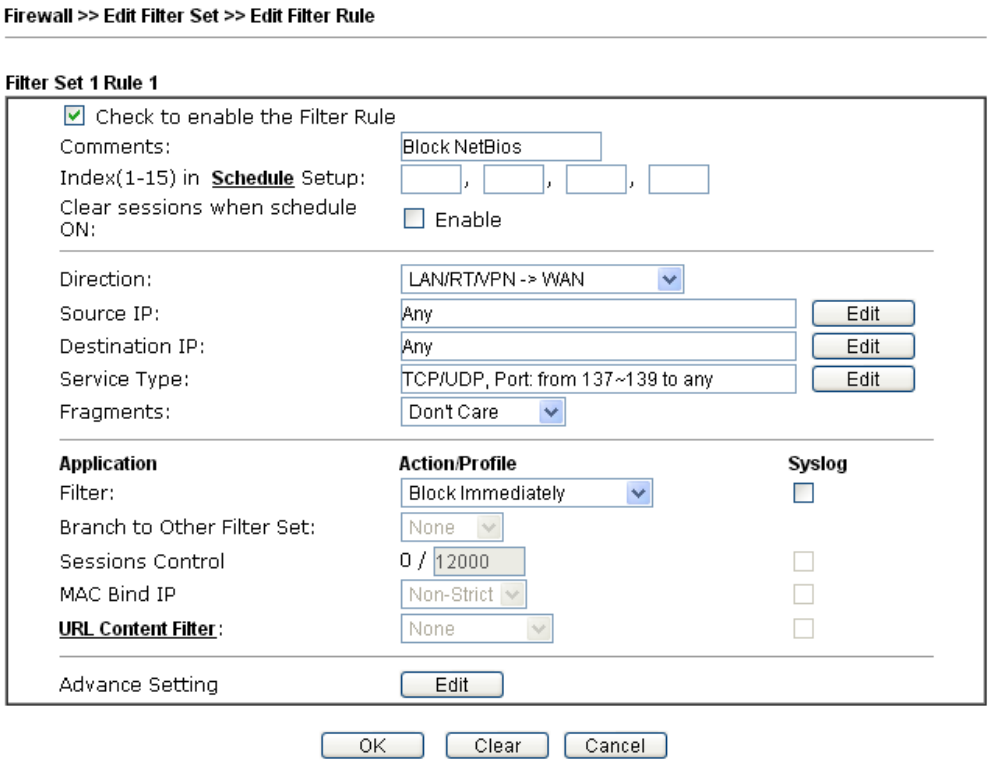
To edit or add a filter, click on the set number to edit the individual set. The following page will be shown. Each filter set contains up to 7 rules. Click on the rule number button to edit each rule. Check **Active** to enable the rule.



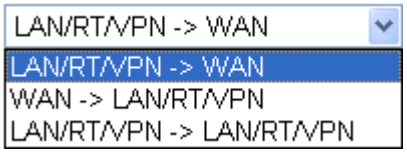
Available settings are explained as follows:

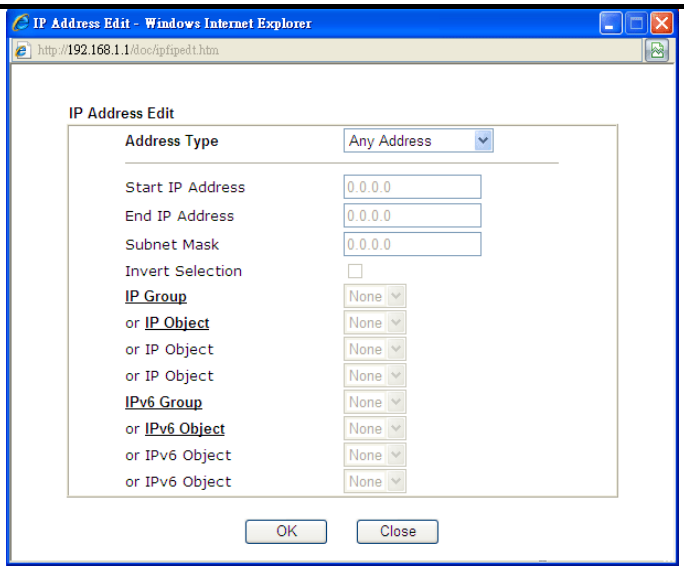
Item	Description
Filter Rule	Click a button numbered (1 ~ 7) to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.
Active	Enable or disable the filter rule.
Comment	Enter filter set comments/description. Maximum length is 23–character long.
Move Up/Down	Use **Up** or **Down** link to move the order of the filter rules.
Next Filter Set	Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.

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

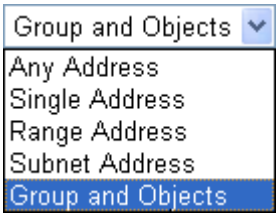


Available settings are explained as follows:

Item	Description
Check to enable the Filter Rule	Check this box to enable the filter rule.
Comments	Enter filter set comments/description. Maximum length is 14- character long.
Index(1-15)	Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications** >> **Schedule** setup. The default setting of this field is blank and the function will always work.
Clear sessions when schedule ON	Check this box to clear the sessions when the above schedule profiles are applied.
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.  **Note:** RT means routing domain for 2nd subnet or other LAN.
Source/Destination IP	Click **Edit** to access into the following dialog to choose the source/destination IP or IP ranges.



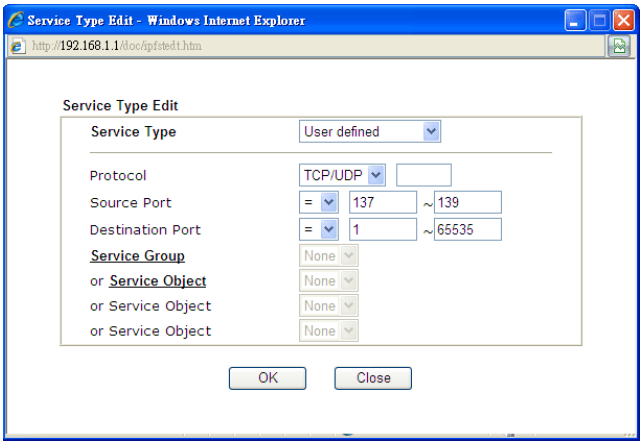
To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.



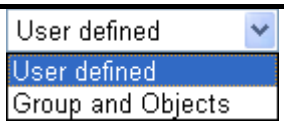
From the **IP Group** drop down list, choose the one that you want to apply. Or use the **IP Object** drop down list to choose the object that you want.

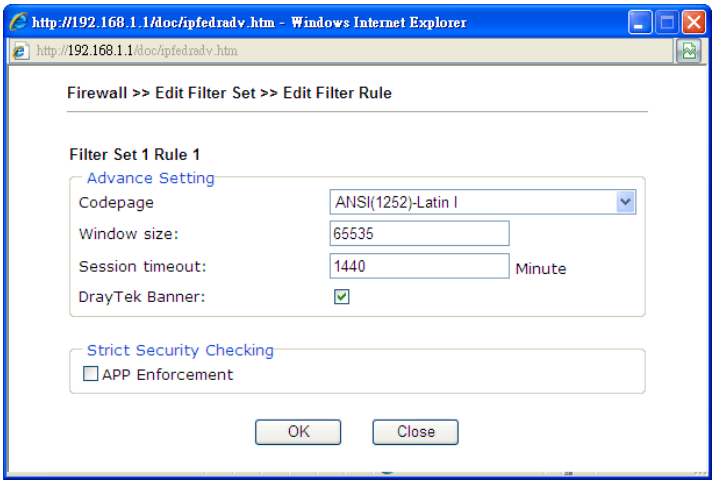
Service Type

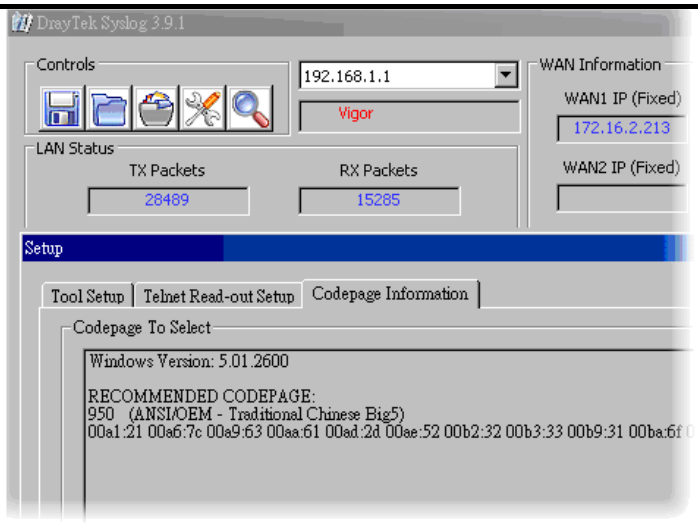
Click **Edit** to access into the following dialog to choose a suitable service type.



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

	 **Protocol -** Specify the protocol(s) which this filter rule will apply to. **Source/Destination Port –** ***(=)*** – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type. ***(!=)*** – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type. ***(>)*** – the port number greater than this value is available. ***(<)*** – the port number less than this value is available for this profile. **Service Group/Object** - Use the drop down list to choose the one that you want.
Fragments	Specify the action for fragmented packets. And it is used for **Data Filter** only. ***Don't care*** **-**No action will be taken towards fragmented packets. ***Unfragmented*** **-**Apply the rule to unfragmented packets. ***Fragmented*** **-** Apply the rule to fragmented packets. ***Too Short*** **-** Apply the rule only to packets that are too short to contain a complete header.
Filter	Specifies the action to be taken when packets match the rule. **Block Immediately -** Packets matching the rule will be dropped immediately. **Pass Immediately -** Packets matching the rule will be passed immediately. **Block If No Further Match -** A packet matching the rule, and that does not match further rules, will be dropped. **Pass If No Further Match -** A packet matching the rule, and that does not match further rules, will be passed through.
Branch to other Filter 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. Be aware that the modem will apply the specified filter rule for ever and will not return to previous filter rule any more.
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.
MAC Bind IP	**Strict** – Make the MAC address and IP address settings configured in **IP Object** for **Source IP** and **Destination IP**

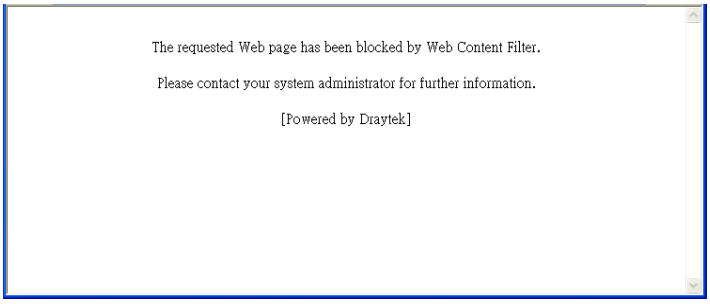
	be bound for applying such filter rule. **No-Strict -** no limitation.
URL Content Filter	Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this modem. Please set at least one profile for choosing in **CSM>> URL Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
Advance Setting	Click **Edit** to open the following window. However, it is **strongly recommended** to use the default settings here.  **Codepage** - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage. If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.



Window size – It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.

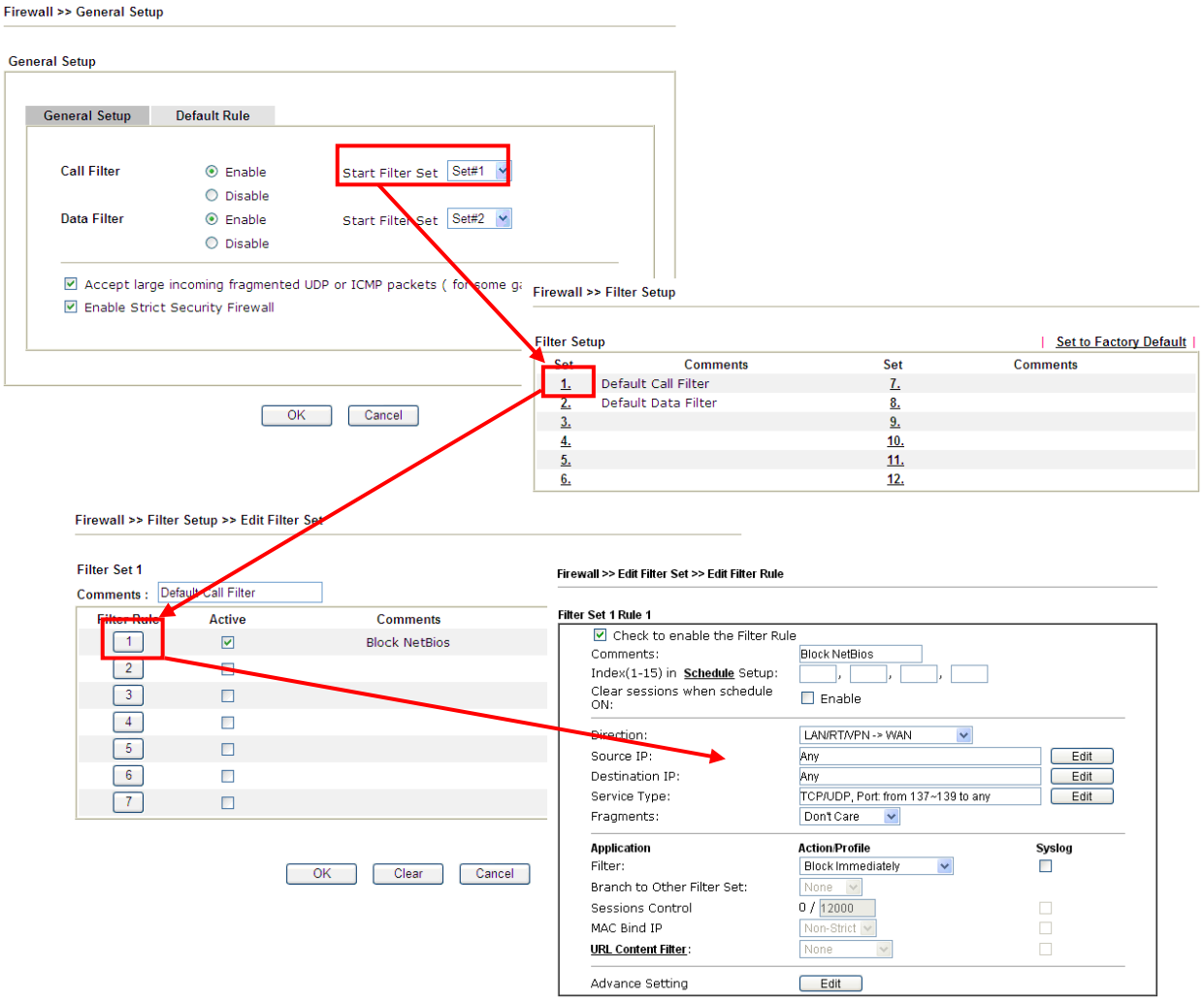
Session timeout–Setting timeout for sessions can make the best utilization of network resources. However, Queue timeout is configured for TCP protocol only; session timeout is configured for the data flow which matched with the firewall rule.

DrayTek Banner – Please uncheck this box and the following screen will not be shown for the unreachable web page. The default setting is Enabled.



Example

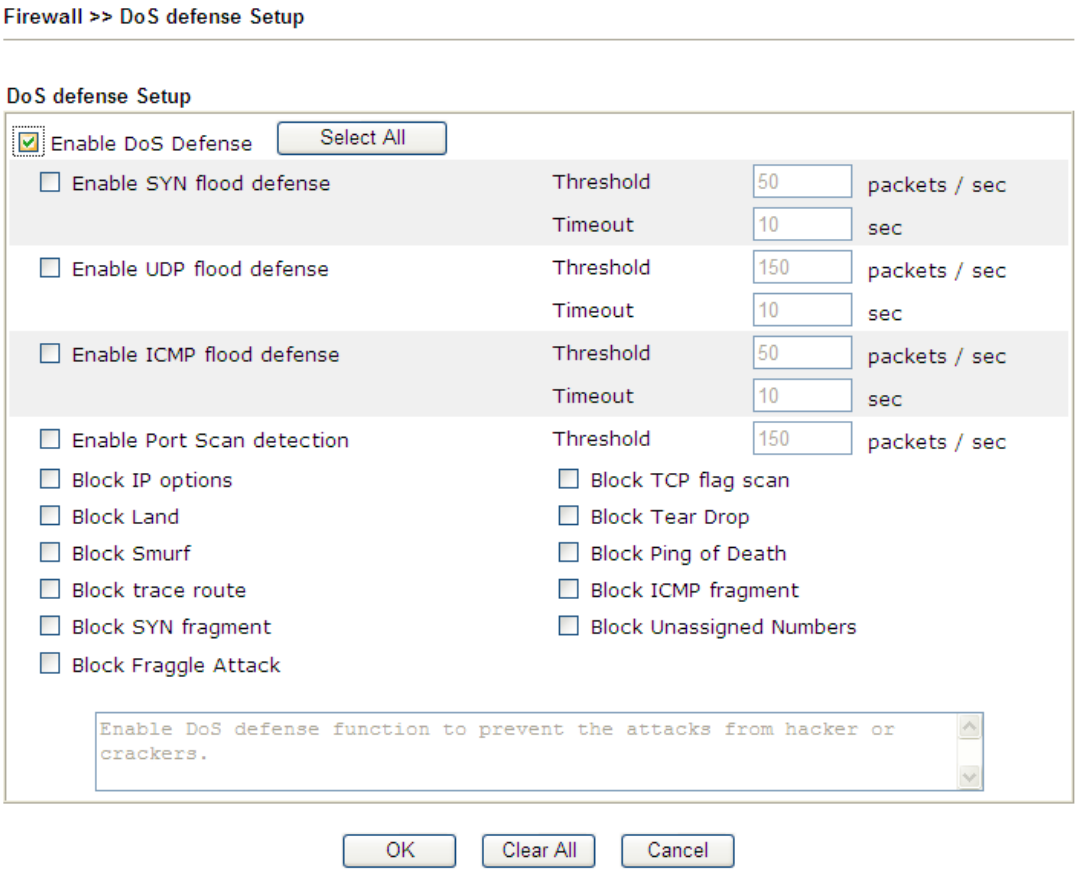
As stated before, all the traffic will be separated and arbitrated using on of two IP filters: call filter or data filter. You may preset 12 call filters and data filters in **Filter Setup** and even link them in a serial manner. Each filter set is composed by 7 filter rules, which can be further defined.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

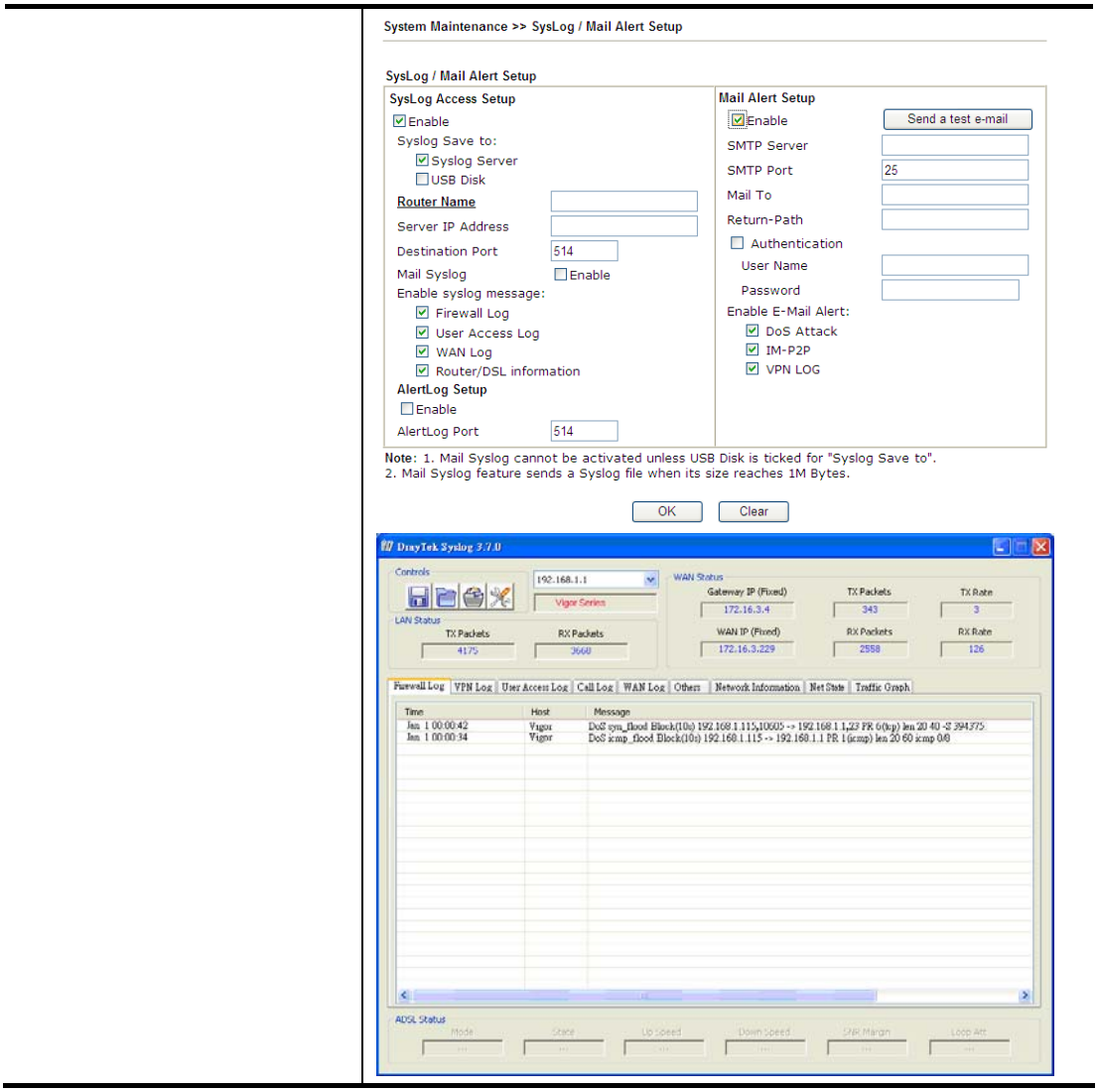


Available settings are explained as follows:

Item	Description
Enable Dos Defense	Check the box to activate the DoS Defense Functionality.
Select All	Click this button to select all the items listed below.
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 modem 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 modem. By default, the threshold and timeout values are set to 50 packets per second and 10 seconds, respectively. That means, when 50 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.
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 modem

	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. That means, when 150 packets per second received, they will be regarded as “attack event” and the session will be paused for 10 seconds.
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 modem 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. That means, when 50 packets per second received, they will be regarded as “attack event” and the session will be paused for 10 seconds.
Enable PortScan detection	Port Scan attacks the Vigor modem 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 modem will send out a warning. By default, the Vigor modem sets the threshold as 150 packets per second. That means, when 150 packets per second received, they will be regarded as “attack event”.
Block IP options	Check the box to activate the Block IP options function. The Vigor modem 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 modem 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 modem will ignore any broadcasting ICMP echo request.
Block trace router	Check the box to enforce the Vigor modem not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor modem 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 modem 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 modems 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 Unassigned Numbers	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 modem should have ability to detect and reject this kind of packets.
Warning Messages	We provide Syslog function for user to retrieve message from Vigor modem. The user, as a Syslog Server, shall receive the report sending from Vigor modem which is a Syslog Client. All the warning messages related to **DoS Defense** will be sent to user and user can review it through Syslog daemon. Look for the keyword **DoS** in the message, followed by a name to indicate what kind of attacks is detected.

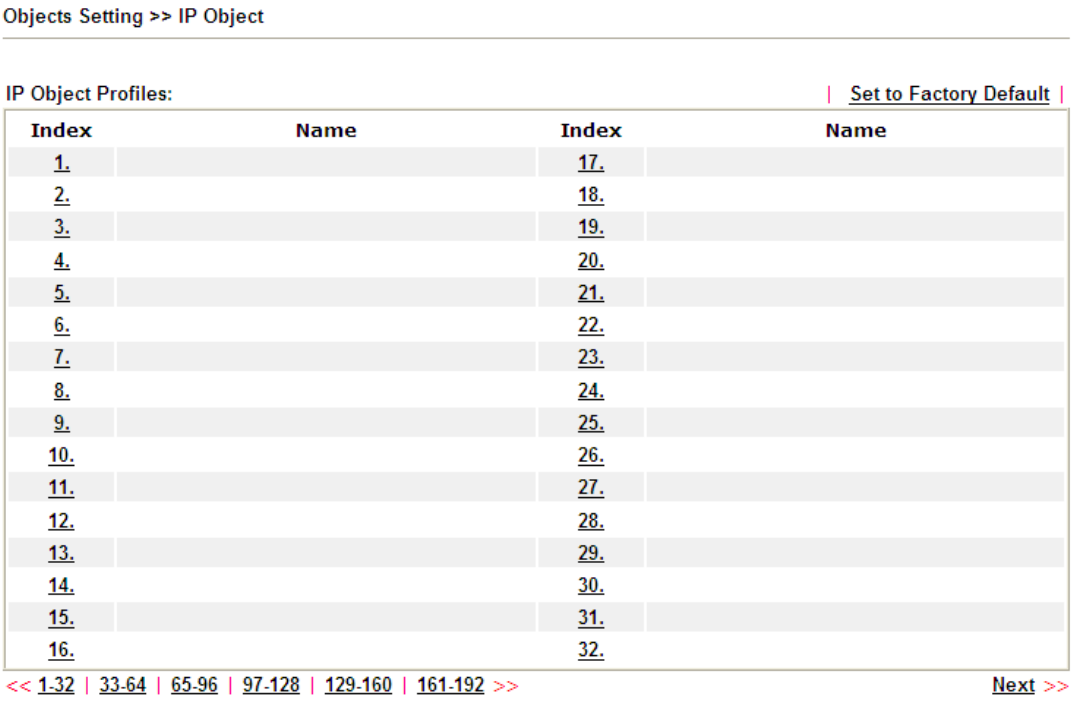

System Maintenance >> SysLog / Mail Alert Setup
SysLog / Mail Alert Setup
SysLog Access Setup
Enable
Syslog Save to:
Syslog Server
USB Disk
Router Name
Server IP Address
Destination Port
514
Mail Syslog
Enable
Enable syslog message:
Firewall Log
User Access Log
WAN Log
Router/DSL information
AlertLog Setup
Enable
AlertLog Port
514
Mail Alert Setup
Enable
Send a test e-mail
SMTP Server
SMTP Port
25
Mail To
Return-Path
Authentication
User Name
Password
Enable E-Mail Alert:
DoS Attack
IM-P2P
VPN LOG
Note: 1. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to".
2. Mail Syslog feature sends a Syslog file when its size reaches 1M Bytes.
OK
Clear
DrayTek Syslog 3.7.0
Controls
192.168.1.1
Vigor Series
WAN Status
Gateway IP (Fixed)
172.16.3.4
TX Packets
343
TX Rate
3
LAN Status
TX Packets
4175
RX Packets
3660
WAN IP (Fixed)
172.16.3.229
RX Packets
2558
RX Rate
126
Firewall Log
VPN Log
User Access Log
Call Log
WAN Log
Others
Network Information
Net State
Traffic Graph
Time
Host
Message
Jan 1 00:00:42
Vigor
DoS syn_flood Block(10s) 192.168.1.115,10605 -> 192.168.1.1,23 PR 6(tcp) len 20 40 -S 394375
Jan 1 00:00:34
Vigor
DoS icmp_flood Block(10s) 192.168.1.115 -> 192.168.1.1 PR 1(icmp) len 20 60 icmp 0/0
ADSL Status
Mode
State
Up Speed
Down Speed
SNR Margin
Loop Att

3.5 Objects Settings

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

3.5.1 IP Object

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



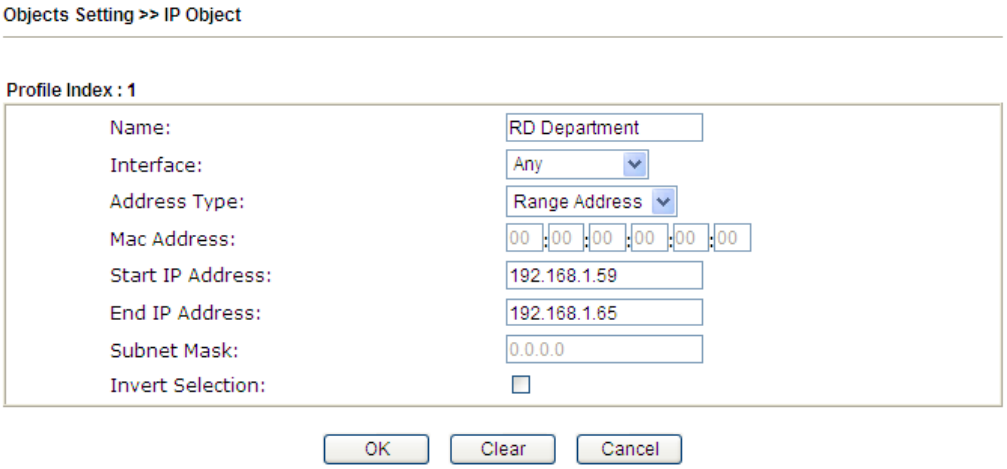
Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

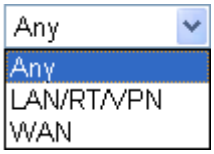
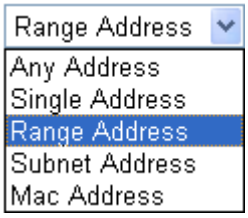
To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.

2. The configuration page will be shown as follows:

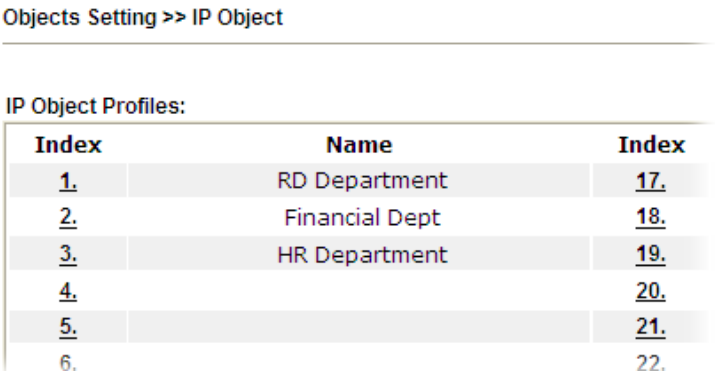


Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose a proper interface.  For example, the **Direction** setting in **Edit Filter Rule** will ask you specify IP or IP range for WAN or LAN or any IP address. If you choose LAN as the **Interface** here, and choose LAN as the direction setting in **Edit Filter Rule**, then all the IP addresses specified with LAN interface will be opened for you to choose in **Edit Filter Rule** page.
Address Type	Determine the address type for the IP address. Select **Single Address** if this object contains one IP address only. Select **Range Address** if this object contains several IPs within a range. Select **Subnet Address** if this object contains one subnet for IP address. Select **Any Address** if this object contains any IP address. Select **Mac Address** if this object contains Mac address. 
MAC Address	Type the MAC address of the network card which will be controlled.

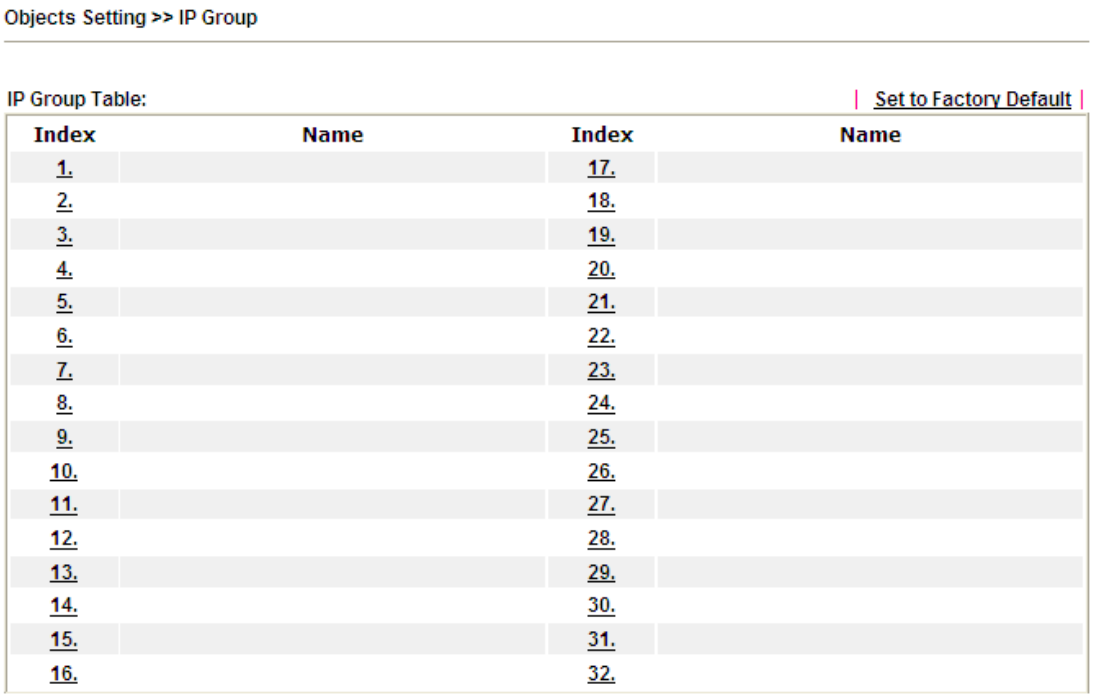
Start IP Address	Type the start IP address for Single Address type.
End IP Address	Type the end IP address if the Range Address type is selected.
Subnet Mask	Type the subnet mask if the Subnet Address type is selected.
Invert Selection	If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.

3. After finishing all the settings here, please click **OK** to save the configuration. Below is an example of IP objects settings.



3.5.2 IP Group

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



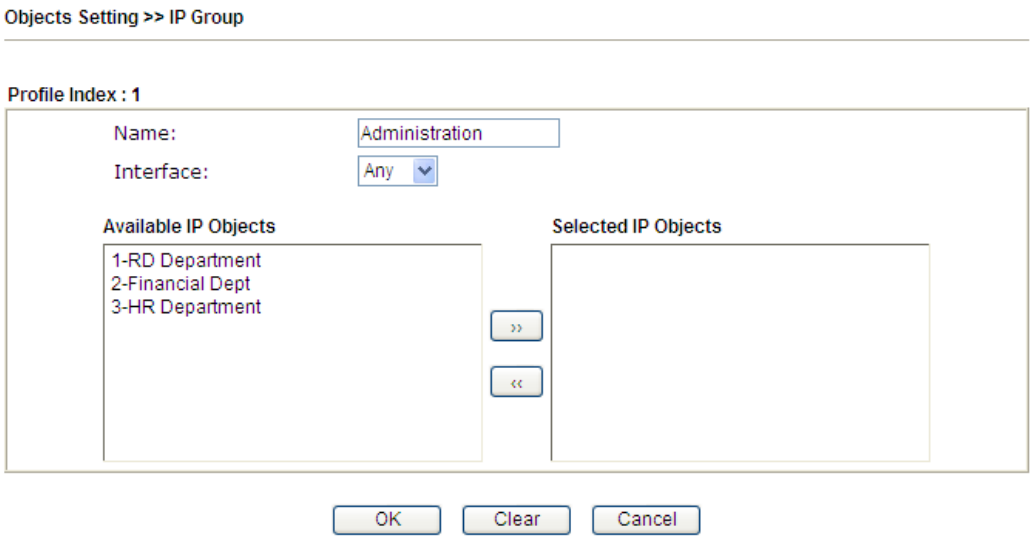
Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.

Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



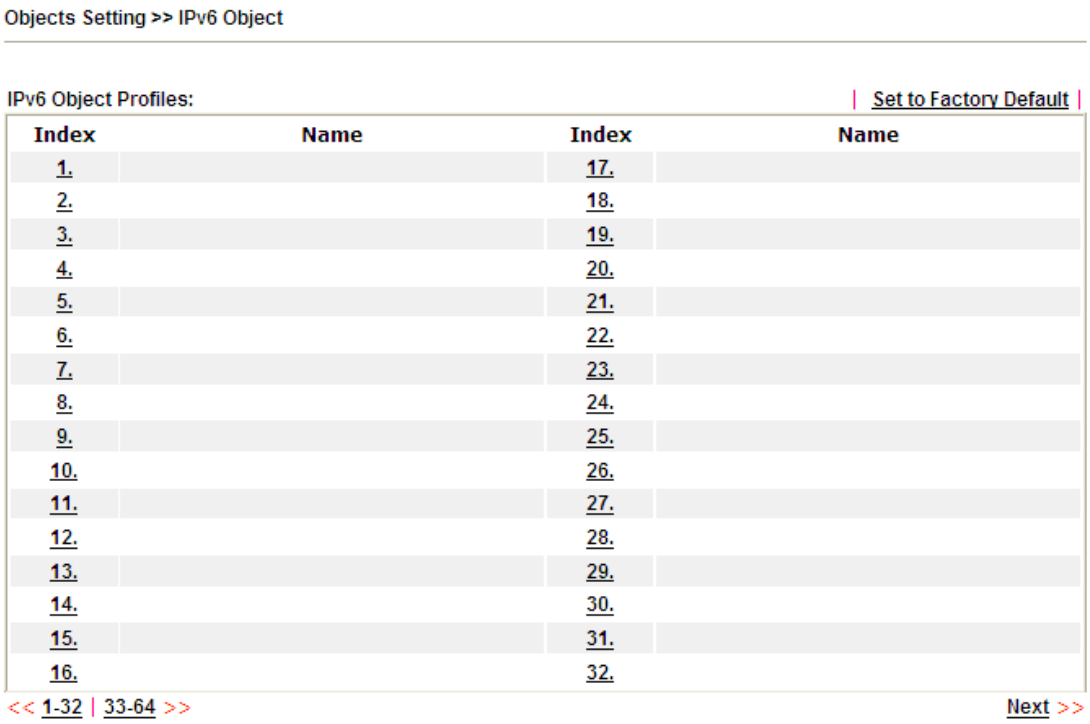
Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose WAN, LAN or Any to display all the available IP objects with the specified interface.
Available IP Objects	All the available IP objects with the specified interface chosen above will be shown in this box.
Selected IP Objects	Click >> button to add the selected IP objects in this box.

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

3.5.3 IPv6 Object

You can set up to 64 sets of IPv6 Objects with different conditions.

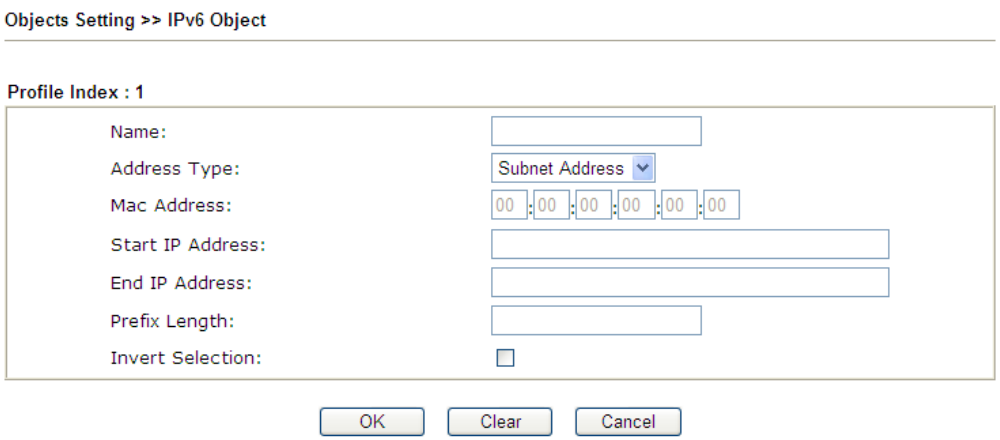


Available settings are explained as follows:

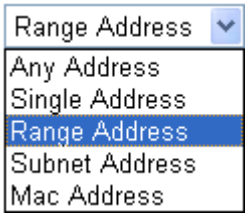
Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



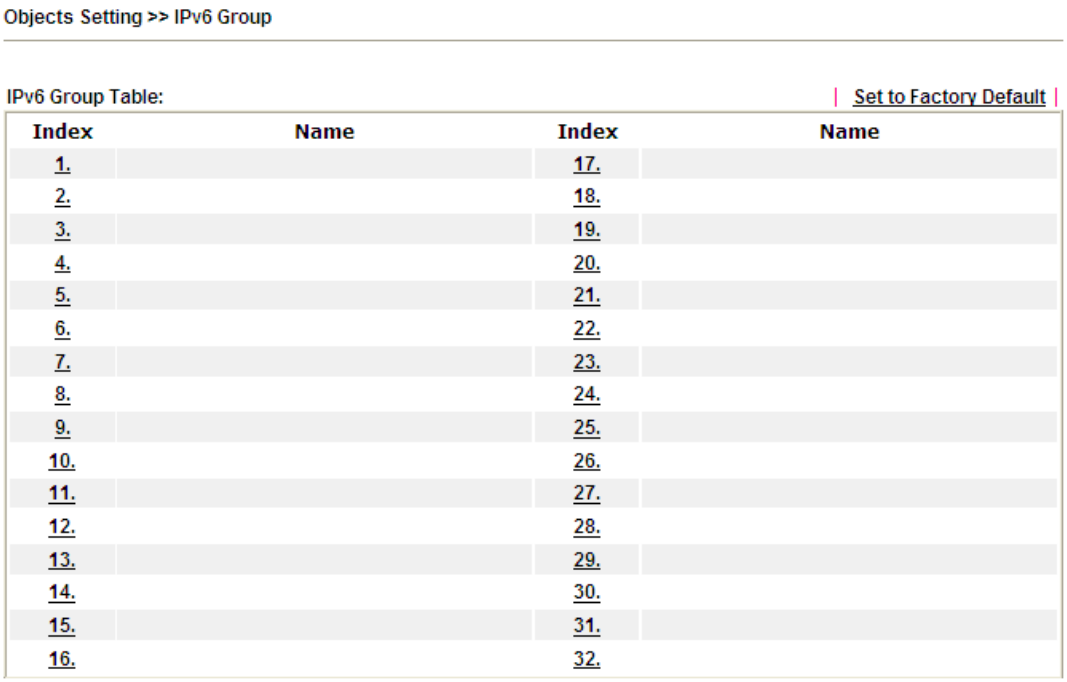
Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Address Type	Determine the address type for the IPv6 address. Select **Single Address** if this object contains one IPv6 address only. Select **Range Address** if this object contains several IPv6s within a range. Select **Subnet Address** if this object contains one subnet for IPv6 address. Select **Any Address** if this object contains any IPv6 address. Select **Mac Address** if this object contains Mac address. 
Mac Address	Type the MAC address of the network card which will be controlled.
Start IP Address	Type the start IP address for Single Address type.
End IP Address	Type the end IP address if the Range Address type is selected.
Prefix Len	Type the number (e.g., 64) for the prefix length of IPv6 address.
Invert Selection	If it is checked, all the IPv6 addresses except the ones listed above will be applied later while it is chosen.

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

3.5.4 IPv6 Group

This page allows you to bind several IPv6 objects into one IPv6 group.

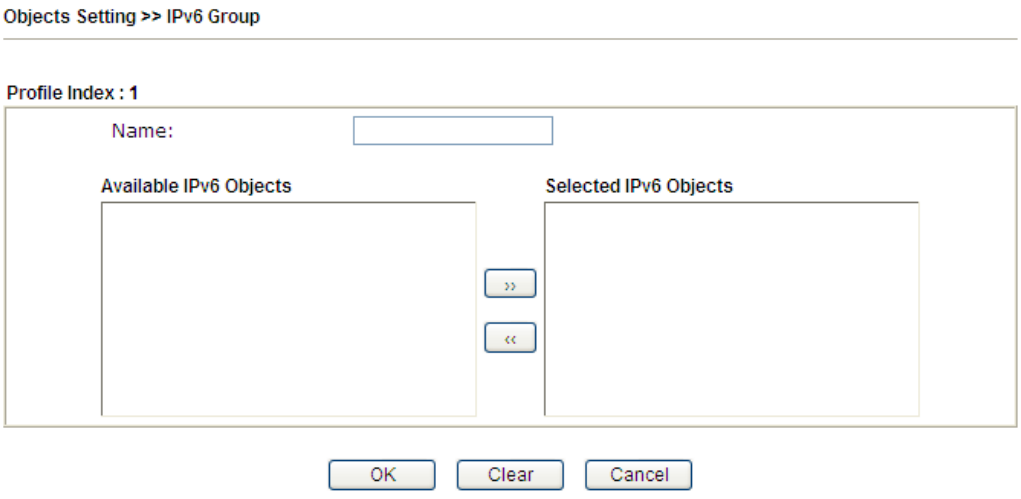


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



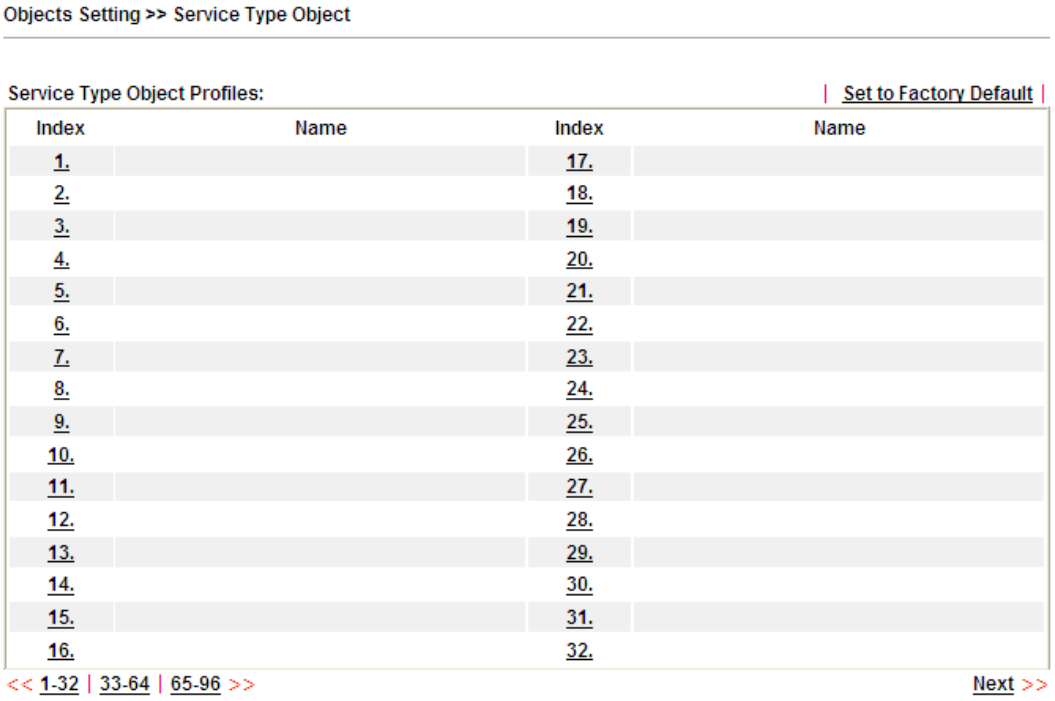
Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Available IPv6 Objects	All the available IPv6 objects with the specified interface chosen above will be shown in this box.
Selected IPv6 Objects	Click >> button to add the selected IPv6 objects in this box.

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

3.5.5 Service Type Object

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

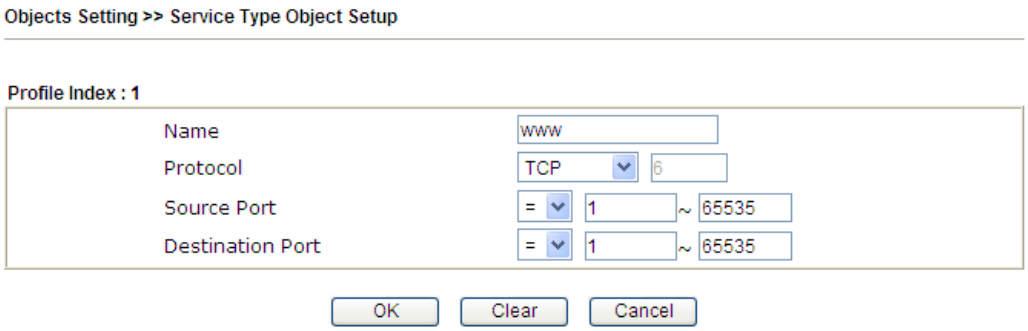


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

To set a new profile, please do the steps listed below:

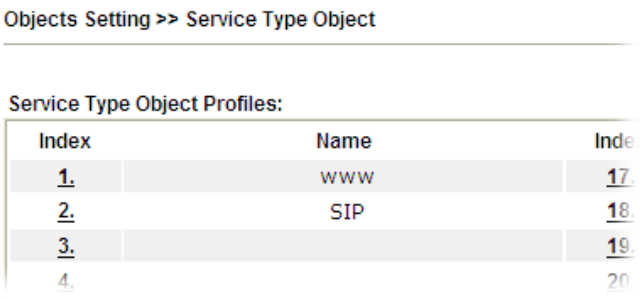
1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



Available settings are explained as follows:

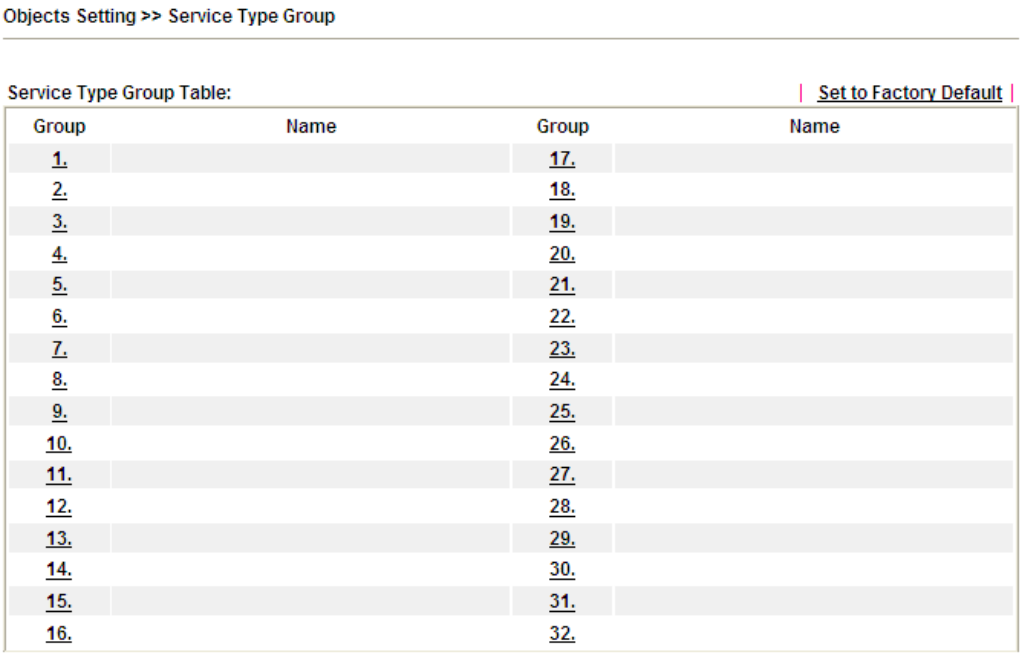
Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Protocol	Specify the protocol(s) which this profile will apply to. TCP 6 Any ICMP IGMP TCP UDP TCP/UDP Other
Source/Destination Port	**Source Port** and the **Destination Port** column are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number. ***(=)*** – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile. ***(!=)*** – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type. ***(>)*** – the port number greater than this value is available. ***(<)*** – the port number less than this value is available for this profile.

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



3.5.6 Service Type Group

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

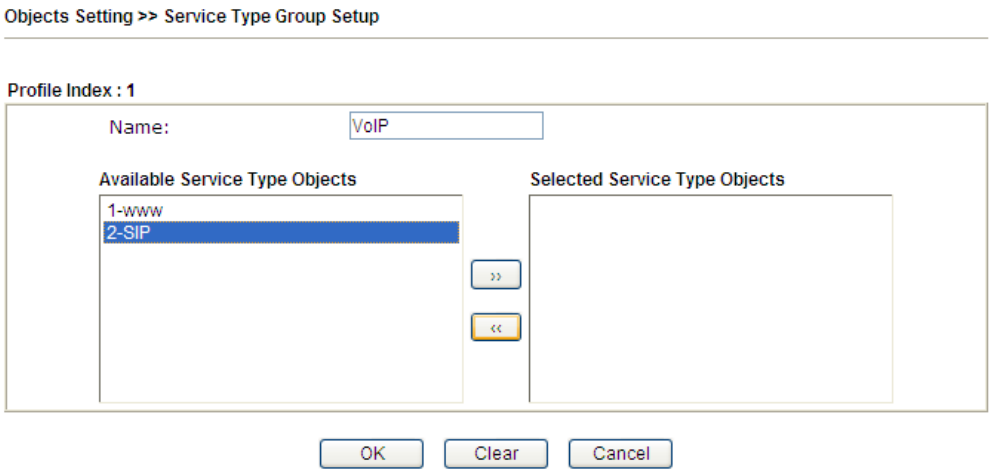


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Group column for configuration in details.
2. The configuration page will be shown as follows:



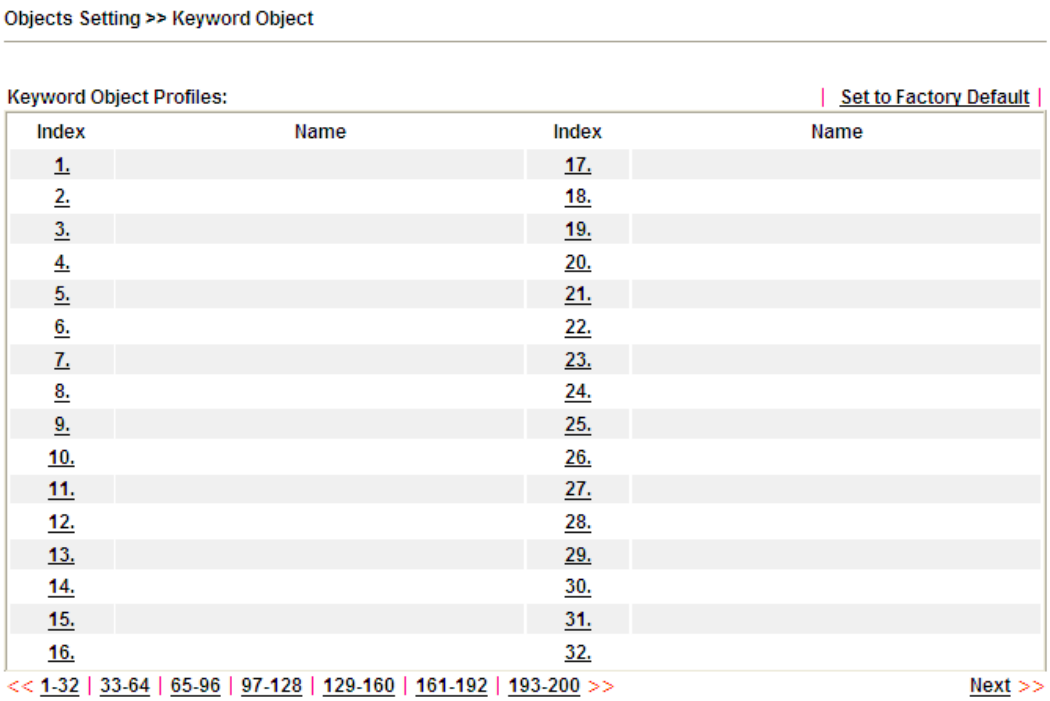
Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Available Service Type Objects	All the available service objects that you have added on **Objects Setting>>Service Type Object** will be shown in this box.
Selected Service Type Objects	Click >> button to add the selected IP objects in this box.

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

3.5.7 Keyword Object

You can set 200 keyword object profiles for choosing as black /white list in **CSM >>URL Web Content Filter Profile.**

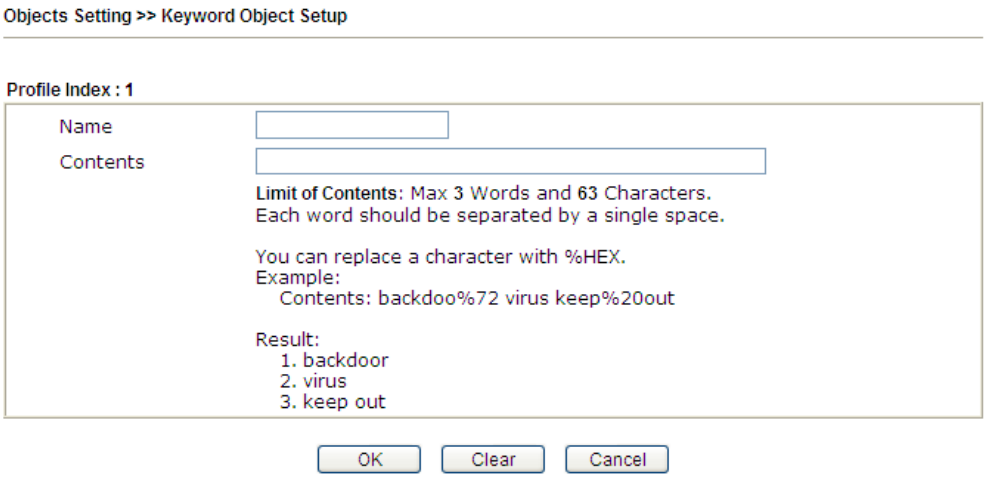


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



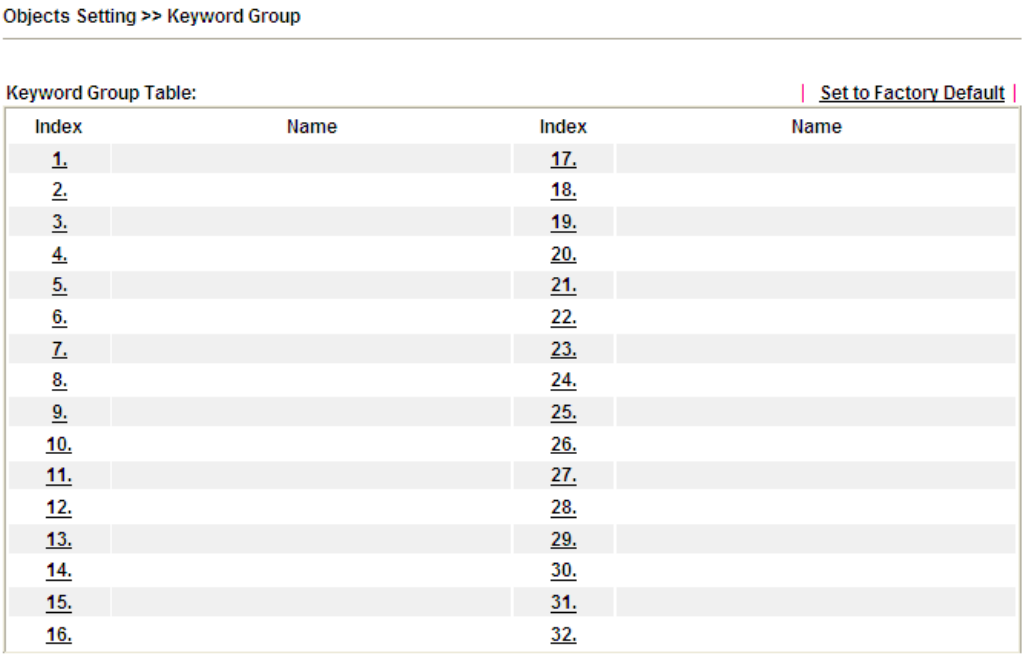
Available settings are explained as follows:

Item	Description
Name	Type a name for this profile, e.g., game. Maximum 15 characters are allowed.
Contents	Type the content for such profile. For example, type *gambling* as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the configuration on Firewall settings.

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

3.5.8 Keyword Group

This page allows you to bind several keyword objects into one group. The keyword groups set here will be chosen as black /white list in **CSM >>URL /Web Content Filter Profile**.

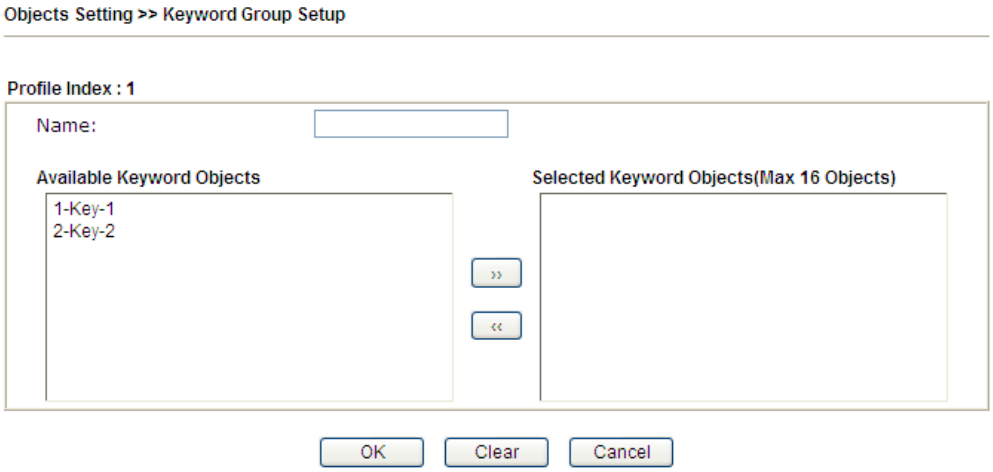


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



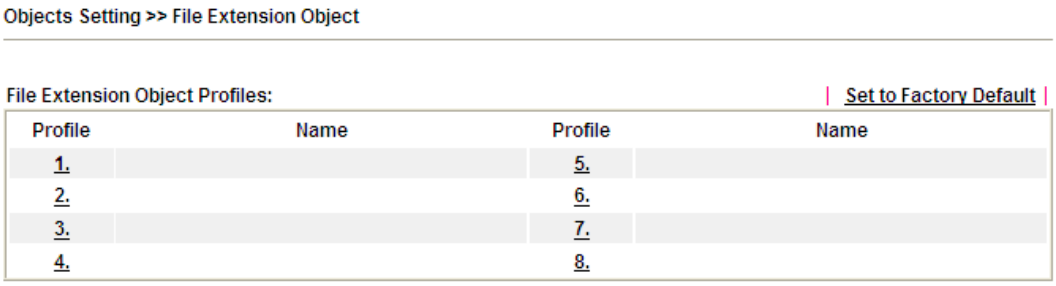
Available settings are explained as follows:

Item	Description
Name	Type a name for this group. Maximum 15 characters are allowed.
Available Keyword Objects	You can gather keyword objects from **Keyword Object** page within one keyword group. All the available Keyword objects that you have created will be shown in this box.
Selected Keyword Objects	Click » button to add the selected Keyword objects in this box.

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

3.5.9 File Extension Object

This page allows you to set eight profiles which will be applied in **CSM>>URL Content Filter**. All the files with the extension names specified in these profiles will be processed according to the chosen action.

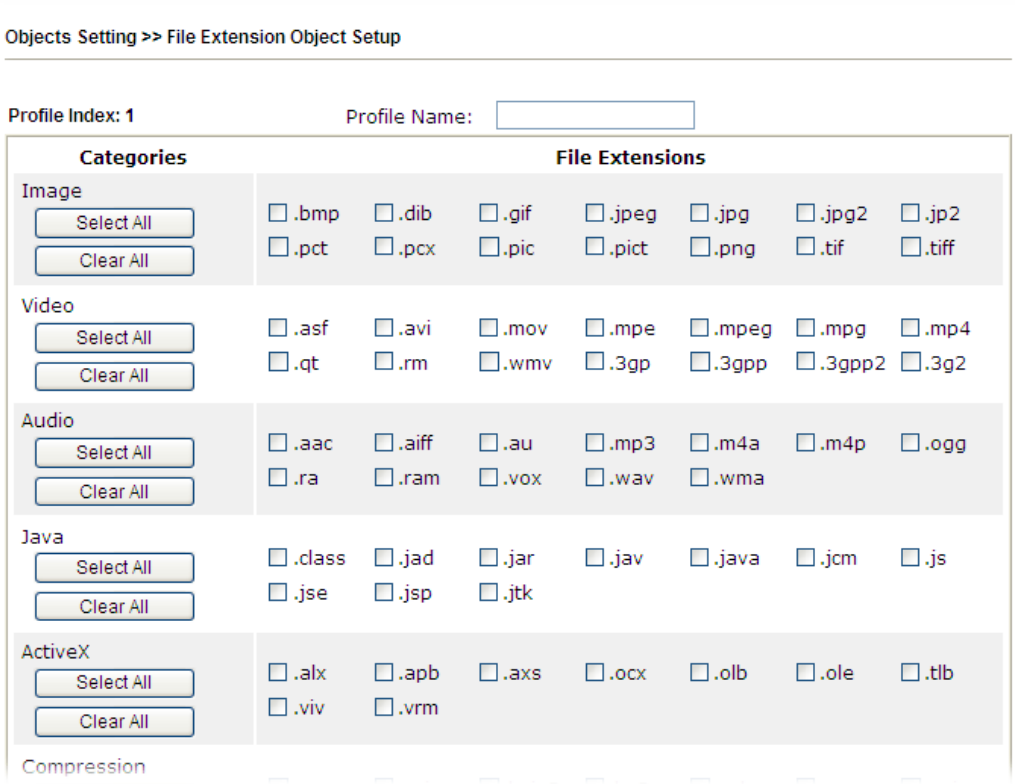


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Profile column for configuration in details.
2. The configuration page will be shown as follows:



Available settings are explained as follows:

Item	Description
Profile Name	Type a name for this profile. The maximum length of the name you can set is 7 characters.

3. Type a name for such profile and check all the items of file extension that will be processed in the modem. Finally, click **OK** to save this profile.

3.6 CSM Profile

Content Security Management (CSM)

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

URL Content Filter

To provide an appropriate cyberspace to users, Vigor modem 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

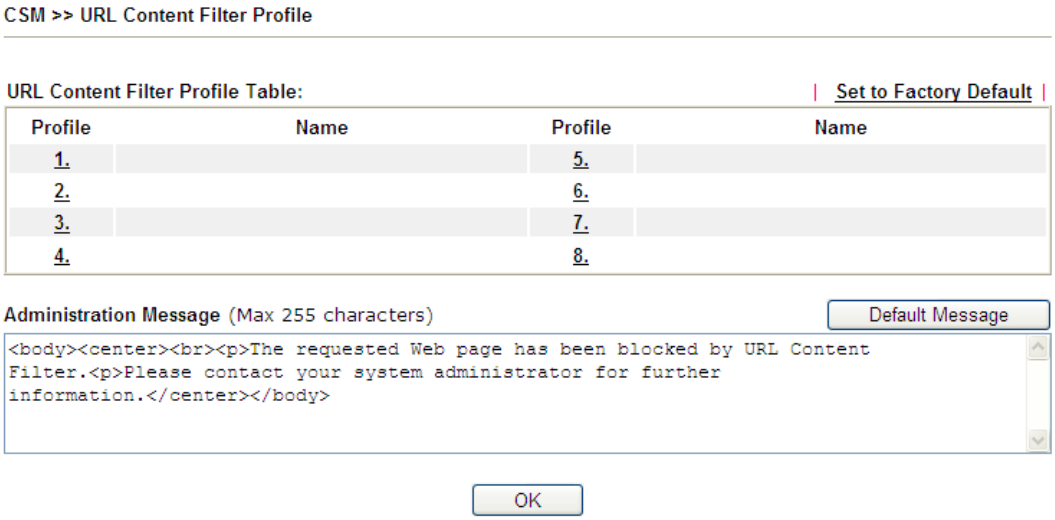
URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor modem 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.

For example, if you add key words such as "sex", Vigor modem 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".

3.6.1 URL Content Filter Profile

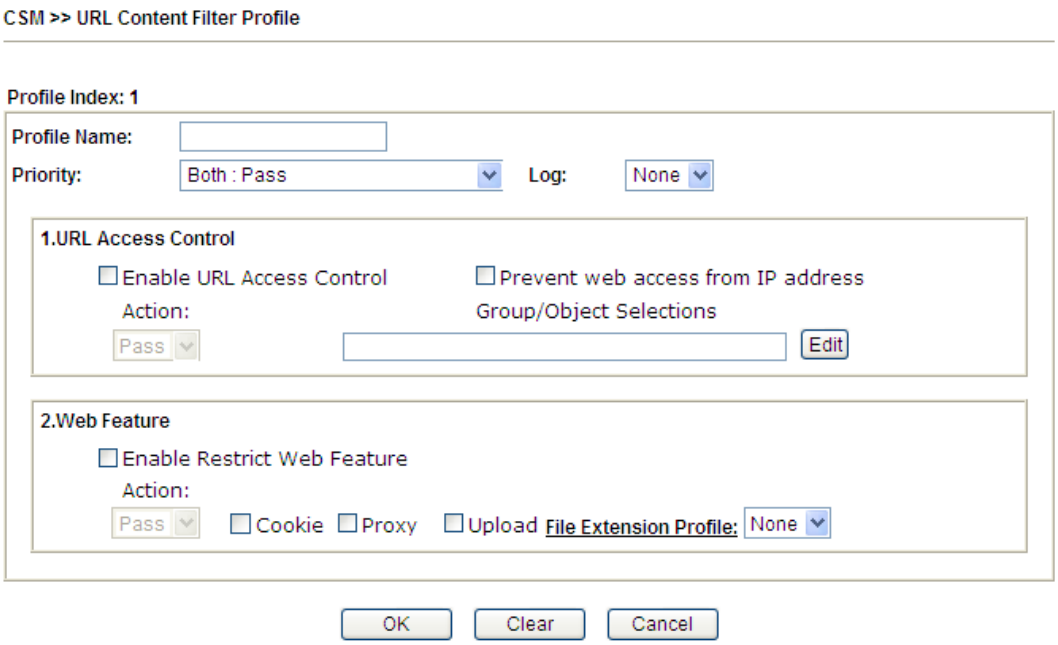
Click **CSM** and click **URL Content Filter Profile** to open the profile setting page.



Each item is explained as follows:

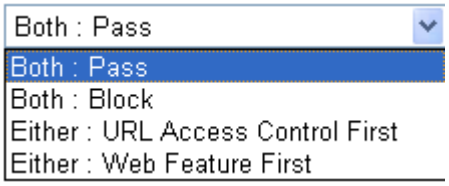
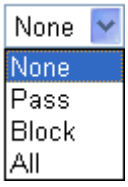
Item	Description
Set to Factory Default	Clear all profiles.
Profile	Display the number of the profile which allows you to click to set different policy.
Name	Display the name of the URL Content Filter Profile.
Administration Message	You can type the message manually for your necessity. **Default Message -** Click this button to apply the default message offered by the modem.

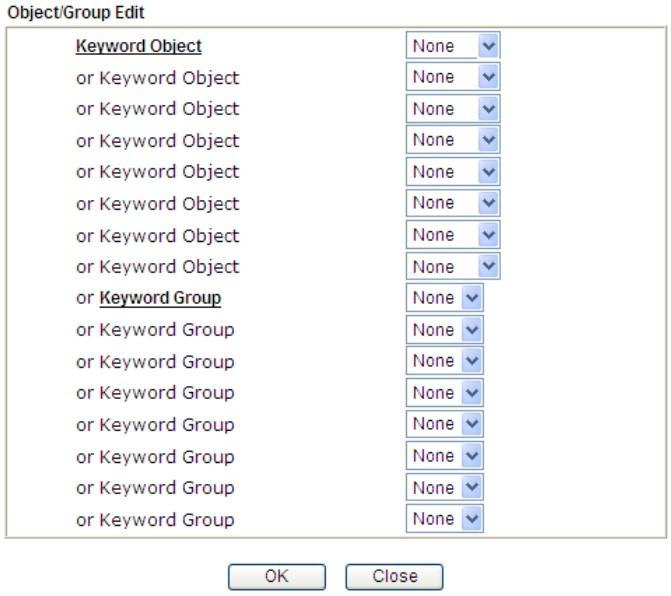
You can set eight profiles as URL content filter. Simply click the index number under Profile to open the following web page.

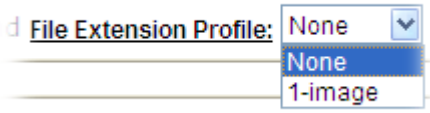


Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Priority	It determines the action that this modem will apply. **Both: Pass** – The modem will let all the packages that match with the conditions specified in URL Access Control and Web Feature below passing through. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive. **Both:Block** –The modem will block all the packages that match with the conditions specified in URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive. **Either: URL Access Control First** – When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the modem will process the packages with the conditions set below for URL first, then Web feature second. **Either: Web Feature First** –When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the modem will process the packages with the conditions set below for web feature first, then URL second.

	
Log	**None** – There is no log file will be recorded for this profile. **Pass** – Only the log about Pass will be recorded in Syslog. **Block** – Only the log about Block will be recorded in Syslog. **All** – All the actions (Pass and Block) will be recorded in Syslog. 
URL Access Control	**Enable URL Access Control** - Check the box to activate URL Access Control. Note that the priority for **URL Access Control** is higher than **Restrict Web Feature**. If the web content match the setting set in URL Access Control, the modem will execute the action specified in this field and ignore the action specified under Restrict Web Feature. **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. **Action** – This setting is available only when **Either : URL Access Control First** or **Either : Web Feature First** is selected. ***Pass*** - Allow accessing into the corresponding webpage with the keywords listed on the box below. ***Block*** **-** Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the keyword set here, it will be processed with reverse action.  **Group/Object Selections** – The Vigor modem provides several 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 modem 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 is, the more efficiently the Vigor modem performs. 
Web Feature	**Enable Restrict Web Feature -** Check this box to make the keyword being blocked or passed. **Action -** This setting is available only when **Either: URL Access Control First** or **Either: Web Feature Firs** is selected. **Pass** allows accessing into the corresponding webpage with the keywords listed on the box below. ***Pass* -** Allow accessing into the corresponding webpage with the keywords listed on the box below. ***Block* -** Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the specified feature set here, it will be processed with reverse action. **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. **Upload** – Check the box to block the file upload by way of web page. **File Extension Profile –** Choose one of the profiles that you configured in **Object Setting>> File Extension Objects** previously for passing or blocking the file downloading.



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

3.7 Applications

Below shows the menu items for Applications.

3.7.1 Dynamic DNS

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

Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The modem provides up to three accounts from three different DDNS service providers. Basically, Vigor modems 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 modem.

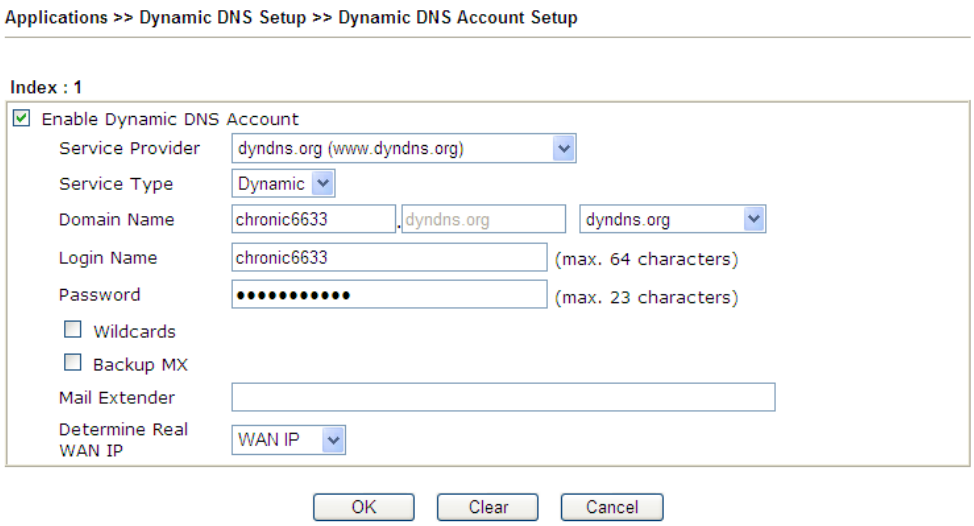
Enable the Function and Add a Dynamic DNS Account

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**.

Available settings are explained as follows:

Item	Description
Enable Dynamic DNS Setup	Check this box to enable DDNS function.
Set to Factory Default	Clear all profiles and recover to factory settings.
View Log	Display DDNS log status.
Force Update	Force the modem updates its information to DDNS server.
Auto-Update interval	Set the time for the modem to perform auto update for DDNS service.
Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).
Domain Name	Display the domain name that you set on the setting page of DDNS setup.
Active	Display if this account is active or inactive.

3. Select Index number 1 to add an account for the modem. 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*.



Available settings are explained as follows:

Item	Description
Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.

Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.
Wildcard and Backup MX	The Wildcard and Backup MX (Mail Exchange) features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.
Mail Extender	If the mail server is defined with another name, please type the name in this area. Such mail server will be used as backup mail exchange.
Force WAN IP Update	When the IP address of the WAN interface in Vigor modem is private IP, the system will detect the Public IP used by the modem in front of Vigor modem and use that Public IP to update DDNS server forcefully.
Determine Real WAN IP	If a Vigor modem is installed behind any NAT modem, you can enable such function to locate the real WAN IP. When the WAN IP used by Vigor modem is private IP, this function can detect the public IP used by the NAT modem and use the detected IP address for DDNS update. There are two methods offered for you to choose: **WAN IP** - If it is selected and the WAN IP of Vigor modem is private, DDNS update will take place right away. **Internet IP** – If it is selected and the WAN IP of Vigor modem is private, it will be converted to public IP before DDNS update takes place.

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 modem.

Delete a Dynamic DNS Account

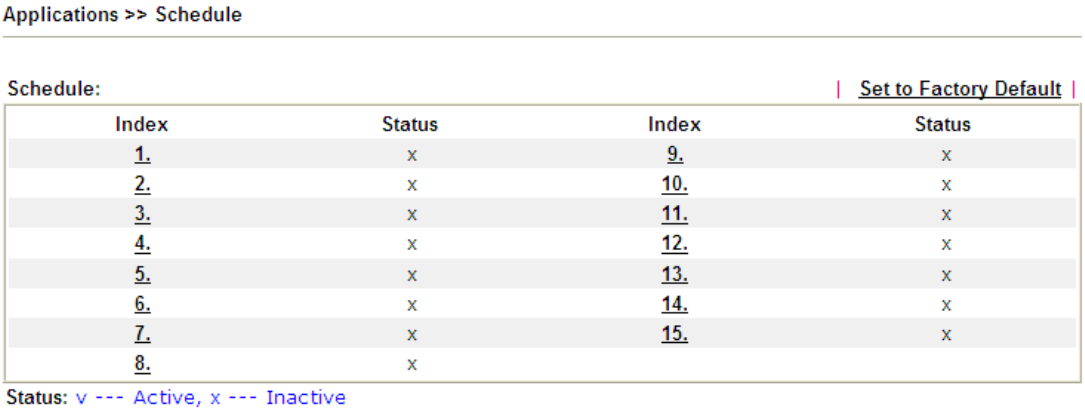
In the DDNS setup menu, click the **Index** number you want to delete and then push **Clear All** button to delete the account.

3.7.2 Schedule

The Vigor modem 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 modem to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule is also applicable to other functions.

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

modem's clock. This method can only be applied when the WAN connection has been built up.



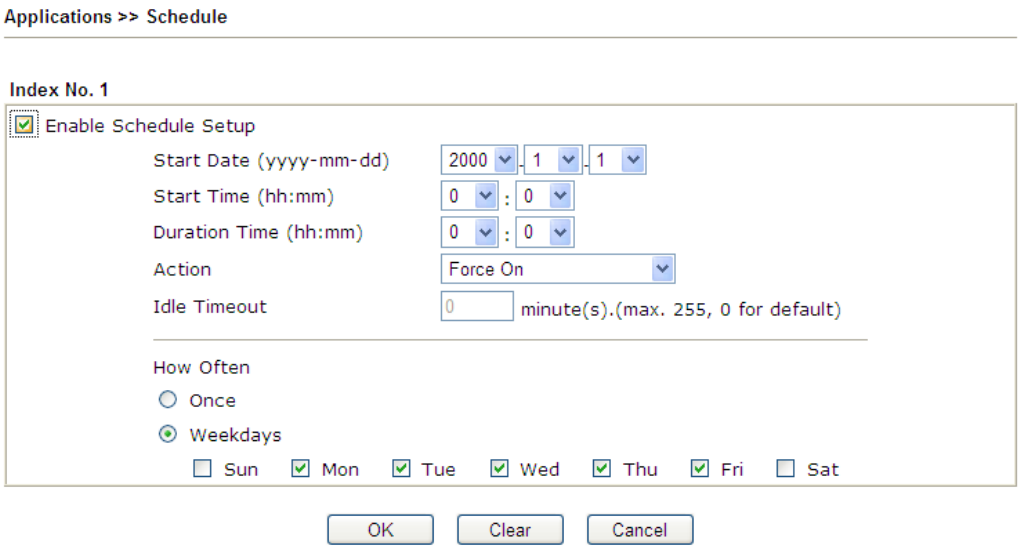
Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles and recover to factory settings.
Index	Click the number below Index to access into the setting page of schedule.
Status	Display if this schedule setting is active or inactive.

You can set up to 15 schedules. Then you can apply them to your **Internet Access** settings.

To add a schedule:

1. Click any index, say Index No. 1.
2. The detailed settings of the call schedule with index 1 are shown below.



Available settings are explained as follows:

Item	Description
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.

3. Click **OK** button to save the settings.

Example

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

Office Hour:

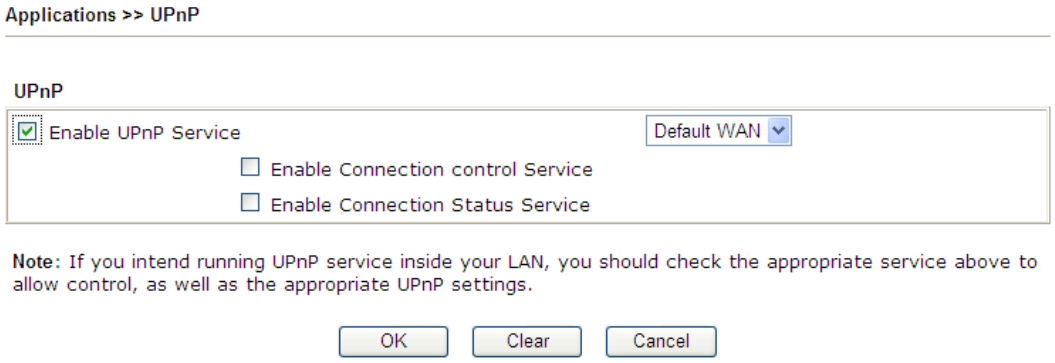
(Force On)

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

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

3.7.3 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 modems, the major feature of UPnP on the modem is “NAT Traversal”. This enables applications inside the firewall to automatically open the ports that they need to pass through a modem. It is more reliable than requiring a modem 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 modem provide the associated support for MSN Messenger to allow full use of the voice, video and messaging features.

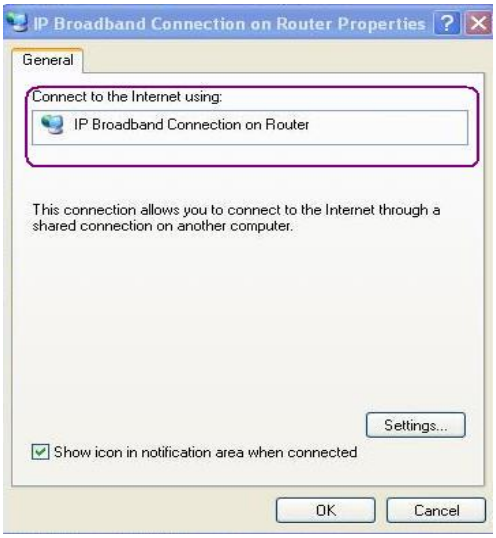


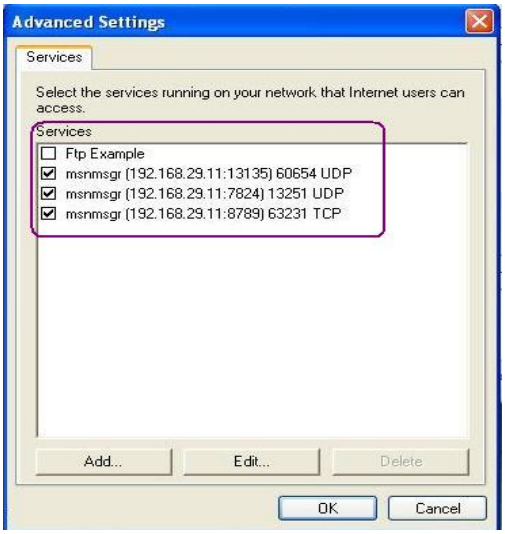
Available settings are explained as follows:

Item	Description
Enable UPNP Service	Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.
Default WAN	It is used to specify the WAN interface for applying such function. The default setting is Default WAN.

After setting **Enable UPNP Service** setting, an icon of **IP Broadband Connection on Modem** 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 modem enables UPnP aware applications such as MSN Messenger to discover what are behind a NAT modem. The application will also learn the external IP address and configure port mappings on the modem. Subsequently, such a facility forwards packets from the external ports of the modem 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

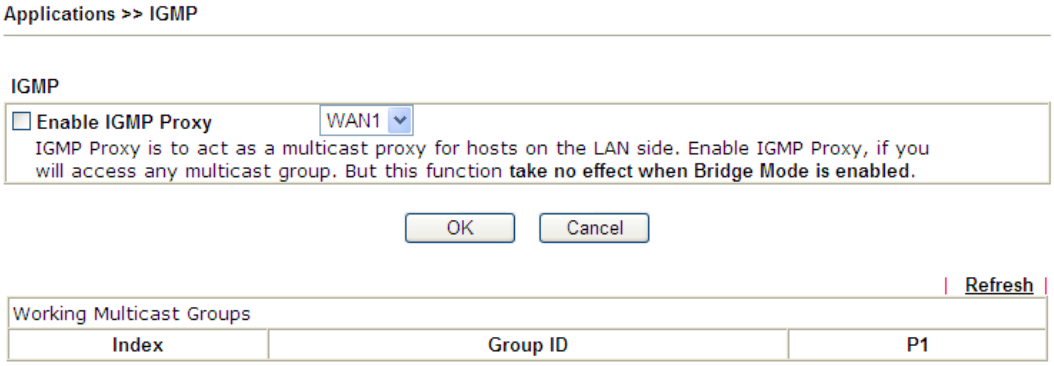
Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

- 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 modem functions, including removing and adding port mappings.

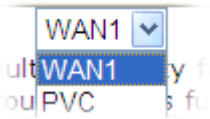
The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

3.7.4 IGMP

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



Available settings are explained as follows:

Item	Description
Enable IGMP Proxy	Check this box to enable this function. The application of multicast will be executed through WAN port. In addition, such function is available in NAT mode. 
Refresh	Click this link to renew the working multicast group status.
Group ID	This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.
P1	It indicates the LAN port used for the multicast group.

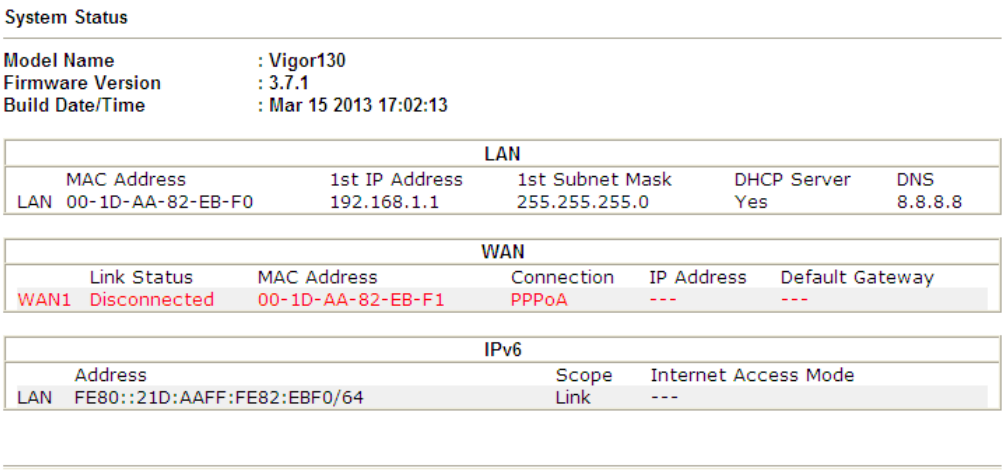
3.8 System Maintenance

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

Below shows the menu items for System Maintenance.

3.8.1 System Status

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



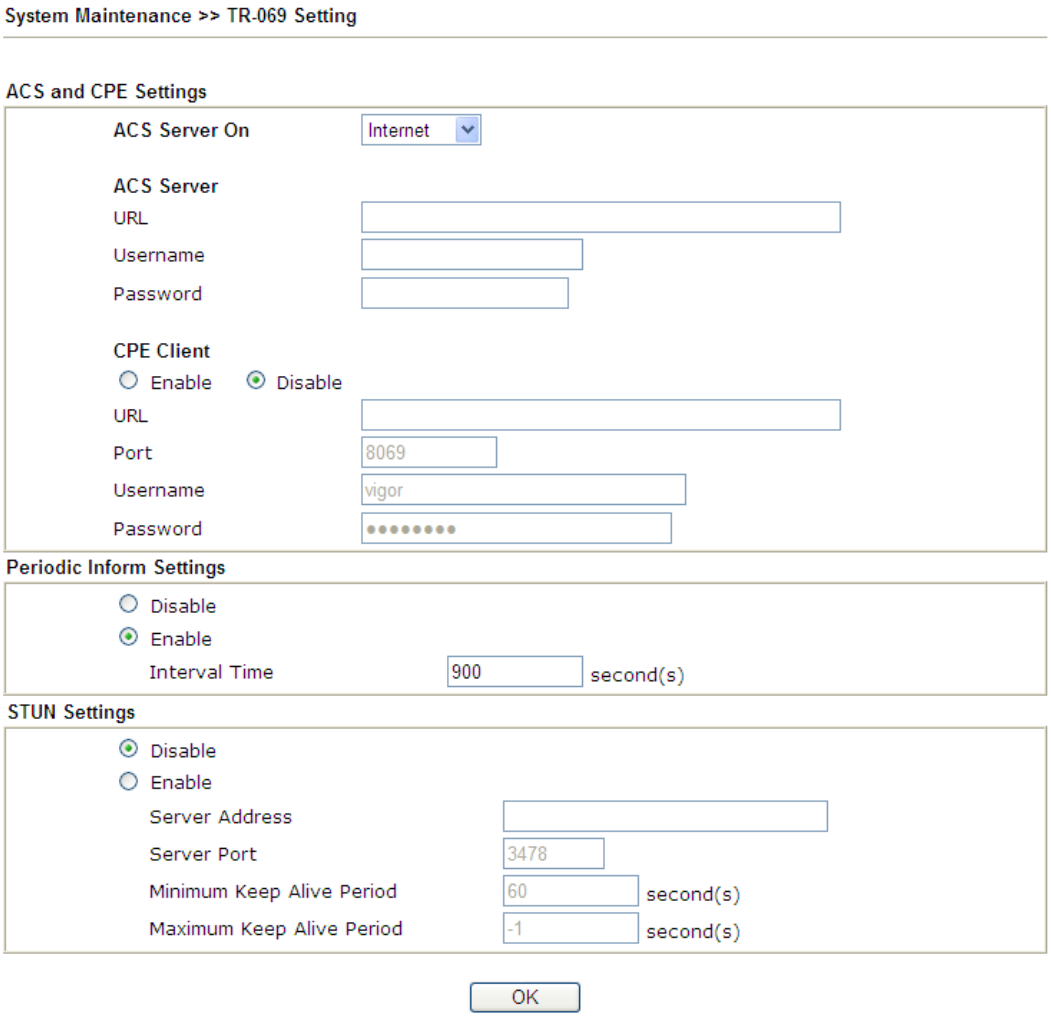
Available settings are explained as follows:

Item	Description
Model Name	Display the model name of the modem.
Firmware Version	Display the firmware version of the modem.
Build Date/Time	Display the date and time of the current firmware build.
LAN	**MAC Address** - Display the MAC address of the LAN Interface. **1st IP Address** - Display the IP address of the LAN interface. **1st Subnet Mask**

	- Display the subnet mask address of the LAN interface. **DHCP Server** - Display the current status of DHCP server of the LAN interface **DNS** - Display the assigned IP address of the primary DNS.
WAN	**Link Status** - Display current connection status. **MAC Address** - Display the MAC address of the WAN Interface. **Connection** - Display the connection type. **IP Address** - Display the IP address of the WAN interface. **Default Gateway** - Display the assigned IP address of the default gateway.
IPv6	**Address -** Display the IPv6 address for LAN. **Scope -** Display the scope of IPv6 address. For example, IPv6 **Link Local** could only be used for direct IPv6 link. It can't be used for IPv6 internet. **Internet Access Mode –** Display the connection mode chosen for accessing into Internet.

3.8.2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.



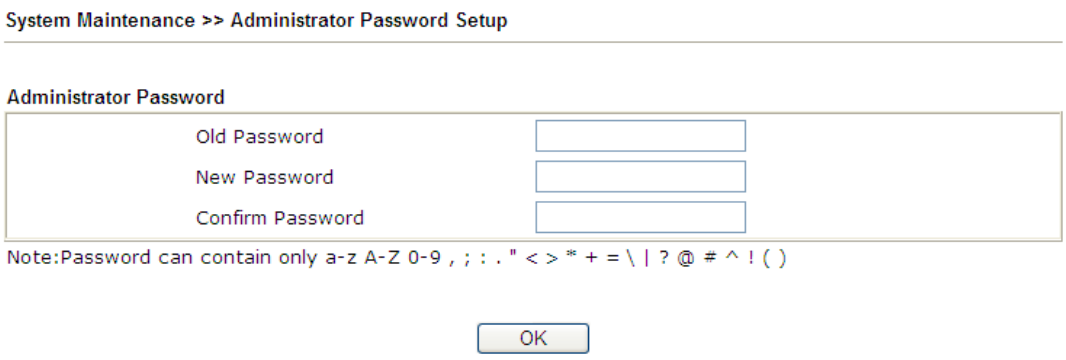
Available settings are explained as follows:

Item	Description
ACS Server On	Choose the interface for the modem connecting to ACS server.
ACS Server	**URL/Username/Password –** Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.
CPE Client	Such information is useful for Auto Configuration Server. **Enable/Disable** – Allow/Deny the CPE Client to connect with Auto Configuration Server. **Port** – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.
Periodic Inform Settings	The default setting is **Enable**. Please set interval time or schedule time for the modem to send notification to CPE.

	Or click **Disable** to close the mechanism of notification.
STUN Settings	The default is **Disable**. If you click **Enable**, please type the relational settings listed below: **Server IP –** Type the IP address of the STUN server. **Server Port –** Type the port number of the STUN server. **Minimum Keep Alive Period –** If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds". **Maximum Keep Alive Period –** If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.

3.8.3 Administrator Password

This page allows you to set new password.



Available settings are explained as follows:

Item	Description
Old Password	Type in the old password. The factory default setting for password is **"admin"**.
New Password	Type in new password in this field.
Confirm Password	Type in the new password again.

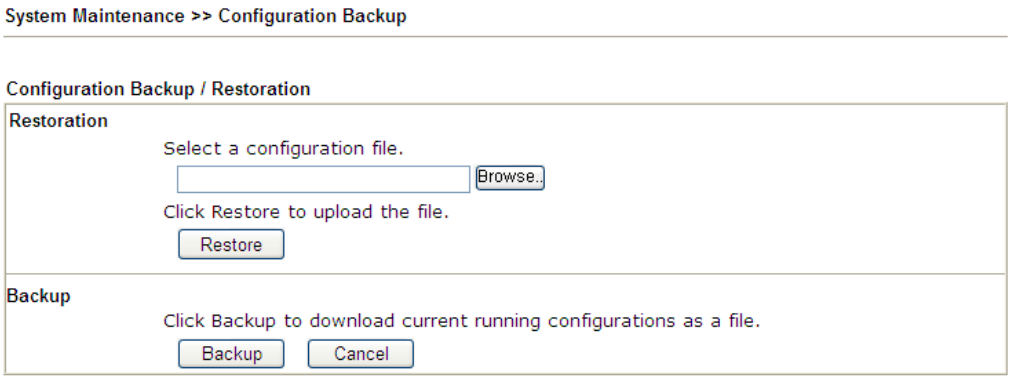
When you click **OK**, the login window will appear. Please use the new password to access into the Web User Interface again.

3.8.4 Configuration Backup

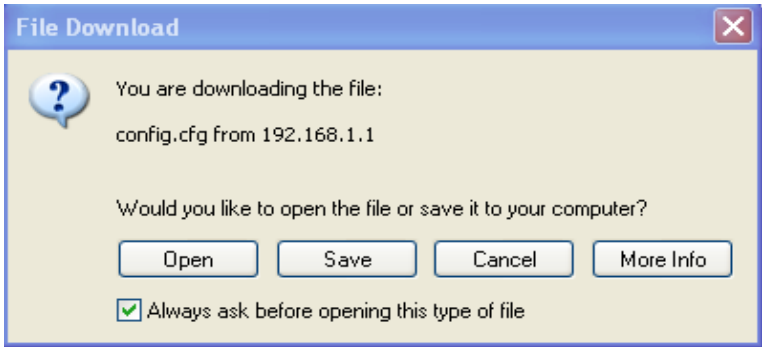
Backup the Configuration

Follow the steps below to backup your configuration.

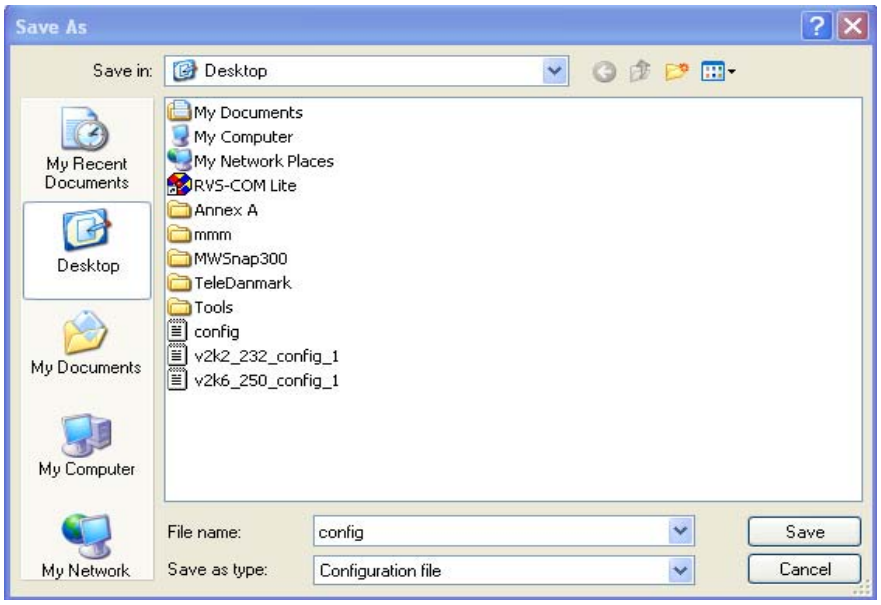
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.



2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.



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



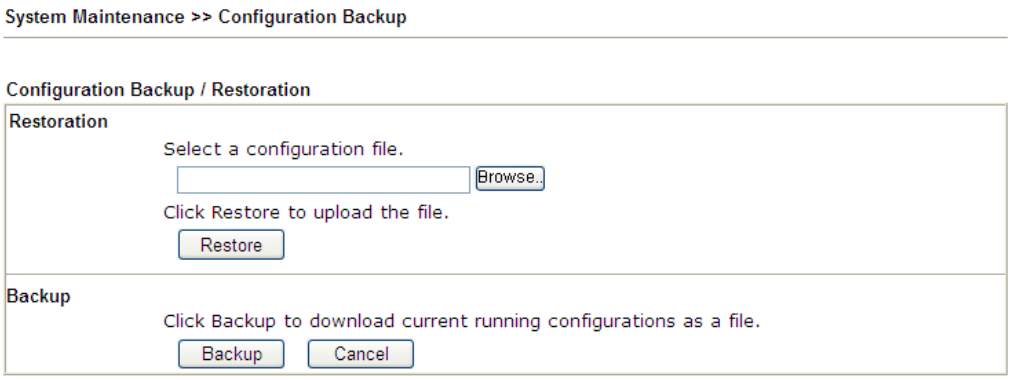
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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

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

Restore Configuration

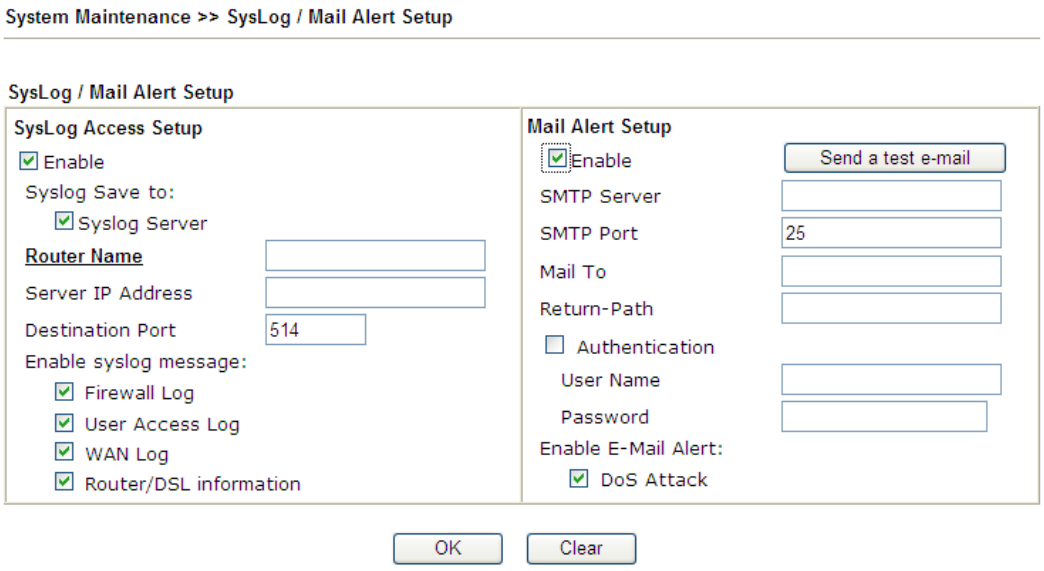
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.



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

3.8.5 Syslog/Mail Alert

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



Available settings are explained as follows:

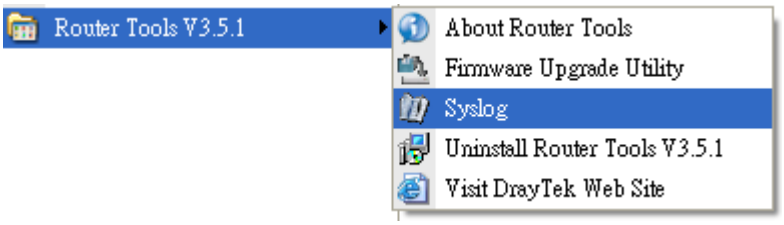
Item	Description
SysLog Access Setup	**Enable** - Check **Enable** to activate function of syslog. **Syslog Save to** – Check **Syslog Server** to save the log to Syslog server.
Router Name	Display the name for such modem configured in **System Maintenance>>Management.** If there is no name here, simply lick the link to access into **System Maintenance>>Management** to set the modem name. **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 listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.
Mail Alert Setup	Check "**Enable**" to activate function of mail alert. **Send a test e-mail** - Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not. **SMTP Server** - The IP address of the SMTP server. **Mail To** - Assign a mail address for sending mails out. **Return-Path** - Assign a path for receiving the mail from outside.

	Authentication - Check this box to activate this function while using e-mail application. **User Name -** Type the user name for authentication. **Password -** Type the password for authentication. **Enable E-mail Alert -** Check the box to send alert message to the e-mail box while the modem detects the item you specify here.

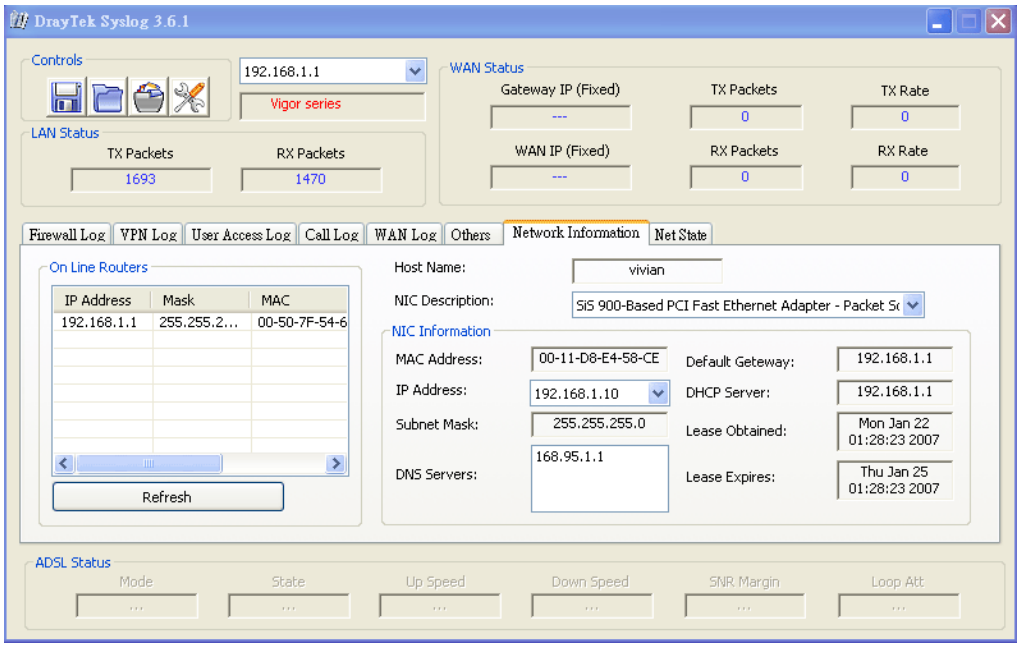
Click **OK** to save these settings.

For viewing the Syslog, please do the following:

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

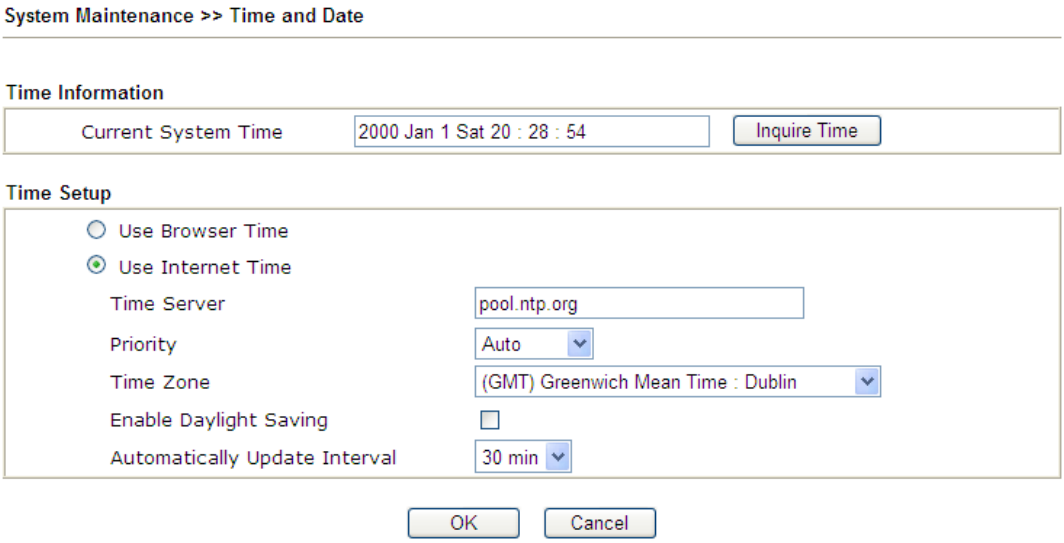


3. From the Syslog screen, select the modem you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the modem. Otherwise, you won't succeed in retrieving information from the modem.



3.8.6 Time and Date

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



Available settings are explained as follows:

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

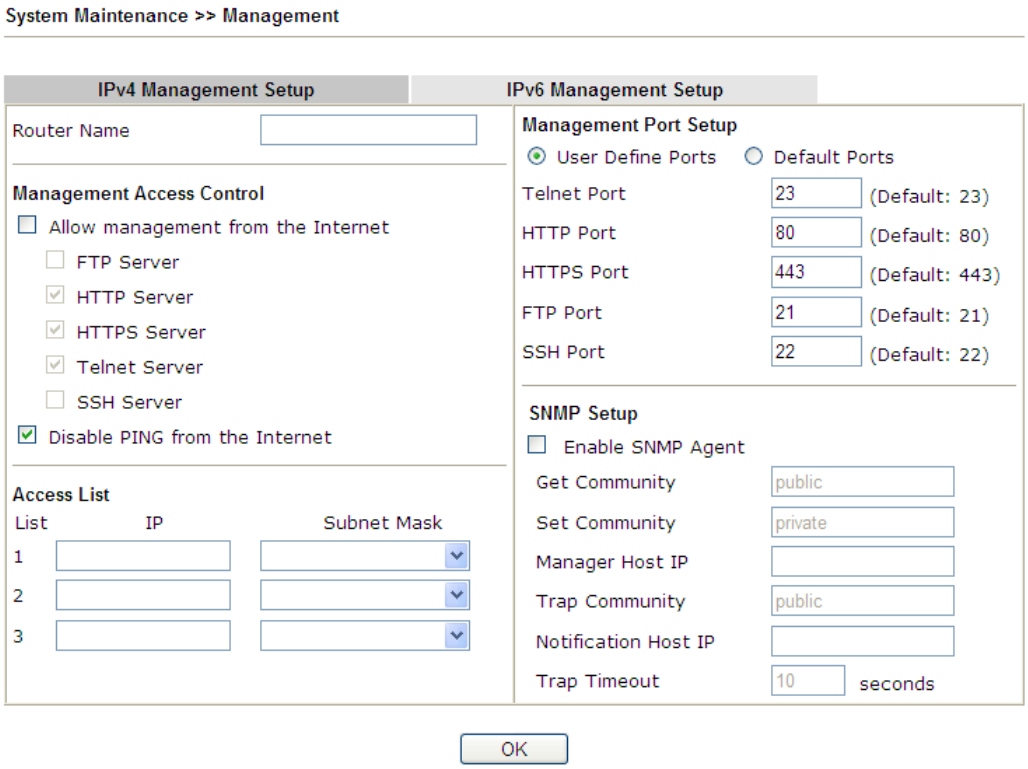
Click **OK** to save these settings.

3.8.7 Management

This page allows you to manage the settings for access control, access list, port setup, and SNMP setup.

The management pages for IPv4 and IPv6 protocols are different.

For IPv4

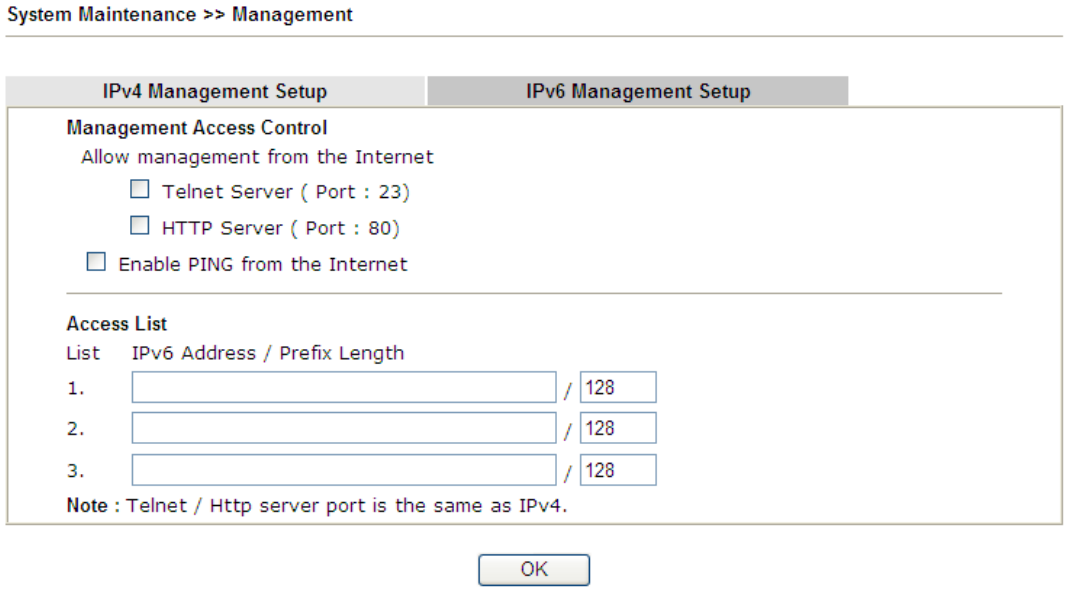


Available settings are explained as follows:

Item	Description
Router Name	Type in the modem name provided by ISP.
Management Access Control	**Allow management from the Internet** - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the modem from Internet. Check the box(es) to specify. **Disable PING from the Internet** - Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.
Access List	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed. **List IP** - Indicate an IP address allowed to login to the modem. **Subnet Mask** - Represent a subnet mask allowed to login to the modem.
Management Port Setup	**User Defined Ports** - Check to specify user-defined port numbers for the Telnet, HTTP and FTP servers.

	Default Ports - Check to use standard port numbers for the Telnet and HTTP servers.
SNMP	**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 IPv4 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 IPv4 address of the host that will receive the trap community. **Trap Timeout -** The default setting is 10 seconds.

For IPv6



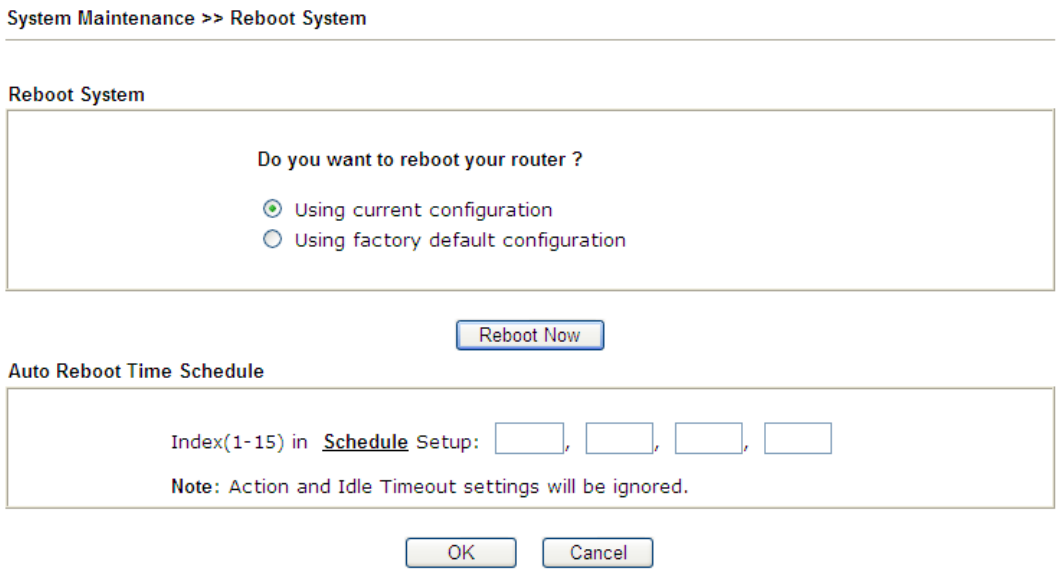
Available settings are explained as follows:

Item	Description
Management Access Control	Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the modem from Internet. Check the box(es) to specify. **Enable PING from the Internet -** Check the checkbox to enable all PING packets from the Internet. For security issue, this function is disabled 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. **IPv6 Address /Prefix Length-** Indicate the IP address(es)

	allowed to login to the modem.

3.8.8 Reboot System

The Web User Interface may be used to restart your modem. Click **Reboot System** from **System Maintenance** to open the following page.



Index (1-15) in Schedule Setup - You can type in four sets of time schedule for performing system reboot. All the schedules can be set previously in **Applications >> Schedule** web page and you can use the number that you have set in that web page.

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

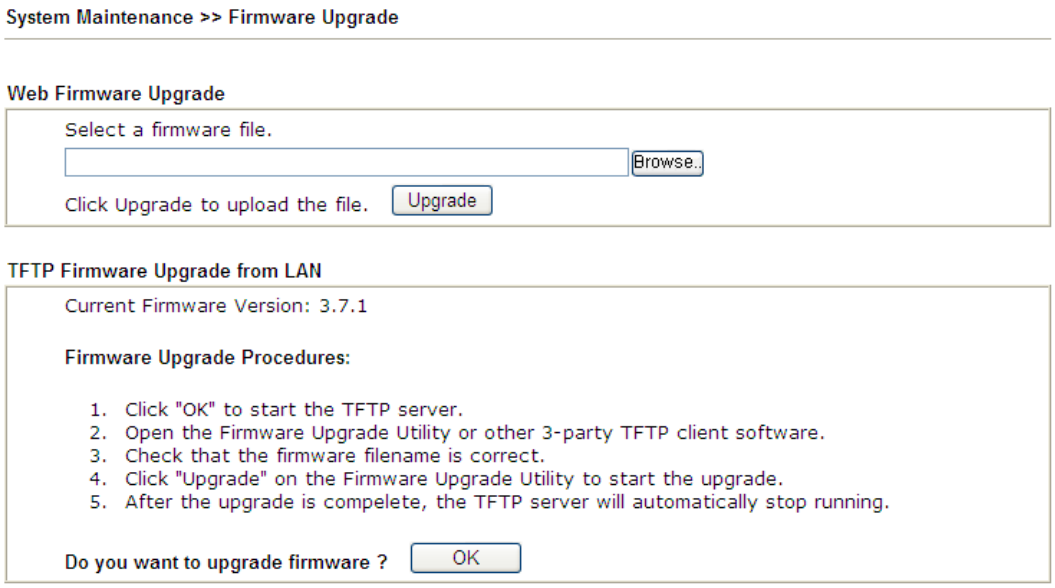
Note: When the system pops up Reboot System web page after you configure web settings, please click **OK** to reboot your modem for ensuring normal operation and preventing unexpected errors of the modem in the future.

3.8.9 Firmware Upgrade

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

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

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



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

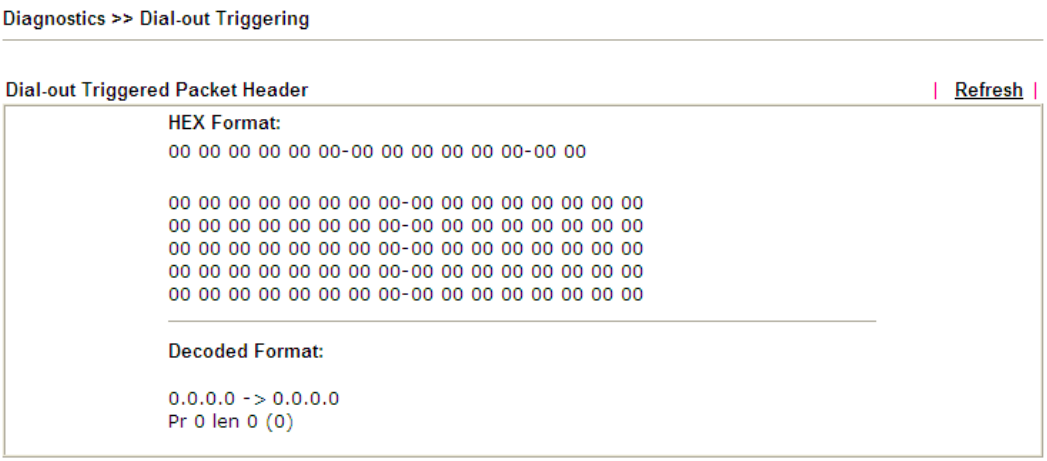
3.9 Diagnostics

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

Below shows the menu items for Diagnostics.

3.9.1 Dial-out Triggering

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

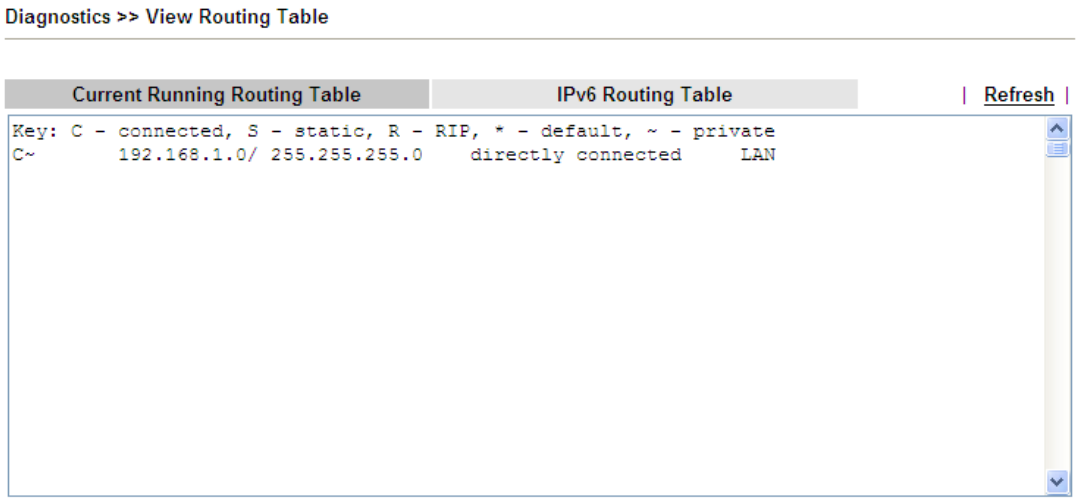


Available settings are explained as follows:

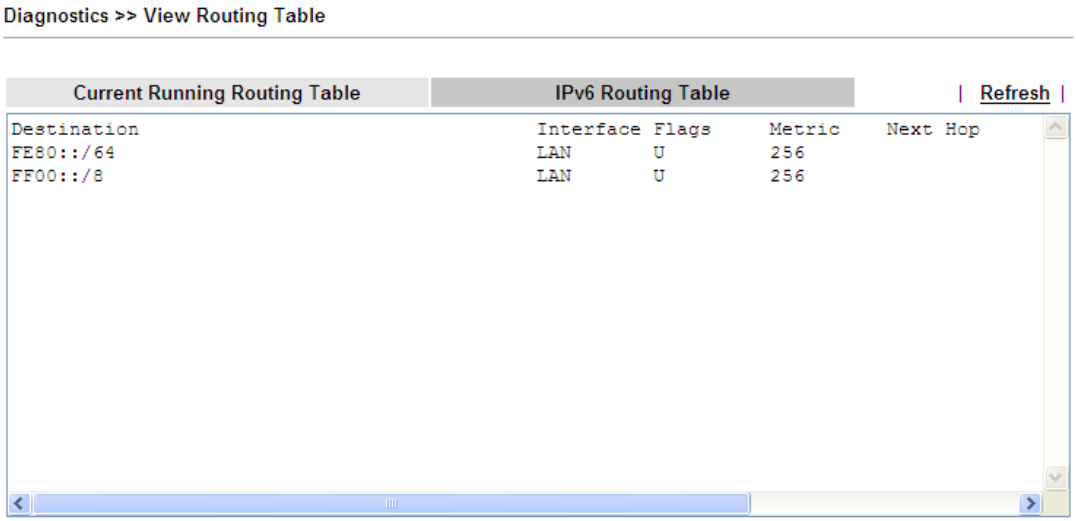
Item	Description
Decoded Format	It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.
Refresh	Click it to reload the page.

3.9.2 Routing Table

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



Note: WAN3, WAN4, WAN5 are router-borne WANs.

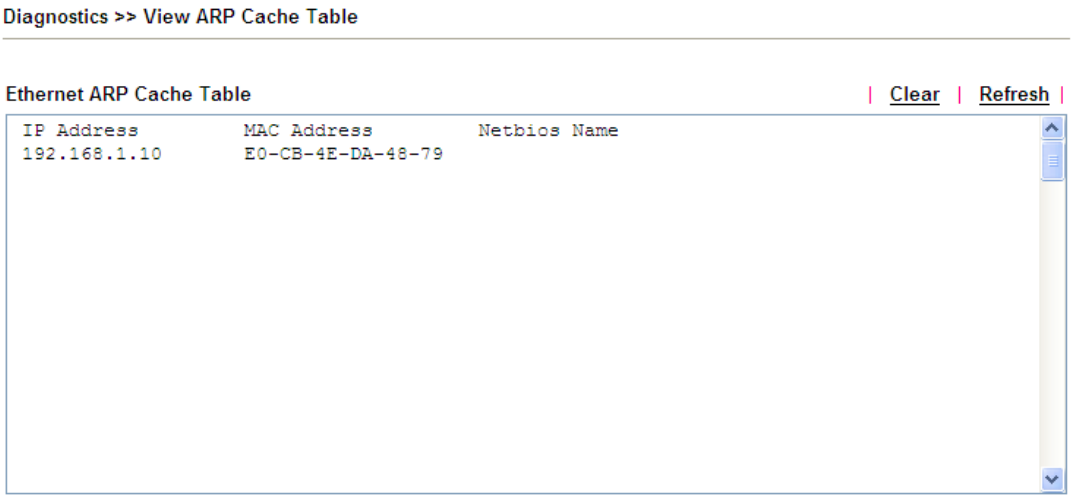


Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

3.9.3 ARP Cache Table

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



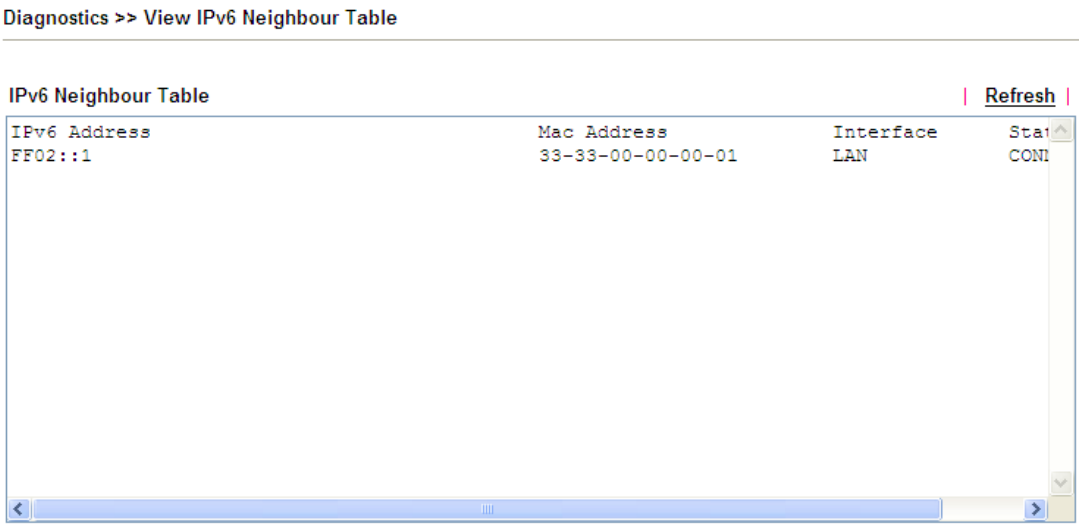
Available settings are explained as follows:

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

3.9.4 IPv6 Neighbour Table

The table shows a mapping between an Ethernet hardware address (MAC Address) and an IPv6 address. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **IPv6 Neighbour Table** to open the web page.



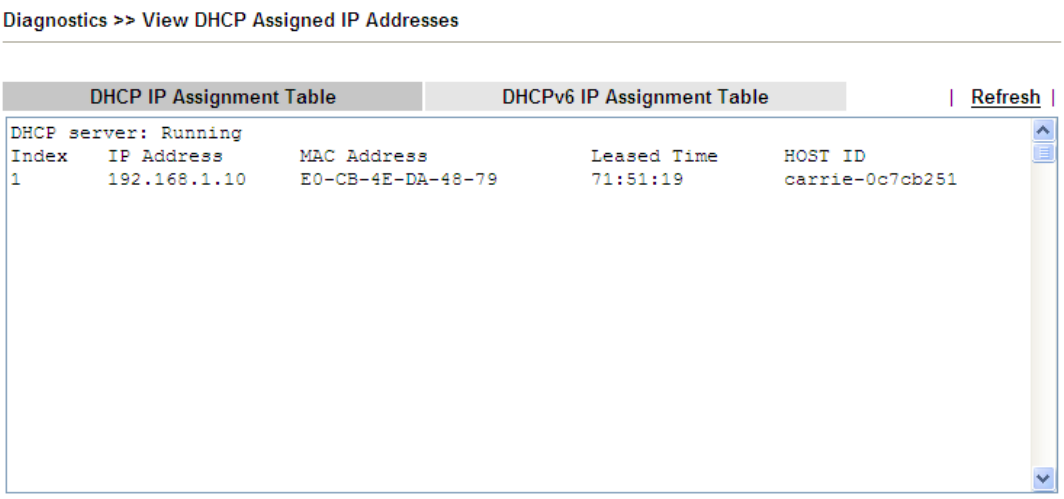
Available settings are explained as follows:

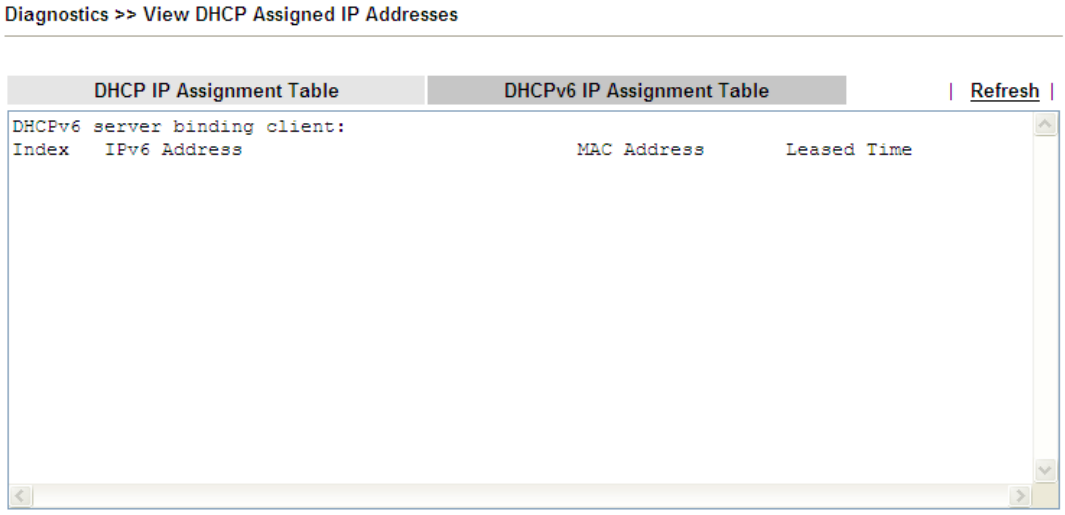
Item	Description
Refresh	Click it to reload the page.

3.9.5 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.





Each item is explained as follows:

Item	Description
Index	It displays the connection item number.
IP Address	It displays the IP address assigned by this modem for specified PC.
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.
Leased Time	It displays the leased time of the specified PC.

HOST ID	It displays the host ID name of the specified PC.
Refresh	Click it to reload the page.

3.9.6 NAT Sessions Table

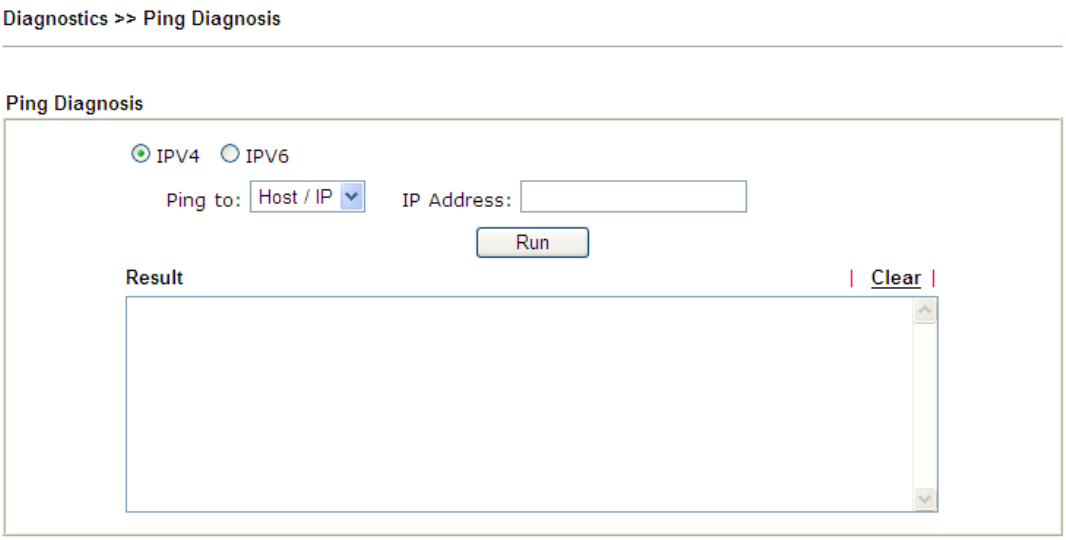
Click **Diagnostics** and click **NAT Sessions Table** to open the list page.

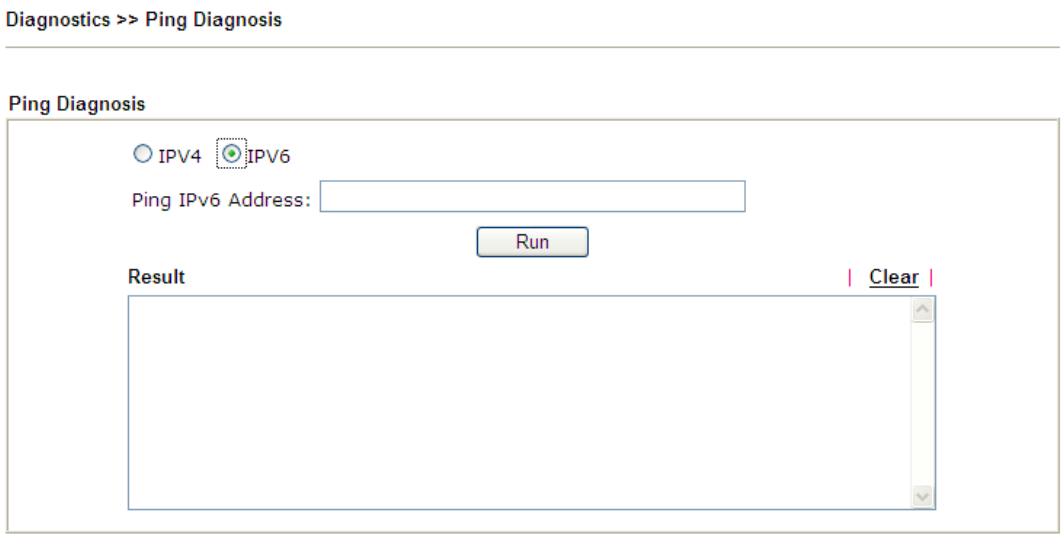
Available settings are explained as follows:

Item	Description
Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the modem used for NAT.
Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It displays the representing number for different interface.
Refresh	Click it to reload the page.

3.9.7 Ping Diagnosis

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





Available settings are explained as follows:

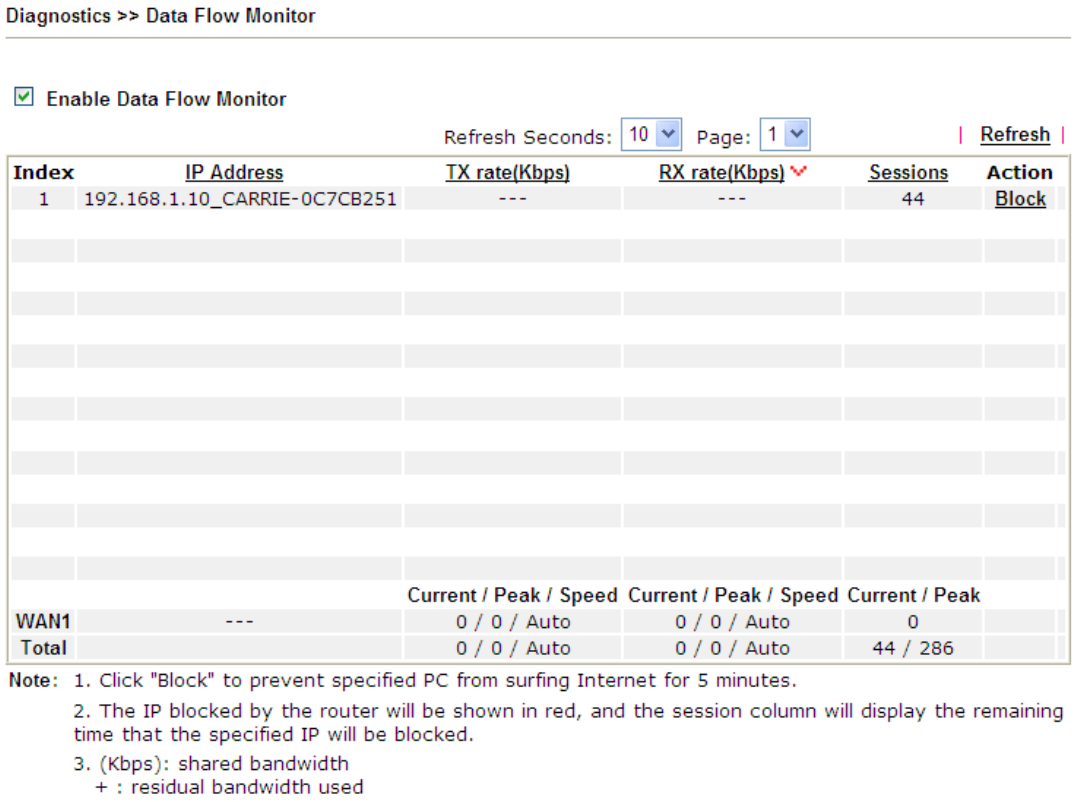
Item	Description
IPV4 /IPV6	Choose the interface for such function.
Ping through	Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the modem automatically.
Ping to	Use the drop down list to choose the destination that you want to ping.
IP Address	Type the IP address of the Host/IP that you want to ping.
Ping IPv6 Address	Type the IPv6 address 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.

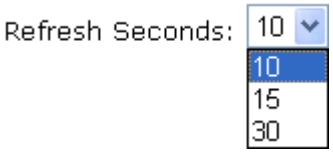
3.9.8 Data Flow Monitor

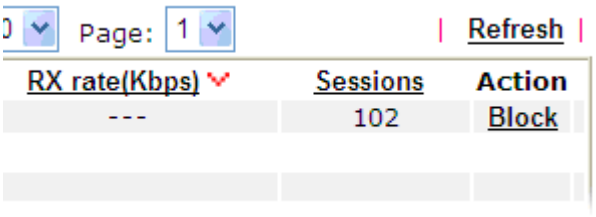
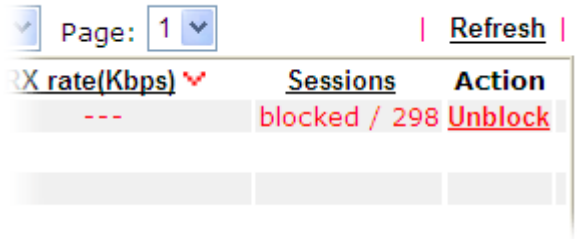
This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds.

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



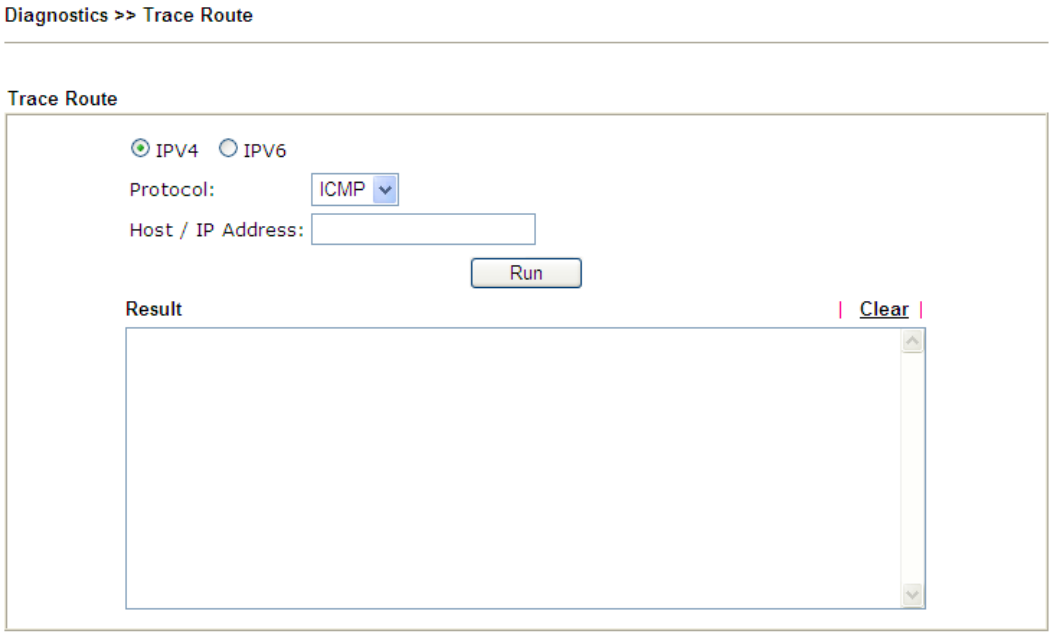
Available settings are explained as follows:

Item	Description
Enable Data Flow Monitor	Check this box to enable this function.
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically. 
Refresh	Click this link to refresh this page manually.
Index	Display the number of the data flow.
IP Address	Display the IP address of the monitored device.
TX rate (kbps)	Display the transmission speed of the monitored device.

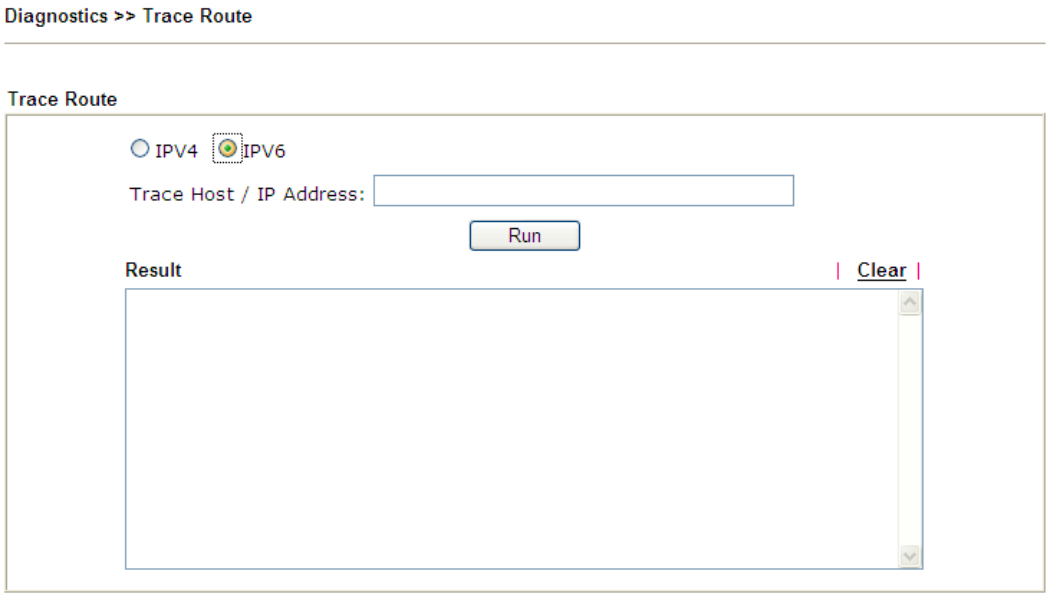
RX rate (kbps)	Display the receiving speed of the monitored device.
Sessions	Display the session number that you specified in Limit Session web page.
Action	**Block** - can prevent specified PC accessing into Internet within 5 minutes.  **Unblock** – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column. 
Current /Peak/Speed	**Current** means current transmission rate and receiving rate for WAN interface. **Peak** means the highest peak value detected by the modem in data transmission. **Speed** means line speed specified in **WAN>>General Setup**. If you do not specify any rate at that page, here will display **Auto** for instead.

3.9.9 Trace Route

Click **Diagnostics** and click **Trace Route** to open the web page. This page allows you to trace the routes from modem 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.



or



Available settings are explained as follows:

Item	Description
IPv4 / IPv6	Click one of them to display corresponding information for it.
Protocol	Use the drop down list to choose the protocol that you want to ping through.

Host/IP Address	It indicates the IP address of the host.
Trace Host/IP Address	It indicates the IPv6 address of the host.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

3.9.10 TSPC Status

IPv6 TSPC status web page could help you to diagnose the connection status of TSPC.

If TSPC has configured properly, the modem will display the following page when the user connects to tunnel broker successfully.

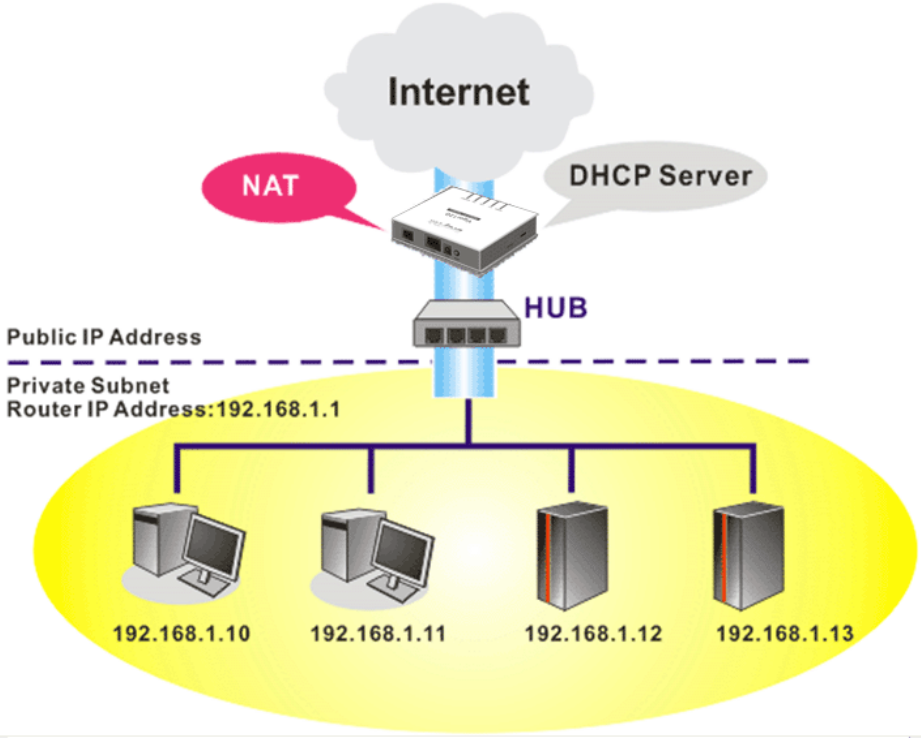
Available settings are explained as follows:

Item	Description
Refresh	Click this link to refresh this page manually.

4 Application and Examples

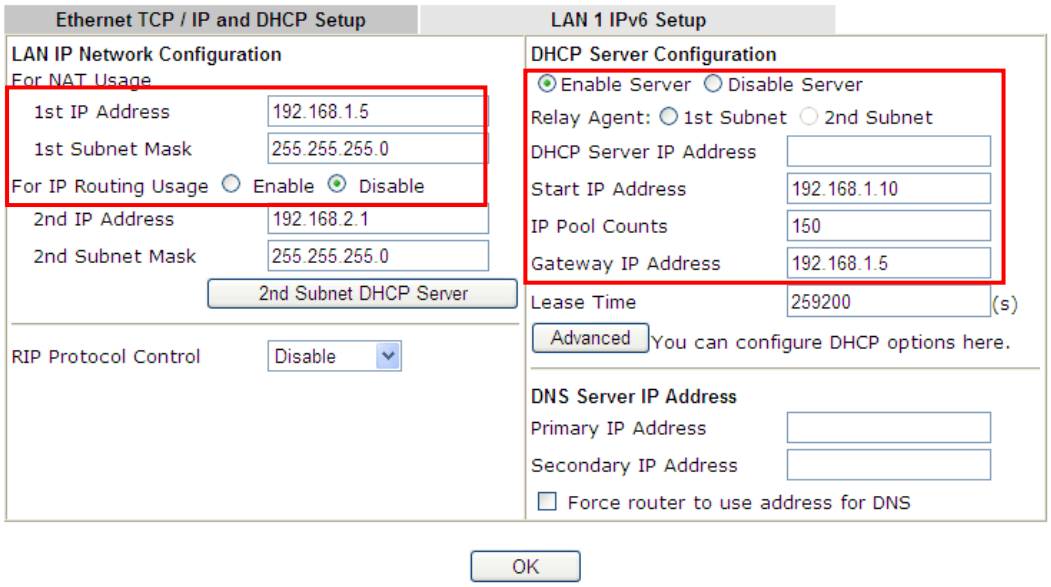
4.1 LAN – Created by Using NAT

An example of default setting and the corresponding deployment are shown below. The default Vigor modem 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.

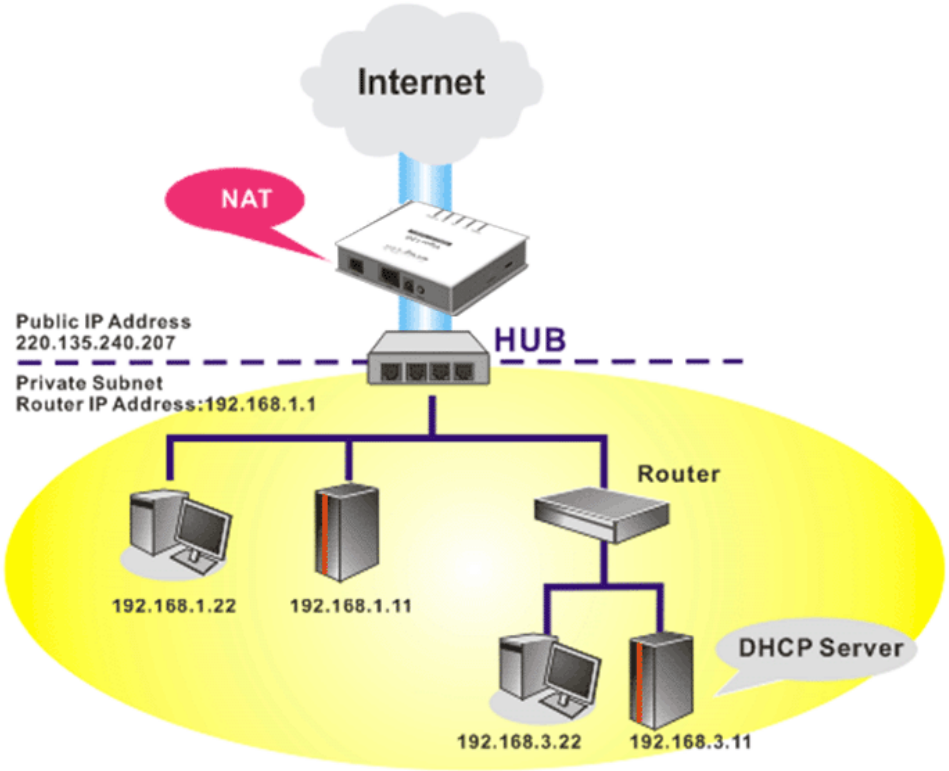


You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.

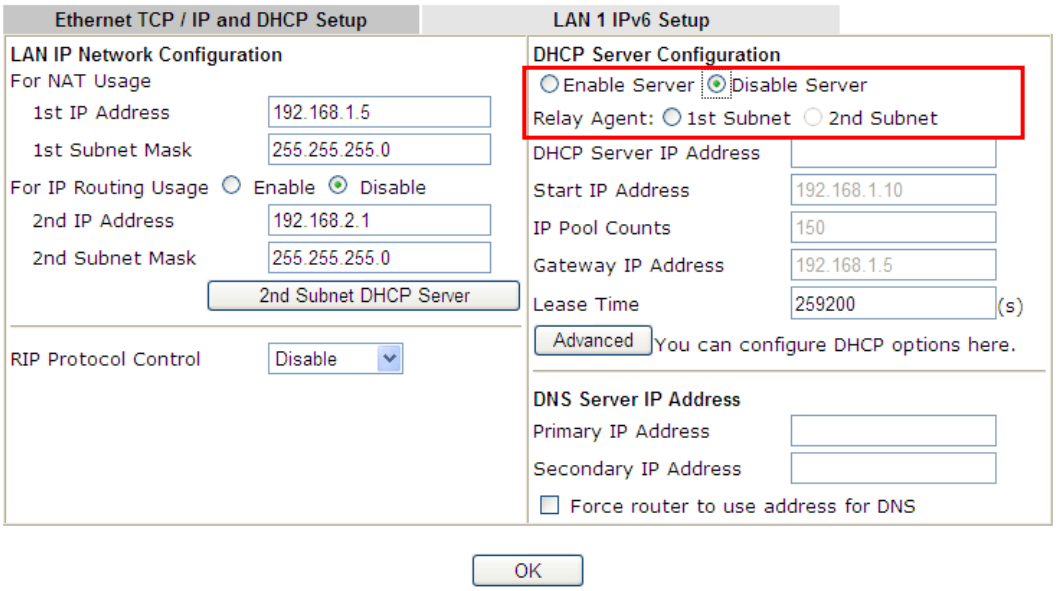
LAN >> General Setup



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



LAN >> General Setup



5 Trouble Shooting

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

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the modem 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 modem still cannot run normally, it is the time for you to contact your dealer for advanced help.

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check the power line and DSL/LAN cable connections.
   Refer to "**1.3 Hardware Installation"** for details.
2. Power on the modem. Make sure the **ACT** LED and **LAN** LED are bright.
3. If not, it means that there is something wrong with the hardware status. Simply back to **"1.3 Hardware Installation"** to execute the hardware installation again. And then, try again.

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

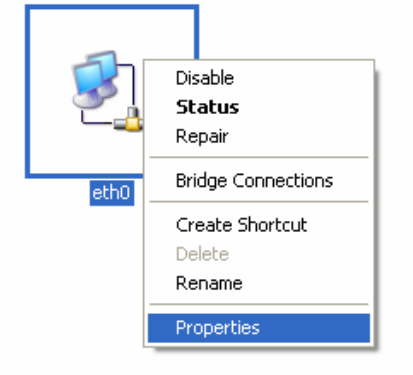
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

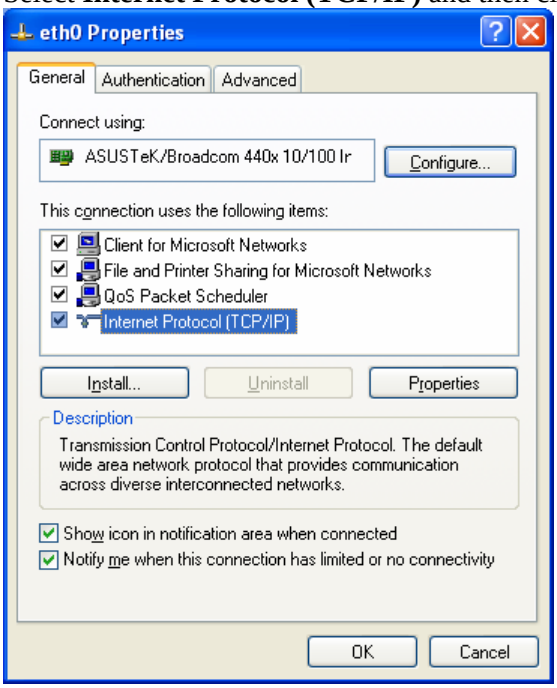
> The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

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

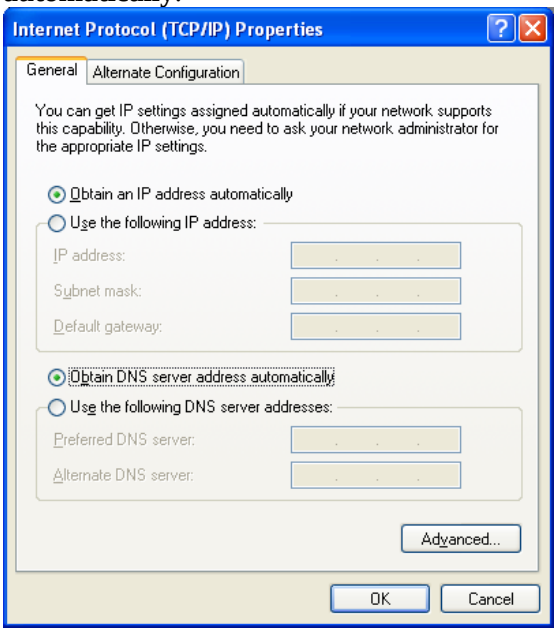
2. Right-click on **Local Area Connection** and click on **Properties**.



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

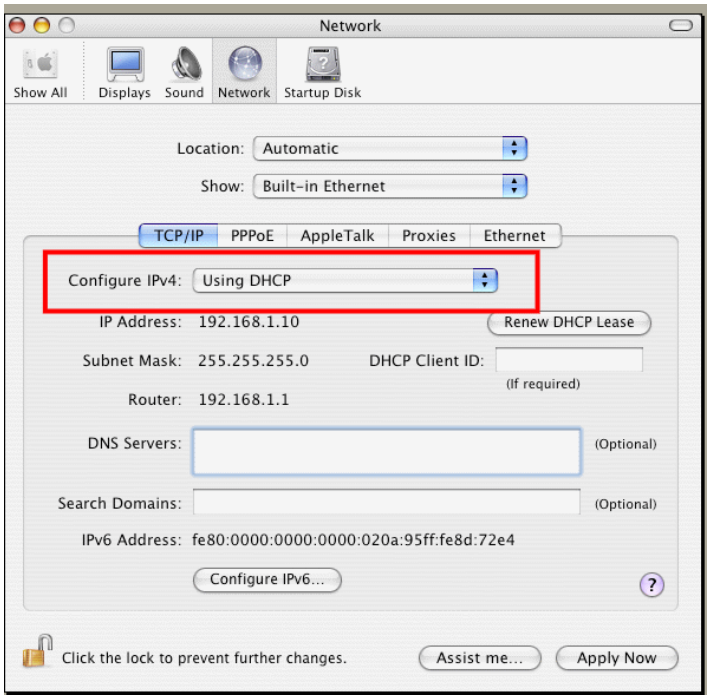


4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



For MacOs

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



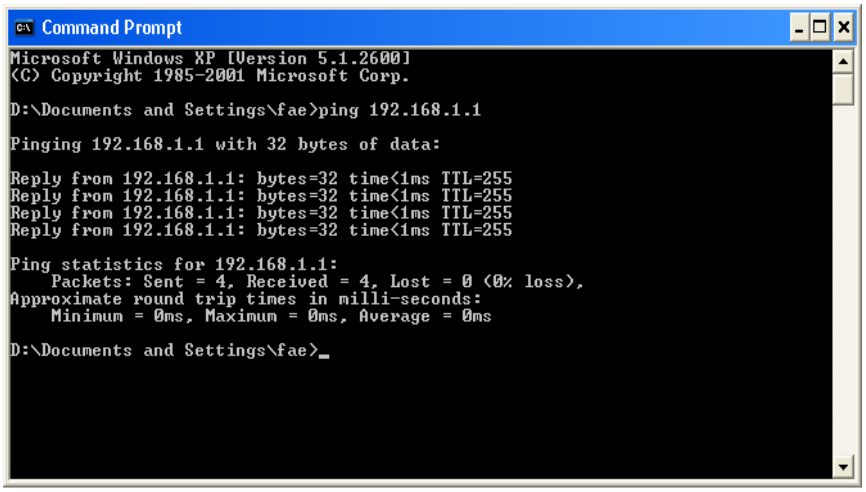
5.3 Pinging the Modem from Your Computer

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

Please follow the steps below to ping the modem correctly.

For Windows

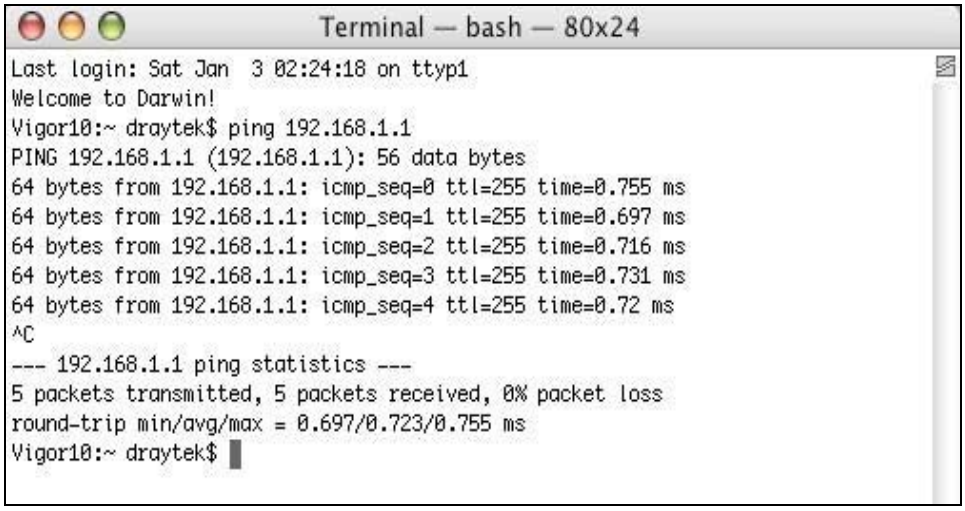
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista). The DOS command dialog will appear.



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

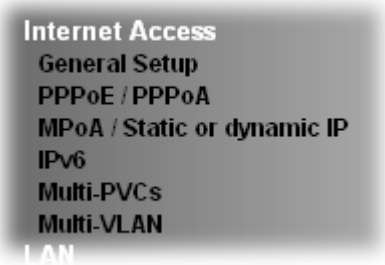
For MacOs (Terminal)

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



5.4 Checking If the ISP Settings are OK or Not

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



5.5 Backing to Factory Default Setting If Necessary

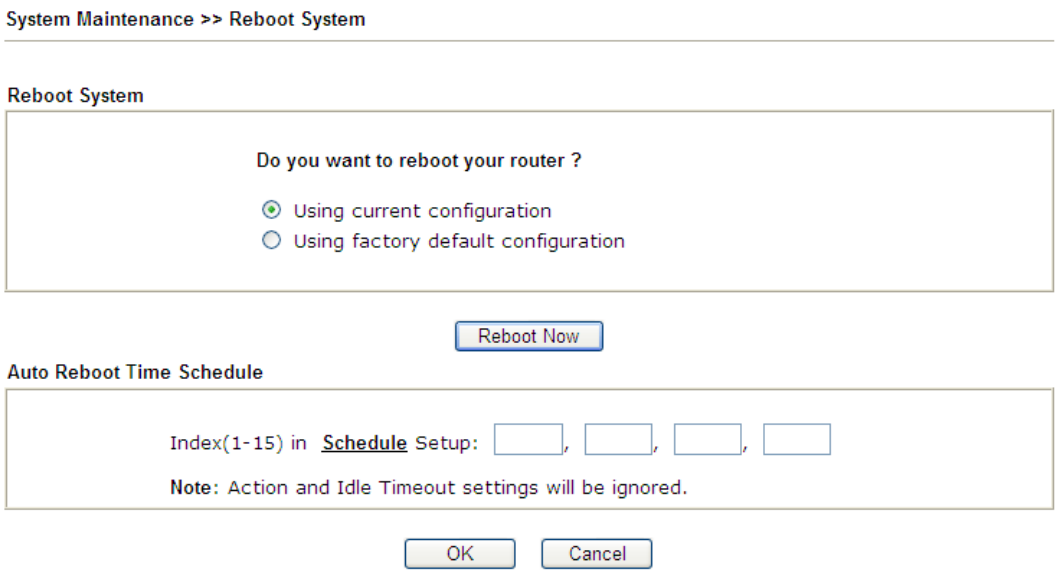
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the modem by software or hardware.

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

Software Reset

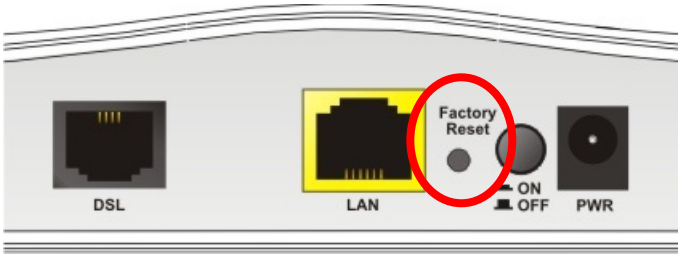
You can reset the modem to factory default via Web page.

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



Hardware Reset

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



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

5.6 Contacting Your Dealer

If the modem 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.