DrayTek

Vigor122

ADSL2/2+ Modem

Your reliable networking solutions partner

User's Guide

V1.0

Vigor122
ADSL2/2+ Modem

User's Guide

Version: 1.0

Firmware Version: V3.2.10

(For future update, please visit DrayTek web site)

Date: July 4, 2016

Copyrights

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, 7 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

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

Be a Registered Owner

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

Firmware & Tools Updates

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

  http://www.DrayTek.com

European Community Declarations

Manufacturer: DrayTek Corp.

Address: No. 26, Fu Shing Road, Hukou Township, Hsinchu Industrial Park, Hsinchu County, Taiwan 303

Product: Vigor122

DrayTek Corp. declares that Vigor122 is in compliance with the following essential requirements and other relevant provisions of R&TTE 1999/5/EC, ErP 2009/125/EC and RoHS 2011/65/EU.

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.

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

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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

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

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

More update, please visit www.draytek.com.

Table of Contents

Part I Installation 1

I-1 Introduction 2

I-1-1 Indicators and Connectors 3

I-2 Hardware Installation 5

I-2-1 Installing Vigor Device 5

I-3 Accessing Web Page 6

I-4 Changing Password 8

I-5 Online Status 9

I-6 Quick Start Wizard 11

I-6-1 Setting PPPoE/PPPoA Connection 11

I-6-2 Setting Routed IP/Bridged IP Connection 14

Part II Connectivity 17

II-1 Internet Access 18

Web User Interface 19

II-1-1 Internet Access 19

II-1-1-1 Details Page for PPPoE/PPPoA 19

II-1-1-2 Details Page for MPoA 21

II-1-2 Multi-PVCs 25

II-2 LAN 27

Web User Interface 28

II-2-1 General Setup 28

II-3 NAT 30

Web User Interface 31

II-3-1 Port Redirection 31

II-3-2 DMZ Host 34

II-3-3 Open Ports 36

II-4 Applications 38

Web User Interface 39

II-4-1 Dynamic DNS 39

II-4-2 Schedule 41

II-4-3 UPnP 43

II-4-4 IGMP 45

II-5 Routing 46

Web User Interface 46

II-5-1 Static Route 46

Part III Security 49

III-1 Firewall 50

Web User Interface 52

III-1-1 General Setup 52
III-1-2 Filter Setup 53
III-1-3 DoS Defense 57

Part IV Management 61

IV-1 System Maintenance 62
Web User Interface 63
IV-1-1 System Status 63
IV-1-2 TR-069 64
IV-1-3 Administrator Password 65
IV-1-4 Configuration Backup 66
IV-1-5 Syslog/Mail Alert 68
IV-1-6 Time and Date 70
IV-1-7 Management 71
IV-1-8 Reboot System 72
IV-1-9 Firmware Upgrade 73

Part V Others 75

V-1 Objects Settings 76
Web User Interface 77
V-1-1 IP Object 77
V-1-2 IP Group 79
V-1-3 Service Type Object 80
V-1-4 Service Type Group 82

Part VI Troubleshooting 85

VI-1 Diagnostics 86
Web User Interface 87
VI-1-1 Dial-out Triggering 87
VI-1-2 Routing Table 88
VI-1-3 ARP Cache Table 88
VI-1-4 DHCP Table 89
VI-1-5 NAT Sessions Table 90
VI-1-6 Ping Diagnosis 90
VI-1-7 Trace Route 91
VI-2 Checking If the Hardware Status Is OK or Not 92
VI-3 Checking If the Network Connection Settings on Your Computer Is OK or Not 93
VI-4 Pinging the modem from Your Computer 96
VI-5 Checking If the ISP Settings are OK or Not 98
VI-6 Backing to Factory Default Setting If Necessary 98
VI-7 Contacting DrayTek 99

Part VII Telnet Commands 101

Accessing Telnet of Vigor122 102

Part I Installation

This part will introduce Vigor router and guide to install the device in hardware and software.

I-1 Introduction

This is a generic International version of the user guide. Specification, compatibility and features vary by region. For specific user guides suitable for your region or product, please contact local distributor.

Vigor122, an ADSL2/2+ modem, integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

DrayTek Vigor122 supports PPPoE/PPPoA relay (PPPoA to PPPoE bridging) and the firewall, router or PC all can log into the Internet (your ISP) directly, having complete control over the ADSL connection.

Therefore it is possible to connect a PPPoE client to the Vigor122 (firewall, Ethernet-WAN router, Apple Airpor or PC) even if the connection to your ISP is still PPPoA (unlike other-brand modems which only offers PPPoE native bridging). This unique feature is very convenient for PPPoA -based ISPs.

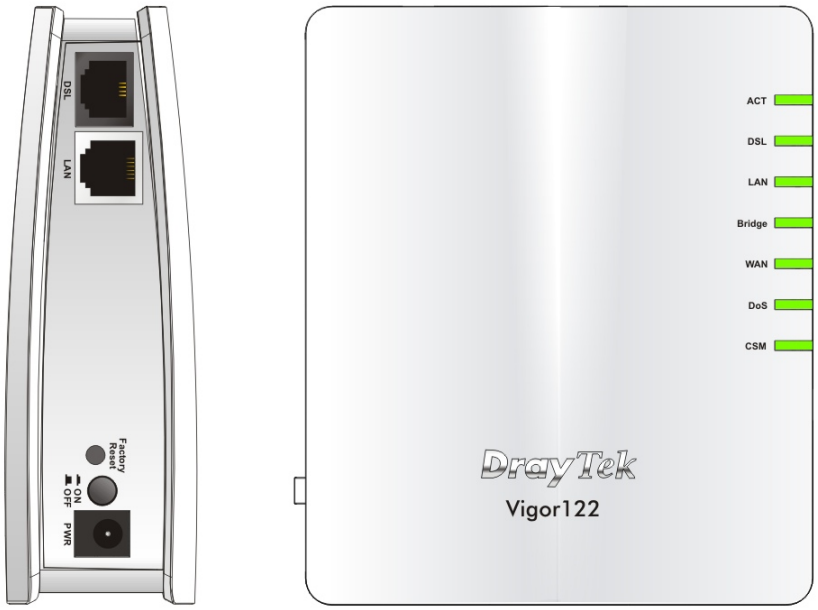
With the Vigor122 bridge/modem, you can have a true single public IP address (or multiple, if you subscribe them) rightly through to your router/or firewall, which also has full control of the ISP connection.

Accordingly, it is ideal for home users and client running multi WAN routers like the Vigor3900, Vigor2960, Vigor3220, Vigor2952, Vigor2925, Vigor2912 series and even connecting to the second WAN port on the Vigor2860 series.

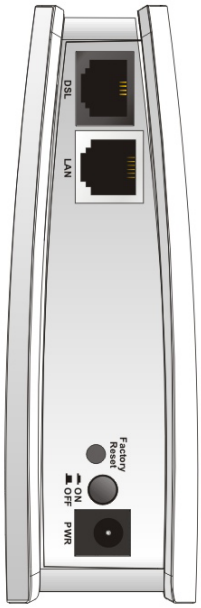
The Vigor122 supports TR-069 and it works with most TR-069-based central management system. VigorACS centralized management system can also facilitate ISP's deployment of installing Vigor122 and provide professional remote management for ISP.

I-1-1 Indicators and Connectors

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



LED	Status	Explanation
ACT	Off	The system is not ready or is failed.
	Blinking	The system is ready and can work normally.
DSL	On	DSL connection synchronized.
	Blinking	DSL connection is synchronizing.
LAN	On	A normal connection is through its corresponding port.
	Off	LAN is disconnected.
	Blinking	Data is transmitting (sending/receiving).
Bridge	On	Bridge mode is enabled.
	Off	Bridge mode is disabled.
WAN	On	Internet connection is established.
	Off	Internet connection is not established.
	Blinking	Data is transmitting (sending/receiving).
DoS	On	The DoS/DDoS function is active.
	Blinking	It will blink while detecting an attack.
CSM	On	The profile(s) of CSM (Content Security Management) for IM/P2P, URL/Web Content Filter application can be enabled from Firewall >>General Setup. (Such profile must be established under CSM menu).



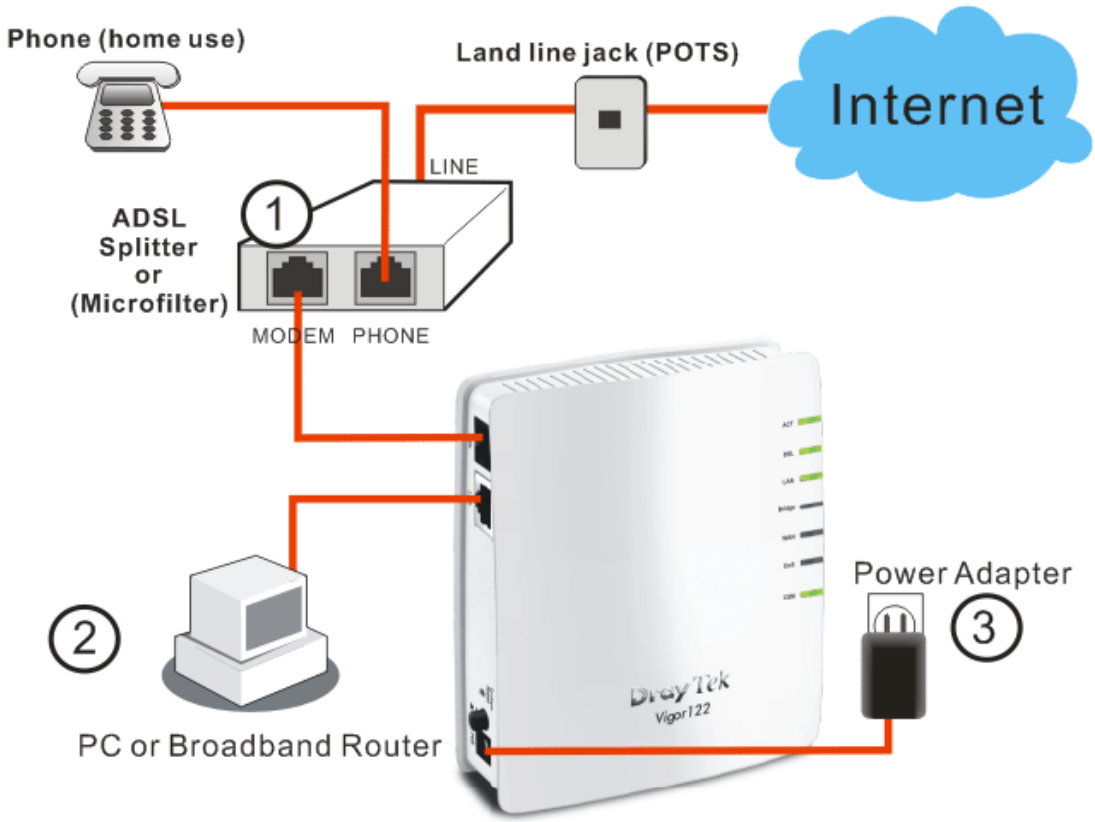
Interface	Description
DSL	Connecter for accessing the Internet through ADSL2/2+.
LAN	Connecter for xDSL / Cable modem or router.
Factory Reset	Restore the default settings. Usage: Turn on the modem. Press the button and keep for more than 10 seconds. Then the modem will restart with the factory default configuration.
On/Off	Power switch.
PWR	PWR: Connecter for a power adapter.

Info For the sake of security, make the accessory kit away from children.

I-2 Hardware Installation

I-2-1 Installing Vigor Device

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



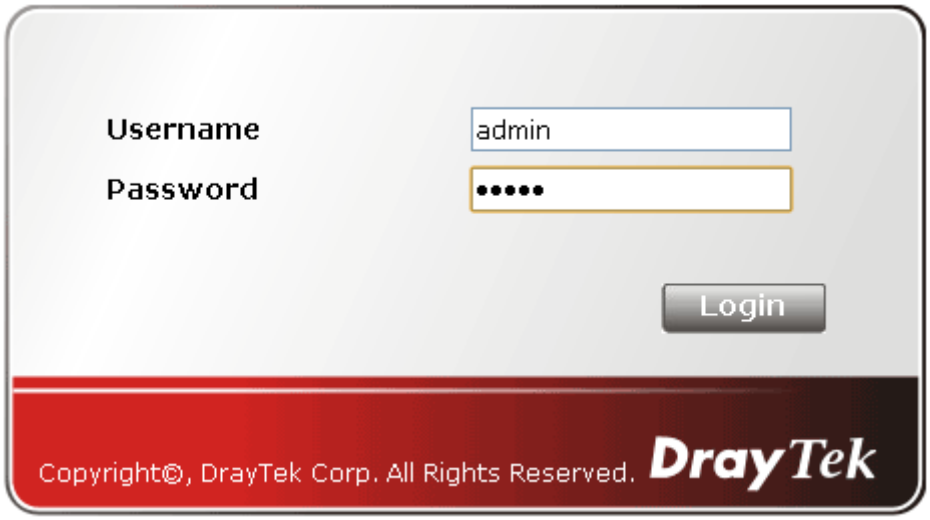
1. Connect the DSL interface to the MODEM port of external ADSL splitter with an ADSL line cable.
2. Connect the LAN port to your computer with a RJ-45 cable.
3. Connect one end of the power adapter to the Power port of this device. Connect the other end to the wall outlet of electricity.
4. Power on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

I-3 Accessing Web Page

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

   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 router 192.168.1.1**. For the detailed information, please refer to the later section - Trouble Shooting of the guide.

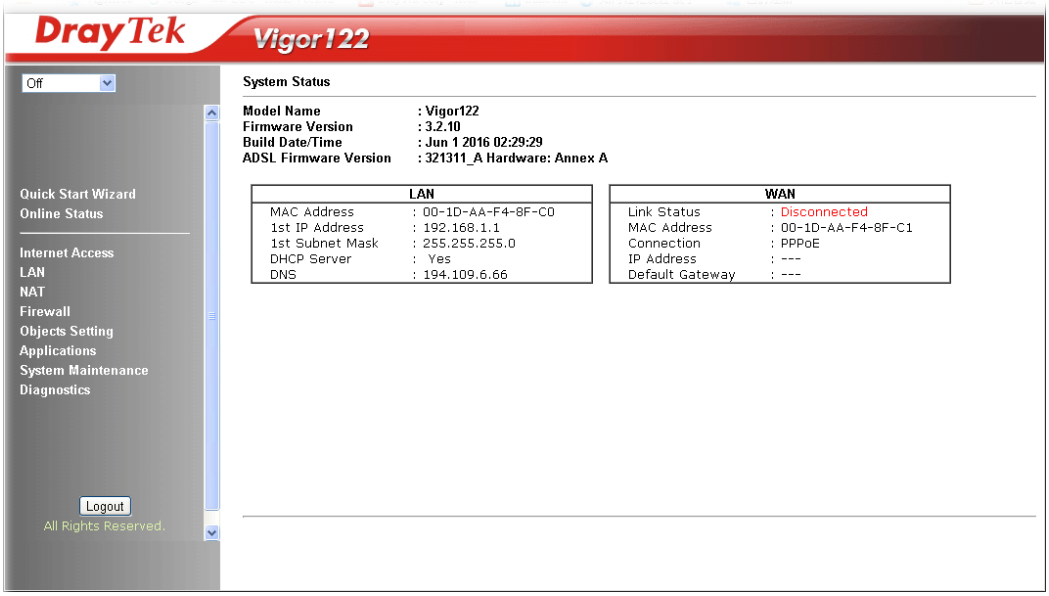
2. Open a web browser on your PC and type **http://192.168.1.1.** The following window will be open to ask for username and password.



3. Please type “admin/admin” as the Username/Password and click **Login**.

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

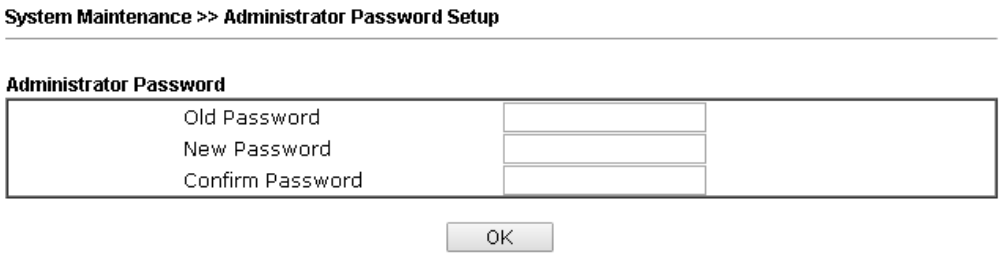
4. Now, the **Main Screen** will appear.



I-4 Changing Password

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

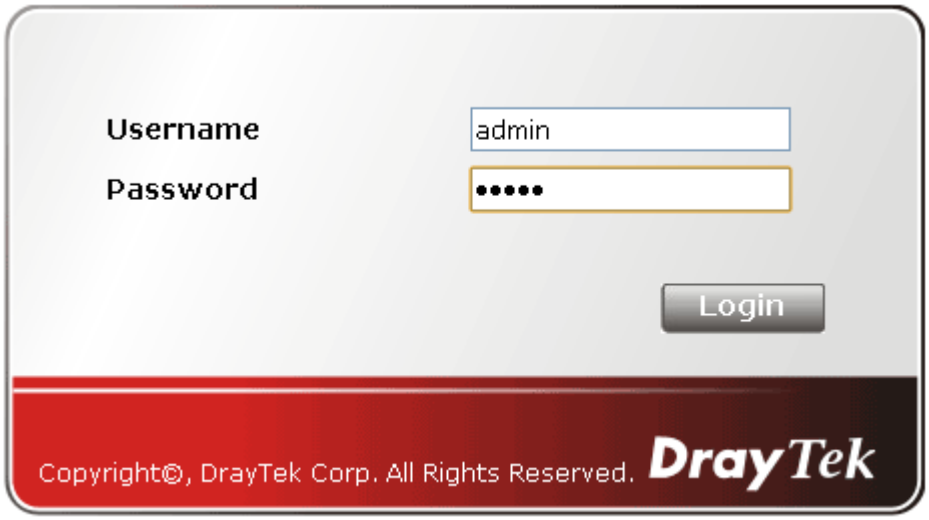
1. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for username and password.
2. Please type “admin/admin” as Username/Password for accessing into the web user interface with admin mode.
3. Go to **System Maintenance** page and choose **Administrator Password**.



4. Enter the login password (the default is “admin”) on the field of **Old Password**. Type **New Password** and **Confirm Password**. Then click **OK** to continue.

Info	The maximum length of the password you can set is 23 characters.

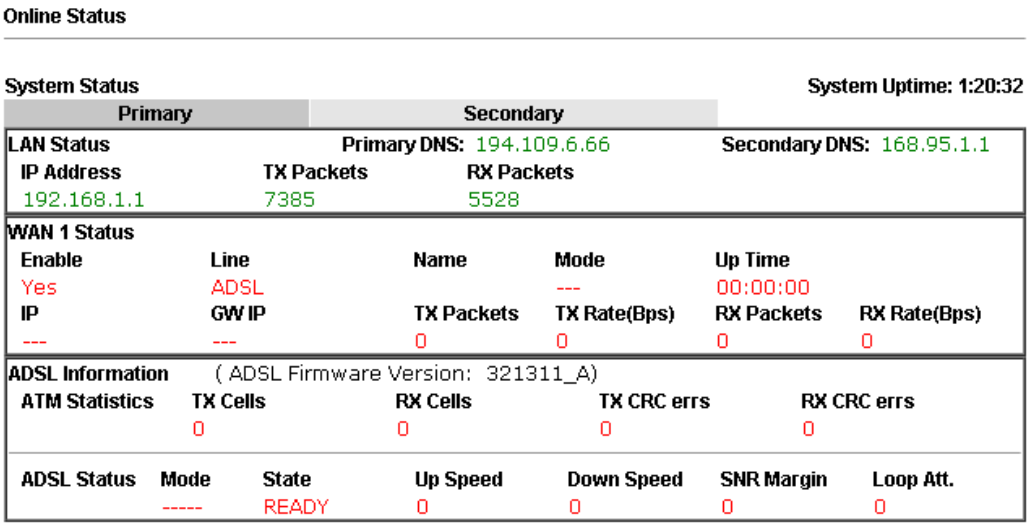
5. Now, the password has been changed. Next time, use the new password to access the Web user interface for this router.



Info	Even the password is changed, the Username for logging onto the web user interface is still “admin”.

I-5 Online Status

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



Detailed explanation (for IPv4) is shown below:

Item	Description
LAN Status	**Primary DNS-**Displays the primary DNS server address for WAN interface. **Secondary DNS -**Displays the secondary DNS server address for WAN interface. **IP Address**-Displays the IP address of the LAN interface. **TX Packets**-Displays the total transmitted packets at the LAN interface. **RX Packets**-Displays the total received packets at the LAN interface.
WAN1 Status	**Enable – Yes** in red means such interface is available but not enabled. **Yes** in green means such interface is enabled. **Line** – Displays the physical connection of this interface. **Name** – Display the name of the modem. **Mode** - Displays the type of WAN connection (e.g., PPPoE). **Up Time** - Displays the total uptime of the interface. **IP** - Displays the IP address of the WAN interface. **GW IP** - Displays the IP address of the default gateway. **TX Packets** - Displays the total transmitted packets at the WAN interface. **TX Rate** - Displays the speed of transmitted octets at the WAN interface. **RX Packets** - Displays the total number of received packets at the WAN interface. **RX Rate** - Displays the speed of received octets at the WAN interface.
ADSL Information	**ATM Statistics –** Display the ATM layer information.

Item	Description
	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.

Info

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

I-6 Quick Start Wizard

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

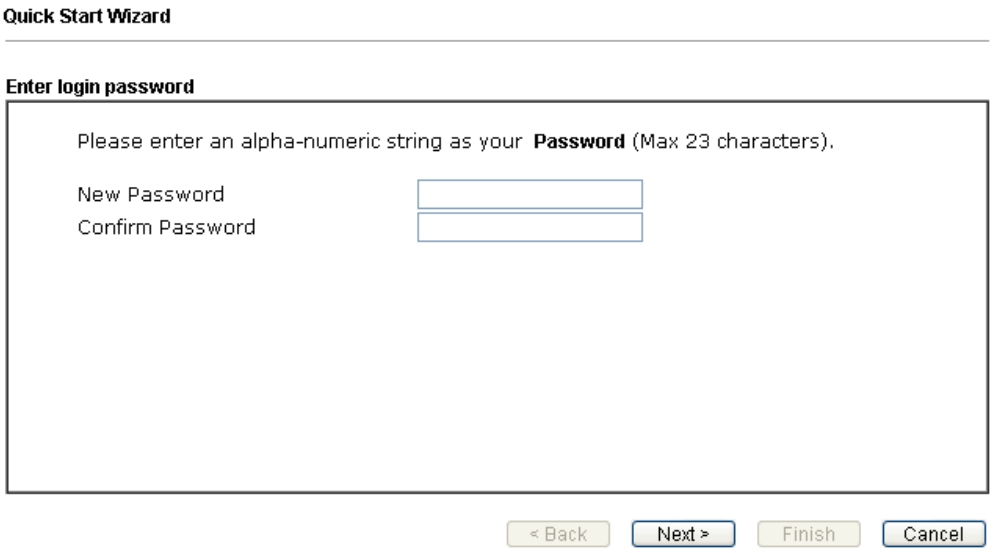
I-6-1 Setting PPPoE/PPPoA Connection

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.

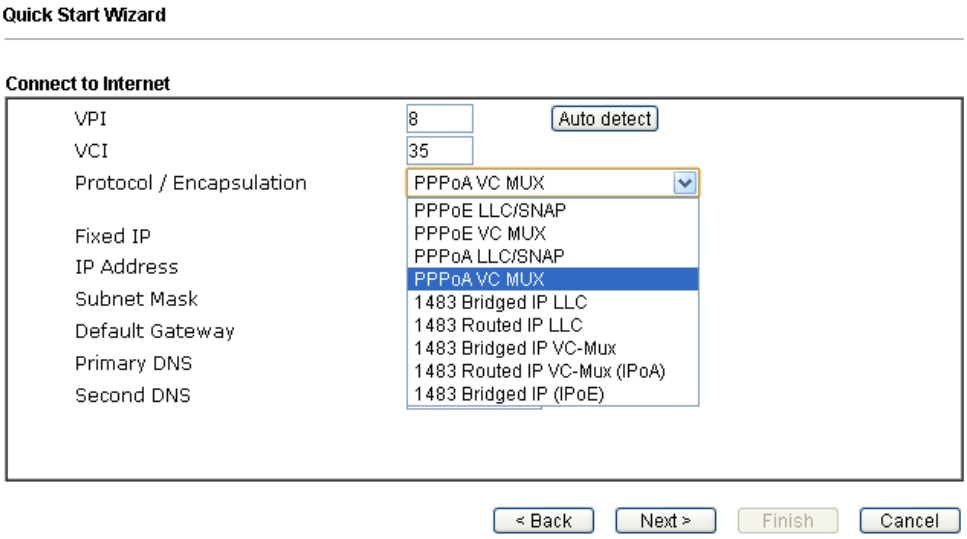
PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.

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**.



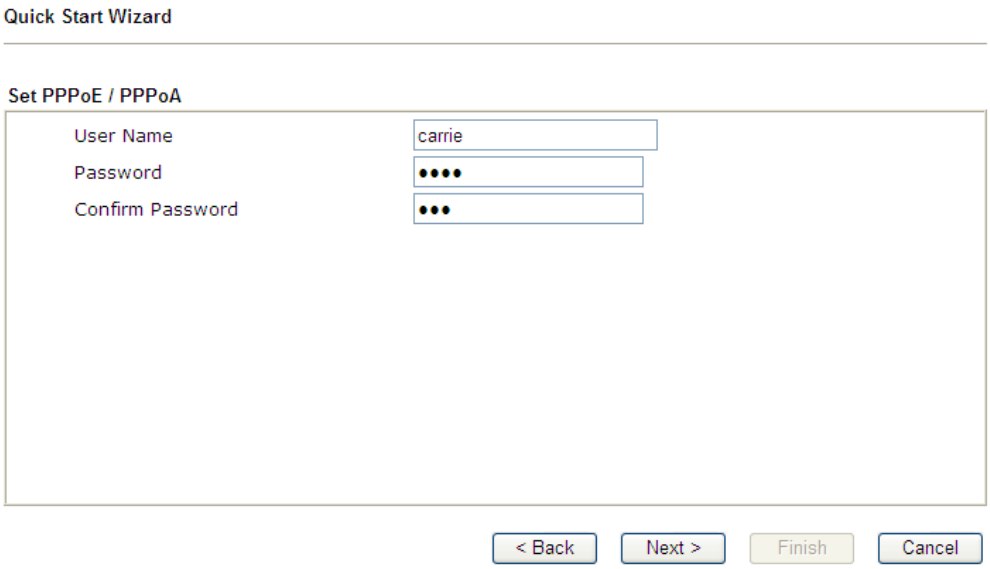
3. You can configure the modem to access the Internet with different protocol/modes such as **PPPoE/PPPoA** or **Bridged** or **Routed**. The modem supports the ADSL WAN interface for Internet access. In this case, choose **PPPoE/PPPoA**.



Available settings are explained as follows:

Item	Description
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.
Auto detect	Click it to detect suitable values below by the modem automatically.
Protocol/Encapsulation	Select an IP mode for this WAN interface. There are several available modes for Internet access such as **PPPoE**, **PPPoA.**
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 **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.

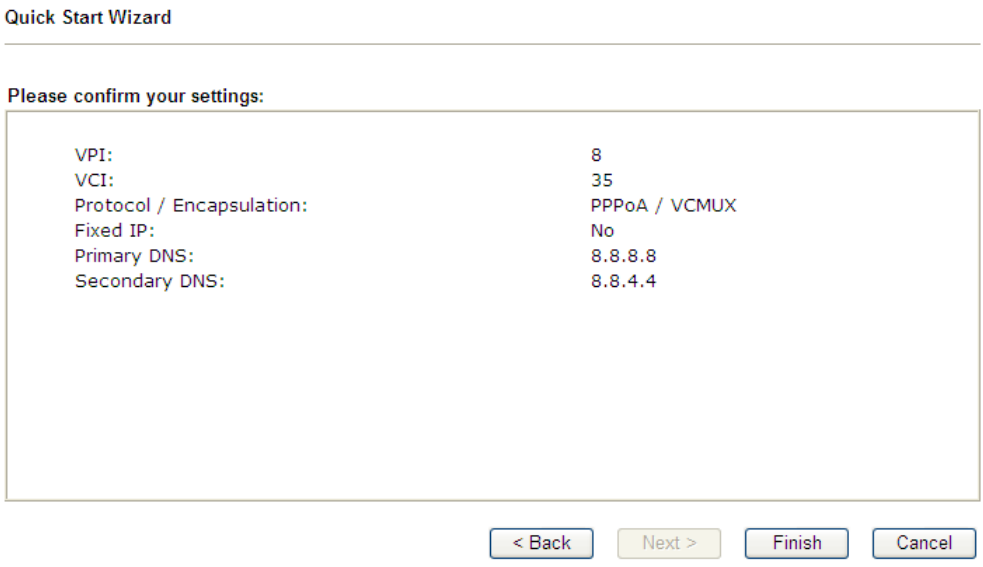
4. After finished the above settings, click **Next** to access into next page.



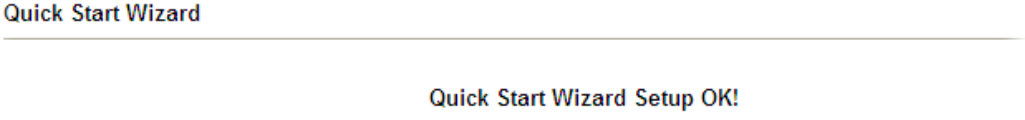
Available parameters are listed belo

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.

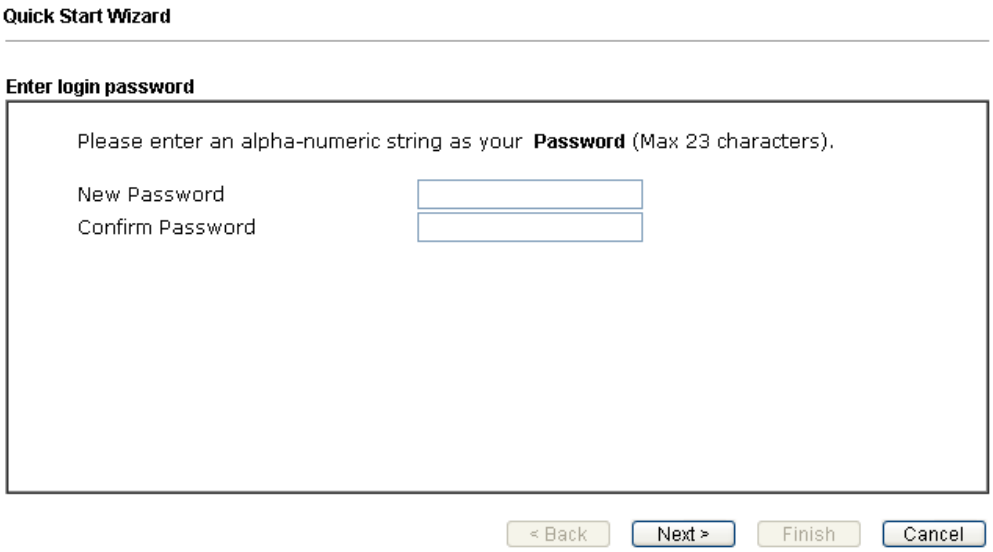


6. Click **Finish.** The Quick Start Wizard Setup OK page will be displayed.

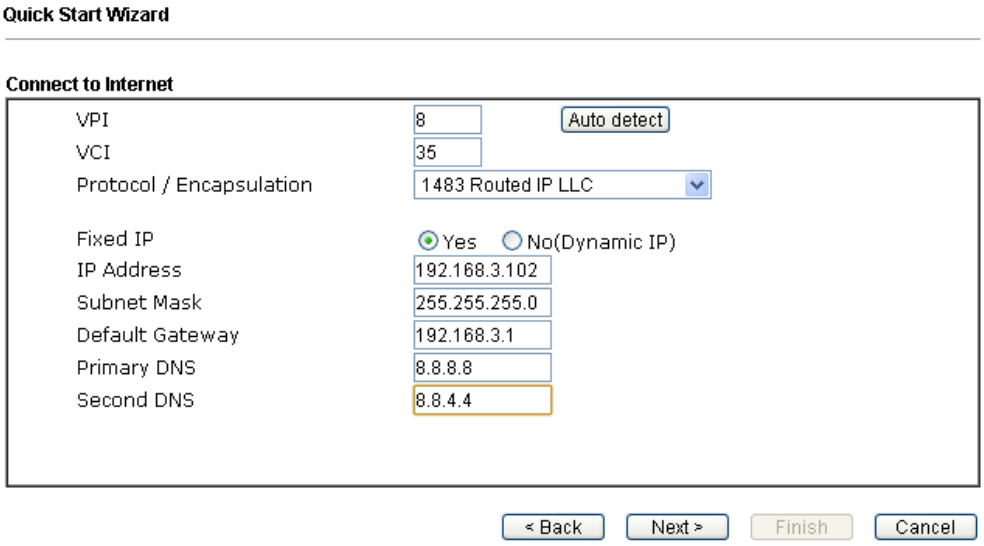


I-6-2 Setting Routed IP/Bridged IP Connection

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. Click **1483 Routed IP** or **1483 Bridged IP** as the Internet Access type. Simply click **Next** to continue.

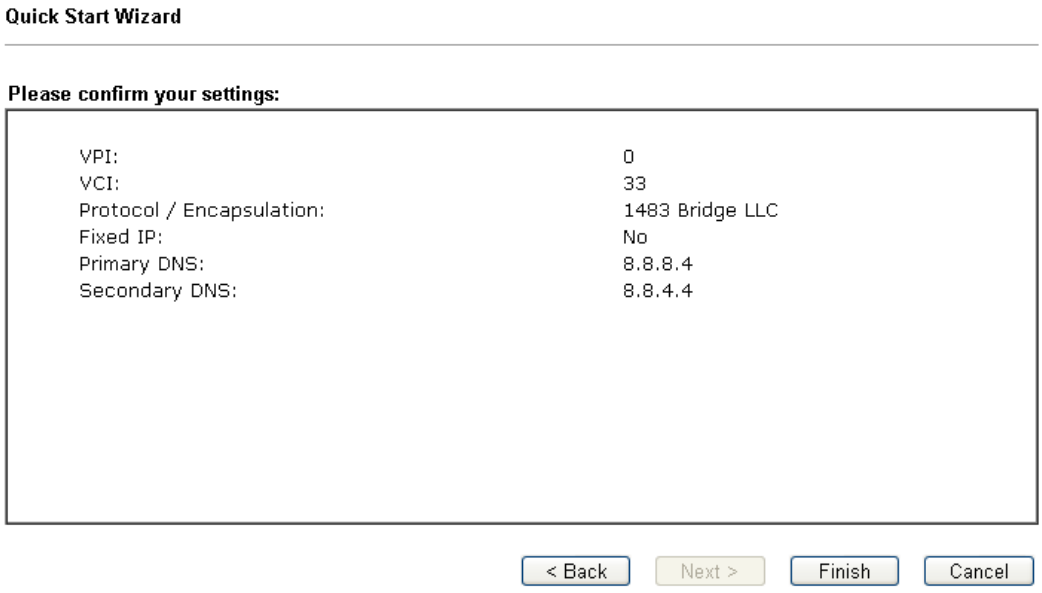


Available settings are explained as follows:

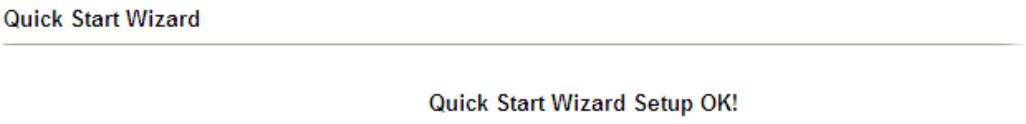
Item	Description
VPI	Stands for **Virtual Path Identifier**. It is an 8-bit header inside each ATM cell that indicates where the cell should be routed. The ATM, is a method of sending data in small packets of fixed sizes. It is used for transferring data to client computers.
VCI	Stands for **Virtual 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.
Auto detect	Click it to detect suitable values below by the modem automatically.
Protocol/Encapsulation	Select an IP mode for this WAN interface. There are several available modes for Internet access such as **1483 Routed IP or 1483 Bridged IP.**
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 **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. Please type in the IP address information originally provided by your ISP. Then click **Next** for next step.



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



6. Now, you can enjoy surfing on the Internet.

This page is left blank.

Part II Connectivity

WAN

It means wide area network. Public IP will be used in WAN.

LAN

It means local area network. Private IP will be used in LAN.

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

NAT

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.

Applications

DDNS, UPnP, IGMP...

Routing

Static Route

II-1 Internet Access

It allows users to access Internet.

Basics of Internet Protocol (IP) Network

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

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

What are Public IP Address and Private IP Address

As the 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 router. The modem itself will also use the default **private IP** address: 192.168.1.1 to communicate with the local hosts. Meanwhile, Vigor router will communicate with other network devices through a **public IP** address. When the data flow passing through, the Network Address Translation (NAT) function of the 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 router begins to connect to your ISP, a serial of discovery process will occur to ask for a connection. Then a session will be created. Your user ID and password is authenticated via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information will usually be assigned by your ISP.

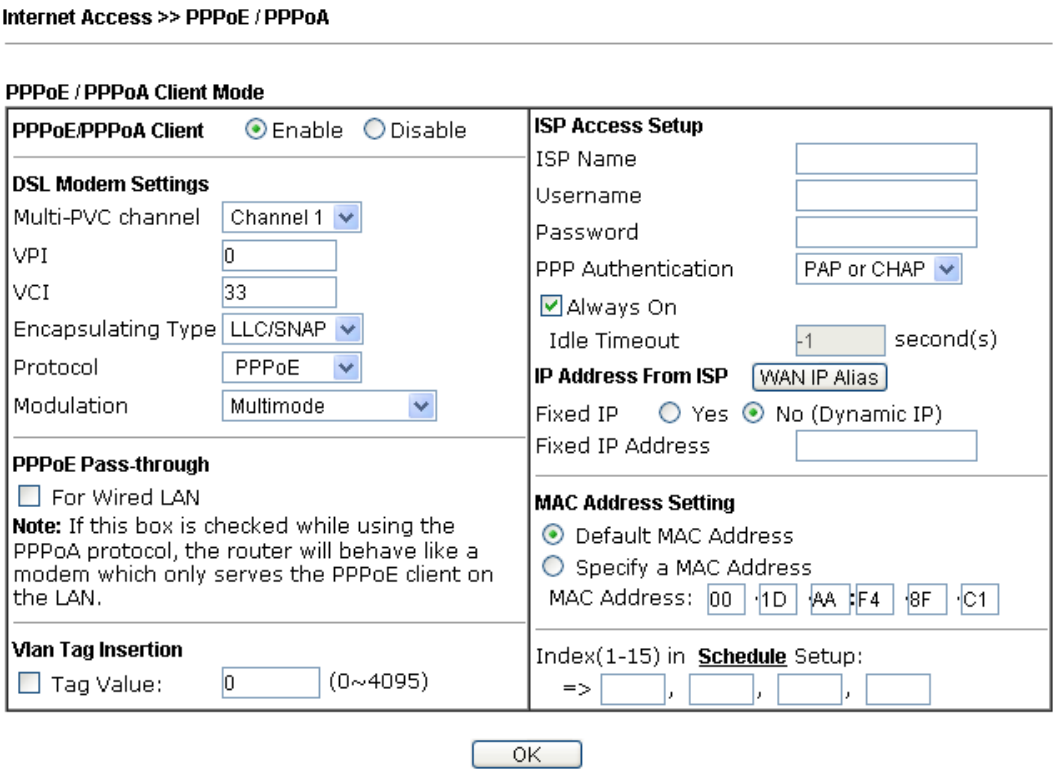
Web User Interface

II-1-1 Internet Access

II-1-1-1 Details Page for 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).

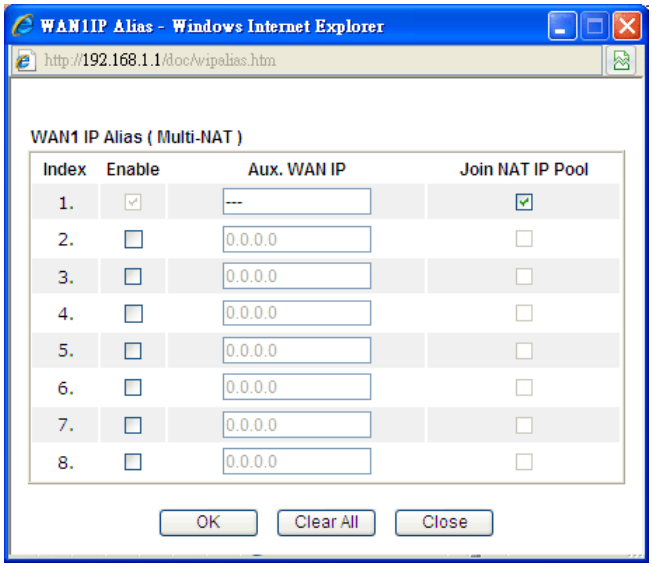
To choose PPPoE or PPPoA as the accessing protocol of the internet, please select **PPPoE/PPPoA** from the **Internet Access** menu. The following web page will be shown.



Available settings are explained as follows:

Item	Description
PPPoE/PPPoA Client	Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.
DSL Modem Settings	Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP.

	Multi-PVC channel - The selections displayed here are determined by the page of **Internet Access** – **Multi PVCs**. **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 Tag Insertion	Check the box to enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out. **Tag value** – Type the value as the VLAN ID number. The range is form 0 to 4095.
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. The maximum length of the user name you can set is 63 characters. **Password** – Type in the password provided by ISP in this field. The maximum length of the password you can set is 62 characters. **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.
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**.
MAC Address Setting	**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.

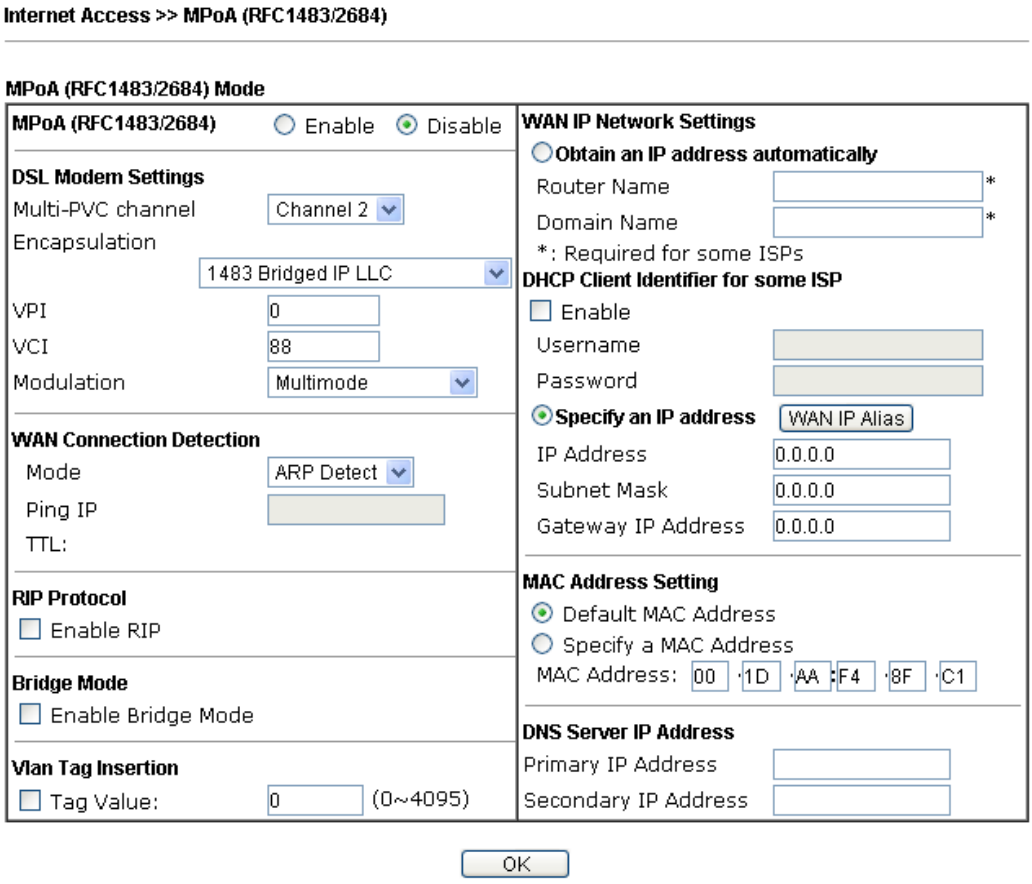
After finishing all the settings here, please click **OK** to activate them.

II-1-1-2 Details Page for MPoA

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

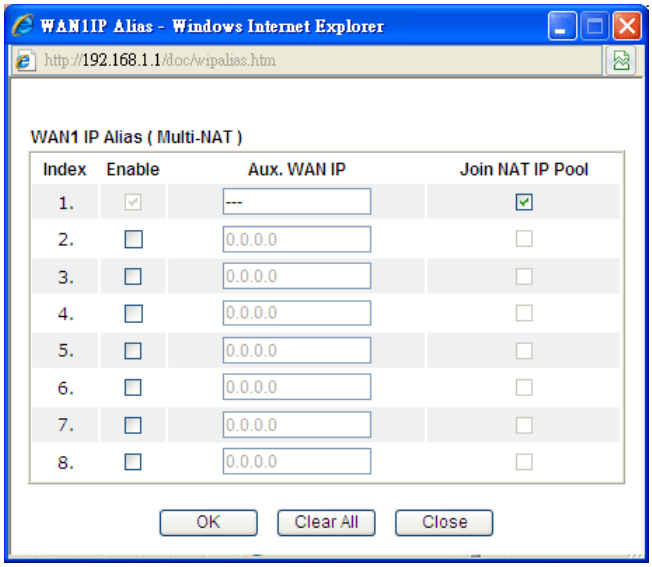
For static IP mode, you usually receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your DSL or Cable ISP service providers. In most cases, a Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you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

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



Available settings are explained as follows:

Item	Description
MPoA (RFC1483/2684)	Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.
DSL Modem Settings	Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP. **Multi-PVC channel** - The selections displayed here are determined by the page of **Internet Access** – **Multi PVCs**. **Encapsulating Type** - Drop down the list to choose the type provided by ISP. **VPI** - Type in the value provided by ISP. **VCI** - Type in the value provided by ISP. **Modulation** – Choose a suitable method for such connection.
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.
RIP Protocol	Routing Information Protocol is abbreviated as RIP（RFC1058） specifying how modems exchange routing tables information. Click **Enable RIP** for activating this function.

Vlan Tag Insertion	Check the box to enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out. **Tag value** – Type the value as the VLAN ID number. The range is form 0 to 4095.
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.
MAC Address Setting	**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.

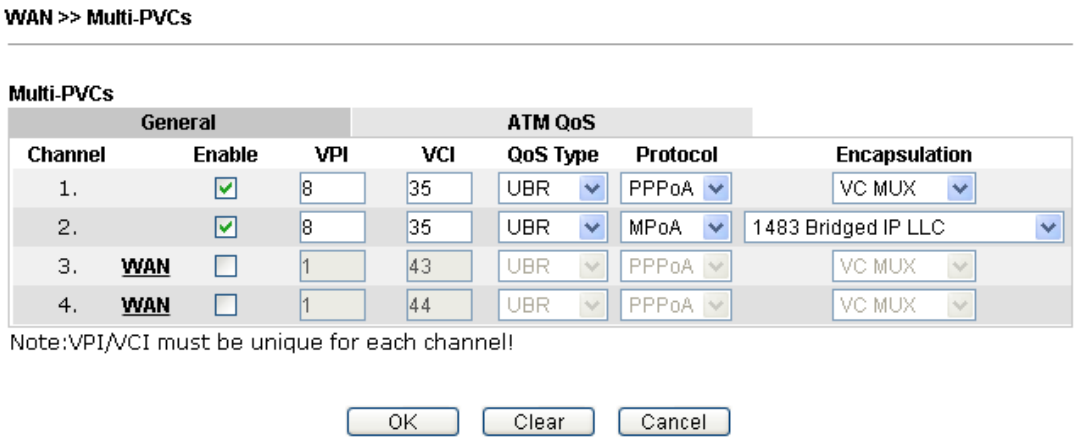
DNS Server IP Address	Type in the primary IP address for the modem. If necessary, type in secondary IP address for necessity in the future.

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

II-1-2 Multi-PVCs

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

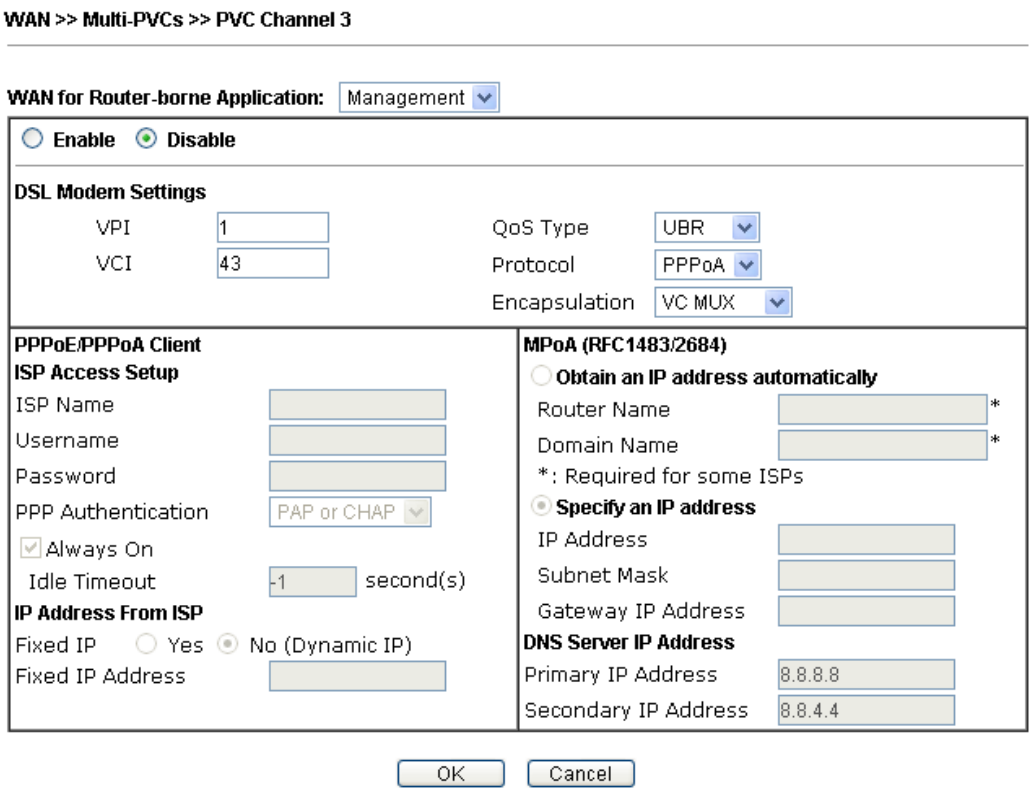
The system allows you to set up to eight channels which are ready for choosing as the first PVC line that will be used as multi-PVC.



Available settings are explained as follows:

Item	Description
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 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:

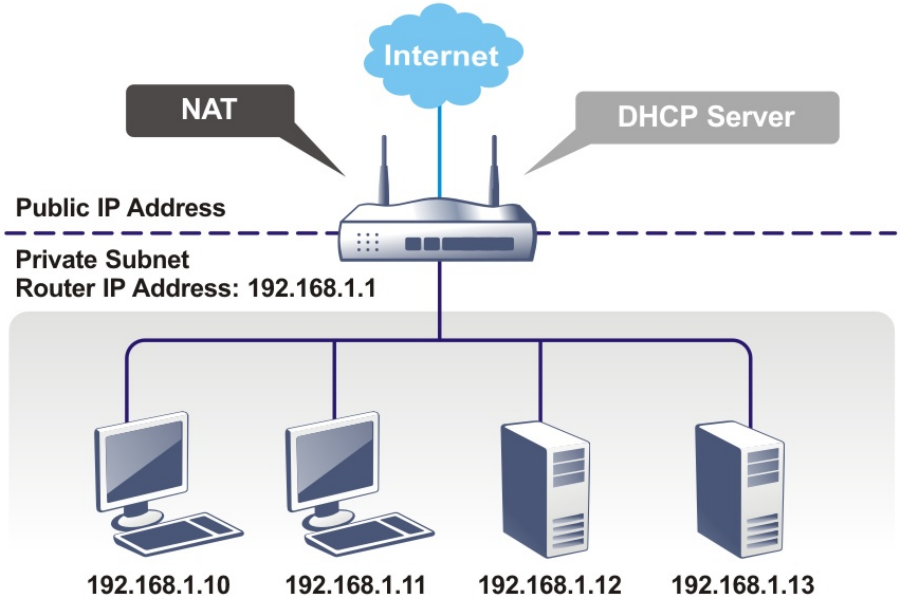
Item	Description
WAN for Router-borne Application	**Management** can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this VLAN will be effective for Web configuration/telnet/TR069.
DSL Modem Settings	Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP. **VPI** - Type in the value provided by ISP. **VCI** - Type in the value provided by ISP. **QoS Type** - Drop down the list to choose the type provided by ISP. **Protocol** - Drop down the list to choose the one provided by ISP. **Encapsulation -** Drop down the list to choose the type provided by ISP.

After finished the above settings, click **OK** to save the settings and return to previous page.

II-2 LAN

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

The most generic function of Vigor router 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 router has a built-in DHCP server that assigns private IP address to each local host. See the following diagram for a briefly understanding.



What is Routing Information Protocol (RIP)

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

What is Static Route

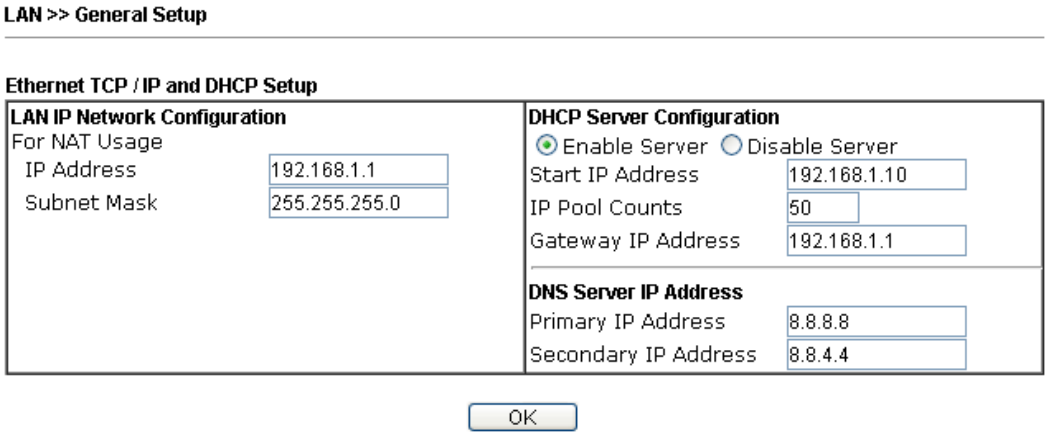
When you have several subnets in your LAN, sometimes a more effective and quicker way for connection is the **Static routes** function rather than other method. You may simply set rules to forward data from one specified subnet to another specified subnet without the presence of RIP.

Web User Interface

II-2-1 General Setup

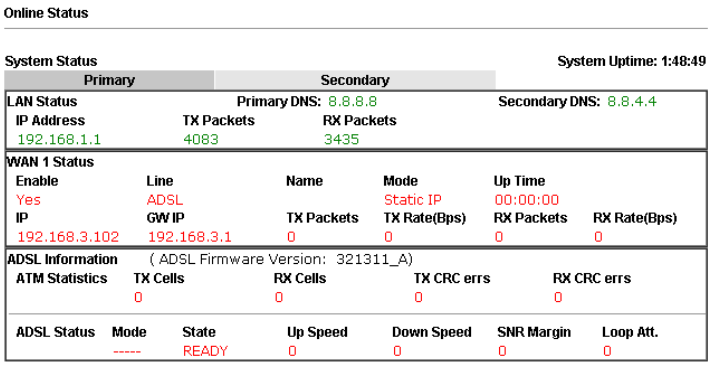
This page provides you the general settings for LAN.

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



Available settings are explained as follows:

Item	Description
Network Configuration	**For NAT Usage,** **IP Address** - Type in private IP address for connecting to a local private network (Default: 192.168.1.1). **Subnet Mask -** Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
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 dispatches 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. **Start IP Address -** Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254. **IP Pool Counts -** Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253. **Gateway IP Address -** Enter a value of the gateway IP address for the DHCP server. The value is usually as same as

	the 1st IP address of the modem, which means the modem is the default gateway.
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:  Online Status System Status — System Uptime: 1:48:49 Primary / Secondary LAN Status — Primary DNS: 8.8.8.8 — Secondary DNS: 8.8.4.4 IP Address: 192.168.1.1 — TX Packets: 4083 — RX Packets: 3435 WAN 1 Status Enable: Yes — Line: ADSL — Name: — Mode: Static IP — Up Time: 00:00:00 IP: 192.168.3.102 — GW IP: 192.168.3.1 — TX Packets: 0 — TX Rate(Bps): 0 — RX Packets: 0 — RX Rate(Bps): 0 ADSL Information (ADSL Firmware Version: 321311_A) ATM Statistics — TX Cells: 0 — RX Cells: 0 — TX CRC errs: 0 — RX CRC errs: 0 ADSL Status — Mode: ----- — State: READY — Up Speed: 0 — Down Speed: 0 — SNR Margin: 0 — Loop Att.: 0 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.

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

II-3 NAT

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

When the outgoing packets destined to some public server on the Internet reach the NAT router, the 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:

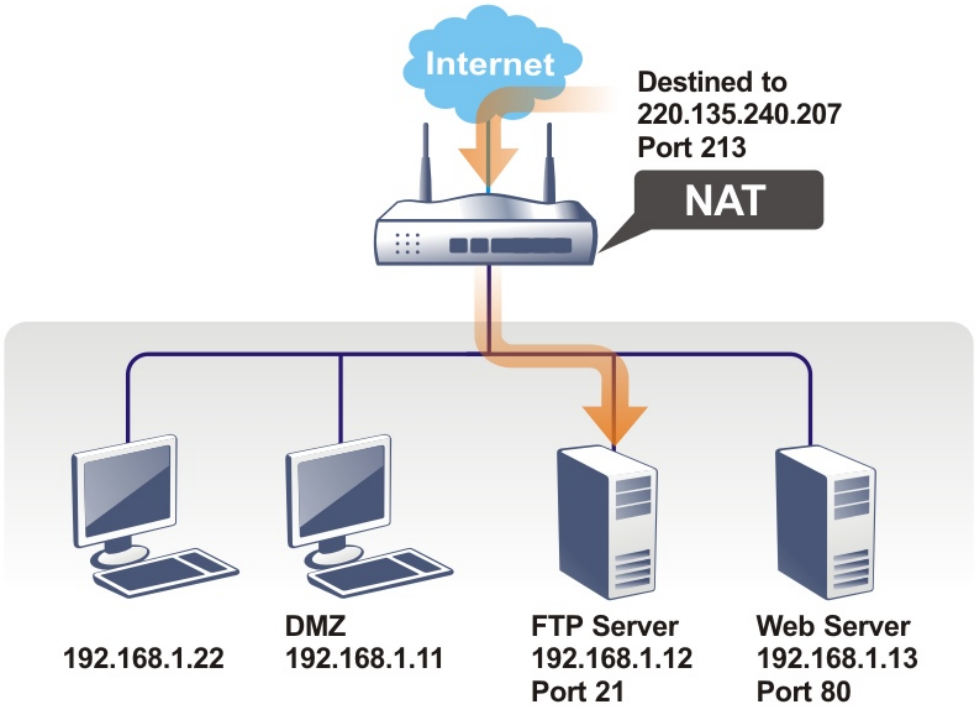
- **Save cost on applying public IP address and apply efficient usage of IP address.** NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- **Enhance security of the internal network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

Info

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.

II-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 40 port-mapping entries for the internal hosts.

NAT >> Port Redirection

Port Redirection | Set to Factory Default |

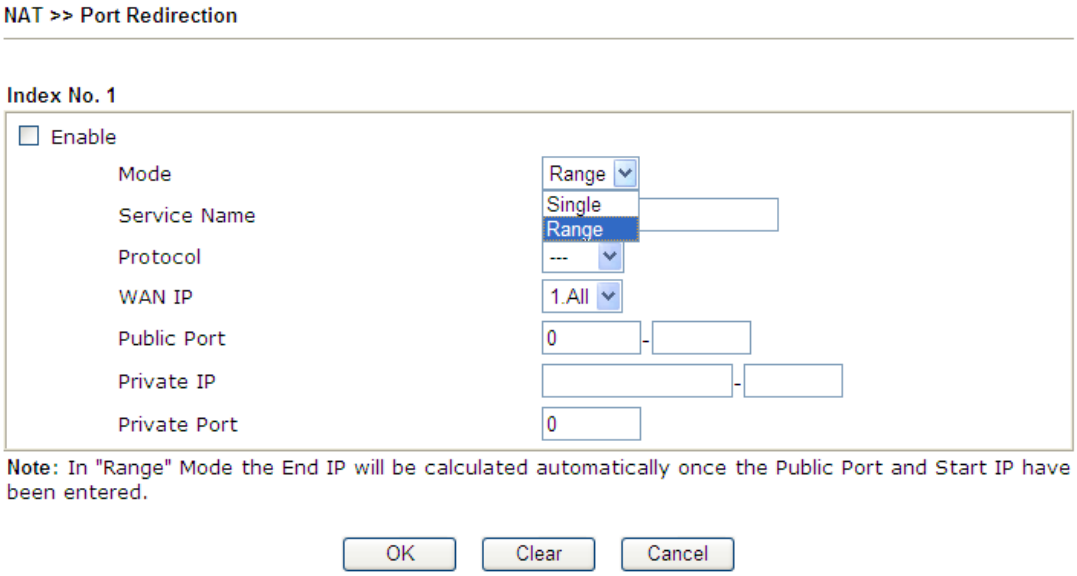
Index	Service Name	Public Port	Private IP	Status
1.				x
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x

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

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.
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:

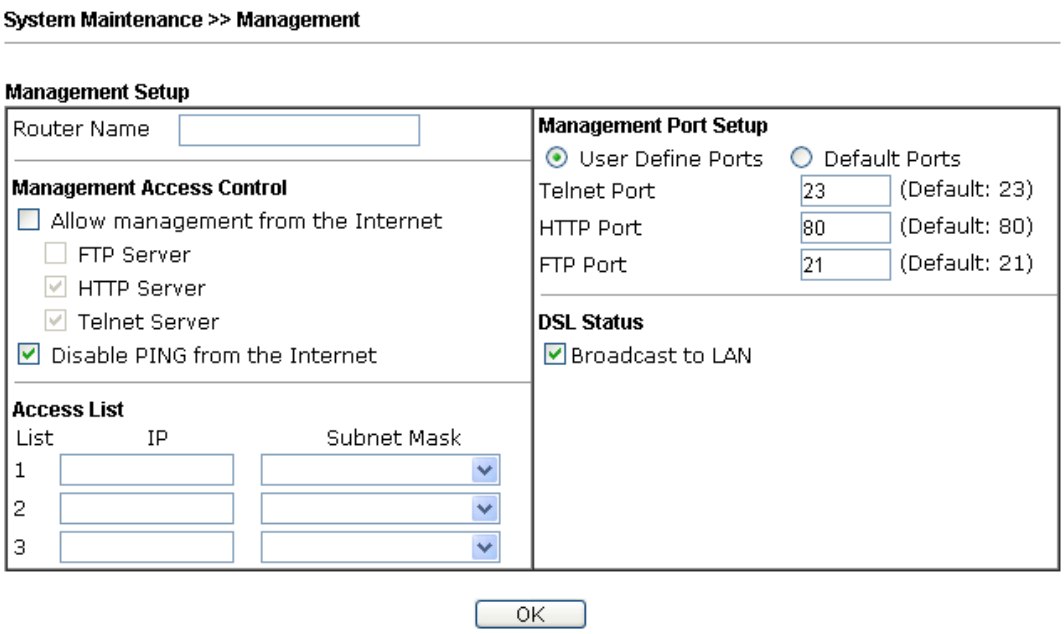
Item	Description
Enable	Check this box to enable such port redirection setting.
Mode	Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select **Range**. In Range mode, if the public port (start port and end port) and the starting IP of private 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. Type the required number on the first box (as the starting port) and the second box (as the ending port).

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). The second one will be assigned automatically later.
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.

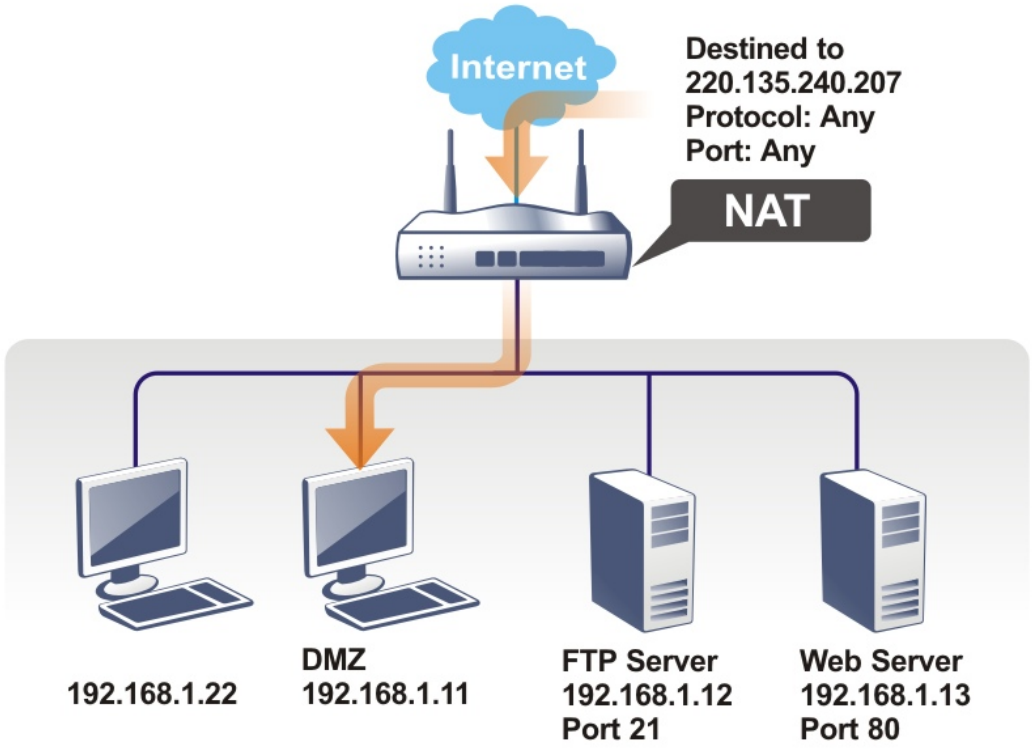
Note that the modem has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the modem in order to avoid confliction.

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.



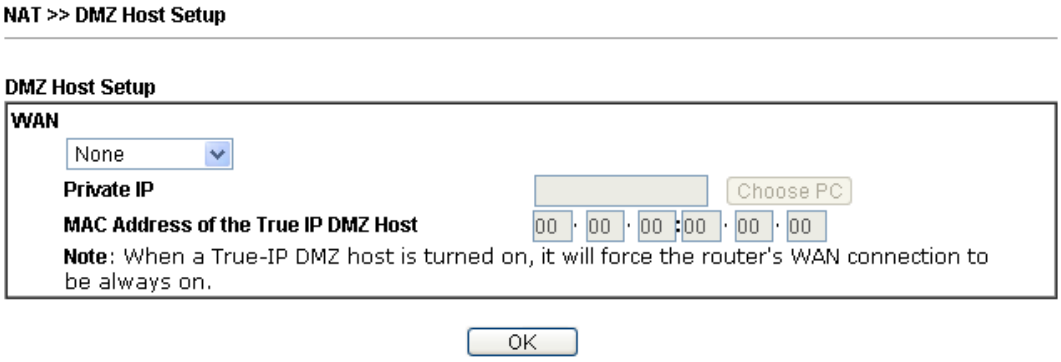
II-3-2 DMZ Host

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

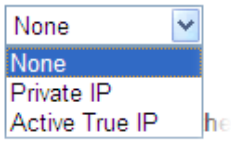
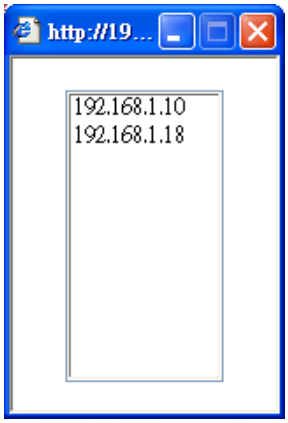


The security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

Click **DMZ Host** to open the following page. You can set different DMZ host for each WAN interface. Click the WAN tab to switch into the configuration page for that WAN.



Available settings are explained as follows:

Item	Description
WAN 1 	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 screen. Click **OK** to save the setting.

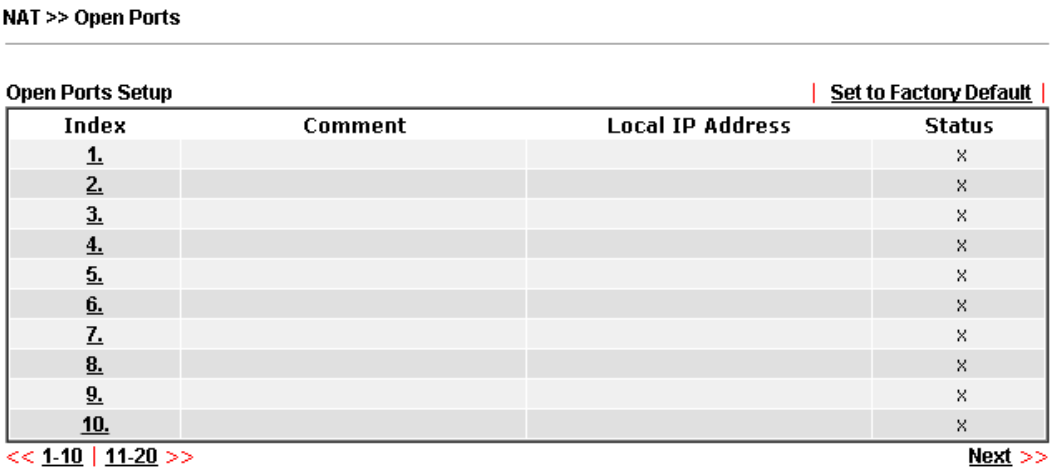
After finishing all the settings here, please click **OK** to save the configuration.

II-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.

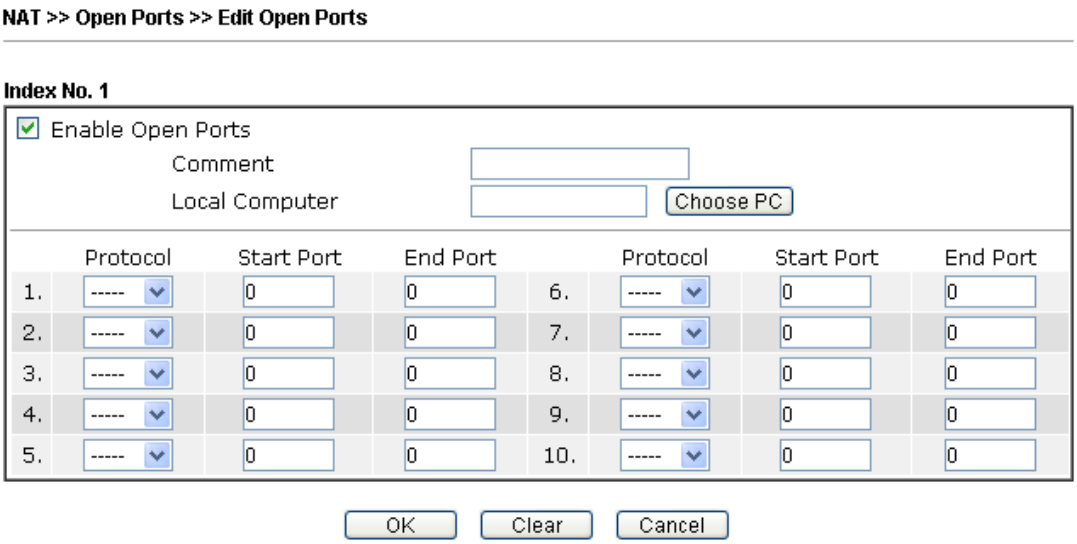
Click **Open Ports** to open the following page:



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.
Aux. WAN IP	Display the IP alias setting used by such index. If no IP alias setting exists, such field will not appear.
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.

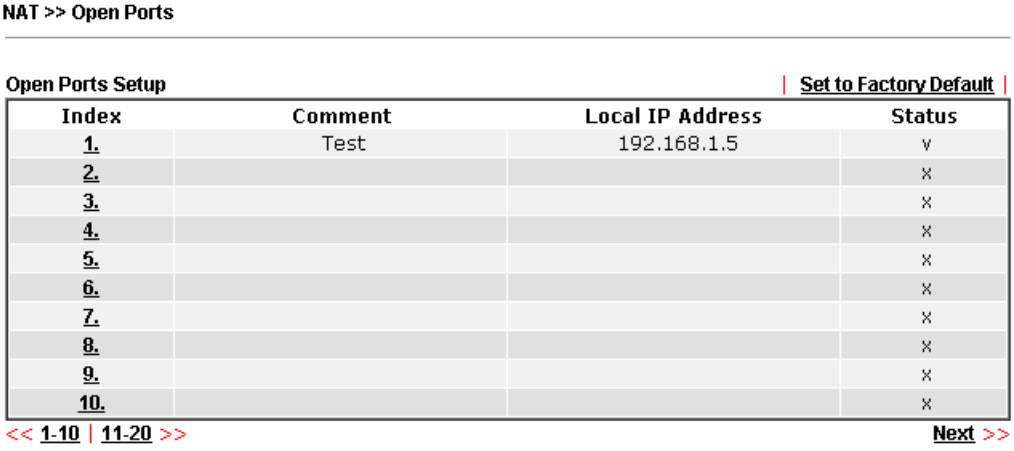
To add or edit port settings, click one index number on the page. The index entry setup page will pop up. In each index entry, you can specify **10** port ranges for diverse services.



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.
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.



II-4 Applications

Dynamic DNS

The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the 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 routers are compatible with the DDNS services supplied by most popular DDNS service providers such as **www.dyndns.org, www.no-ip.com, www.dtdns.com, www.changeip.com, www.dynamic- nameserver.com.** You should visit their websites to register your own domain name for the modem.

Schedule

The Vigor router has a built-in 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.

UPnP

The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on the modem is “NAT Traversal”. This enables applications inside the firewall to automatically open the ports that they need to pass through a router.

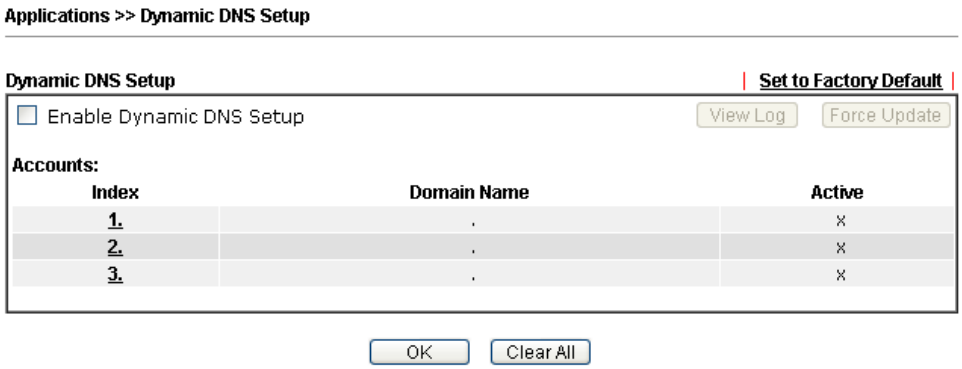
IGMP

IGMP is the abbreviation of Internet Group Management Protocol. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups. For invoking IGMP Snooping function, you have to check the Enable IGMP Proxy box first for activating the IGMP proxy function.

II-4-1 Dynamic DNS

Enable the Function and Add a Dynamic DNS Account

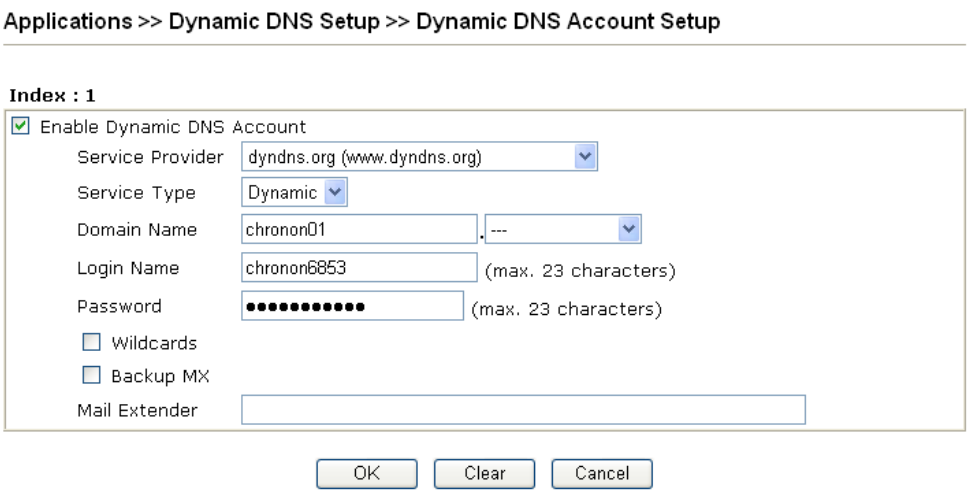
1. Assume you have a registered domain name from the DDNS provider, say *hostname.dyndns.org*, and an account with username: *test* and password: *test*.
2. In the DDNS setup menu, check **Enable Dynamic DNS Setup**.



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.
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.

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

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.

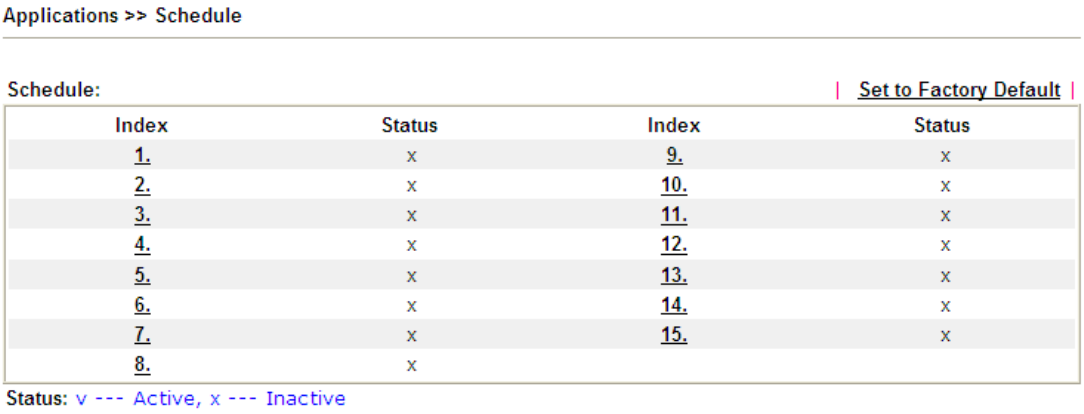
Delete a Dynamic DNS Account

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

II-4-2 Schedule

The Vigor router has a built-in 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 router'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.



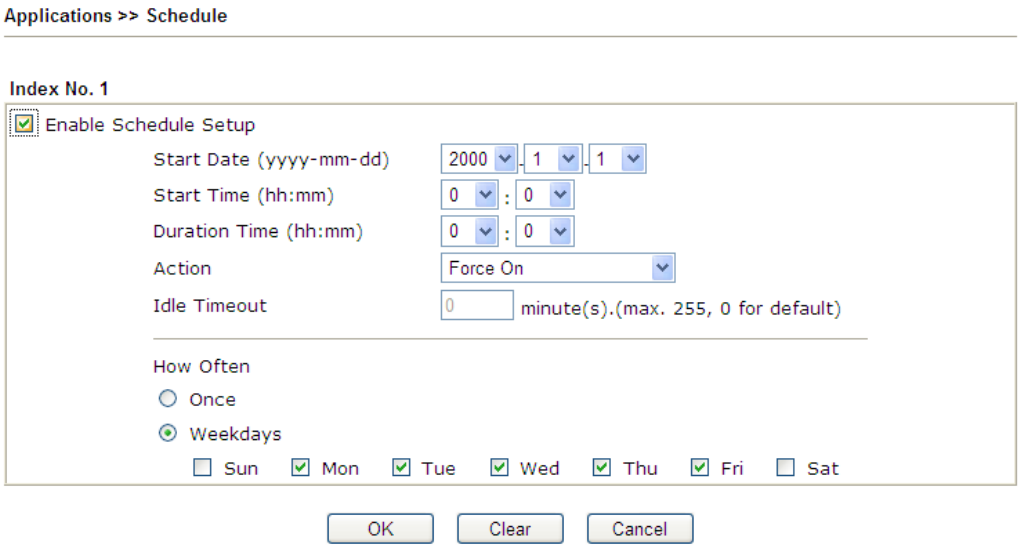
Available settings are explained as follows:

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**.

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)

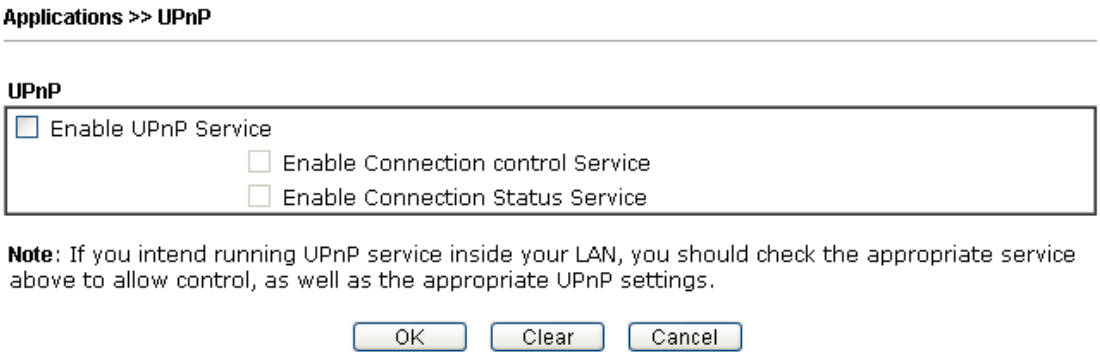
Mon - Sun **9:00 am** **to** **6:00 pm**

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.

II-4-3 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 routers, 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 router.

Info UPnP is required for some applications such as PPS, Skype, eMule...and etc. If you are not familiar with UPnP, it is suggested to turn off this function for security.



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 reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

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

Security Considerations

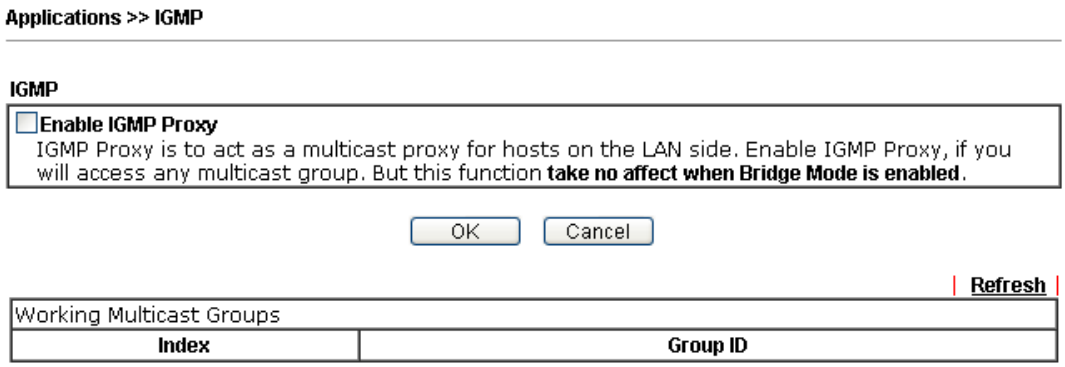
Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

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

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

II-4-4 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.
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.

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

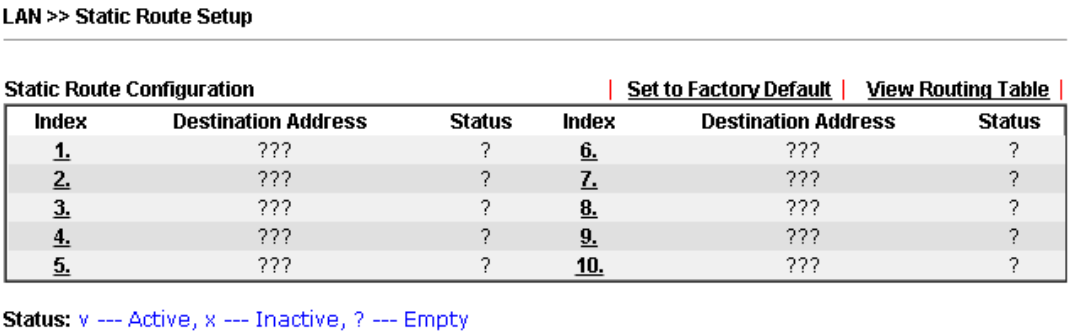
II-5 Routing

Specify routing policy to determine the direction of the data transmission.

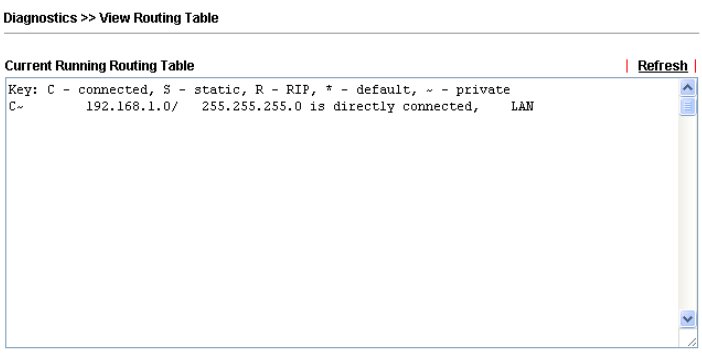
Web User Interface

II-5-1 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.



Available settings are explained as follows:

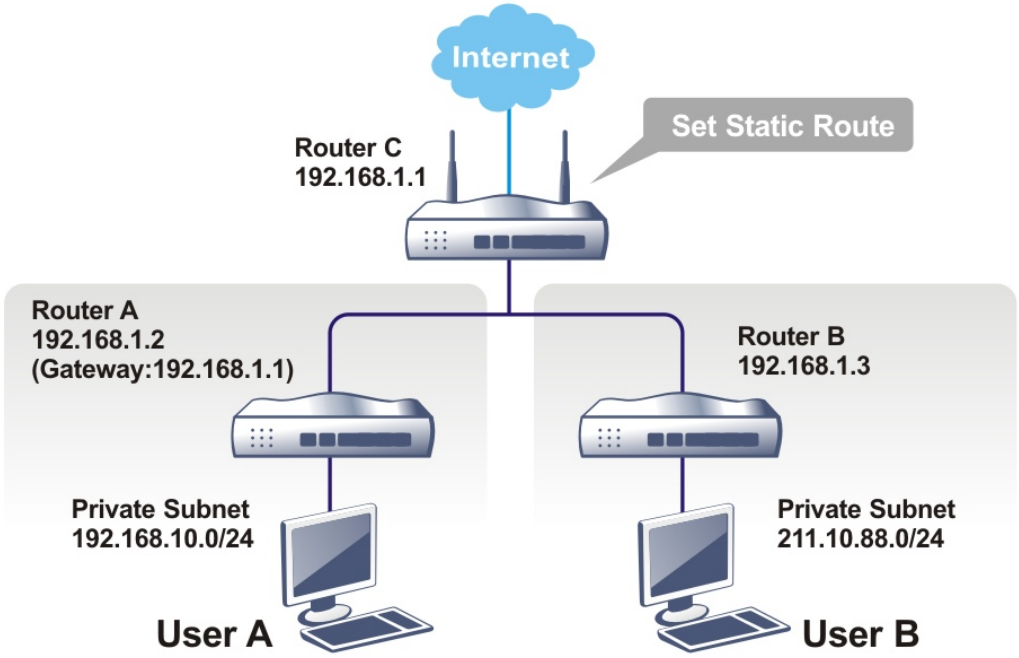
Item	Description
Index	The number (1 to 30) under Index allows you to open next page to set up static route.
Destination Address	Displays the destination address of the static route.
Status	Displays the status of the static route.
Set to Factory Default	Clear all of the settings and return to factory default settings.
Viewing Routing Table	Displays the routing table for your reference. 

Add Static Routes to Private and Public Networks

Here is an example (based on IPv4) of setting Static Route in Main Router 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 Router to surf the Internet.
- create a private subnet 192.168.10.0 using an internal Router A (192.168.1.2)
- create a public subnet 211.100.88.0 via an internal Router B (192.168.1.3).
- have set Main Router 192.168.1.1 as the default gateway for the modem A 192.168.1.2.

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

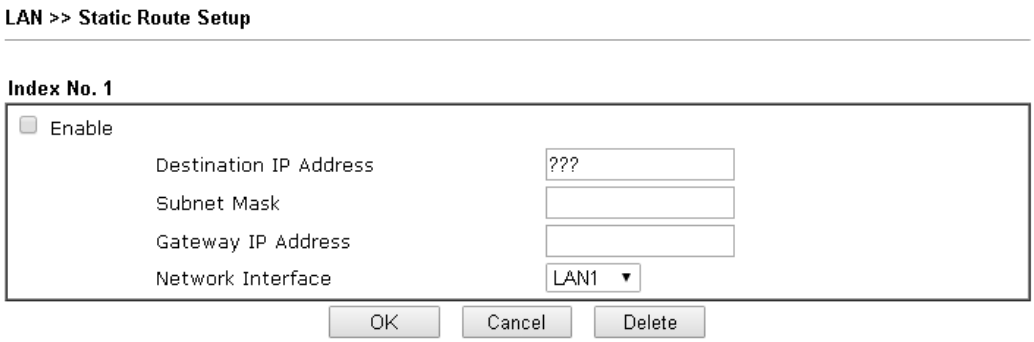


1. Go to **LAN** page and click **General Setup**, select 1st Subnet as the **RIP Protocol Control.** Then click the **OK** button.

Info

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

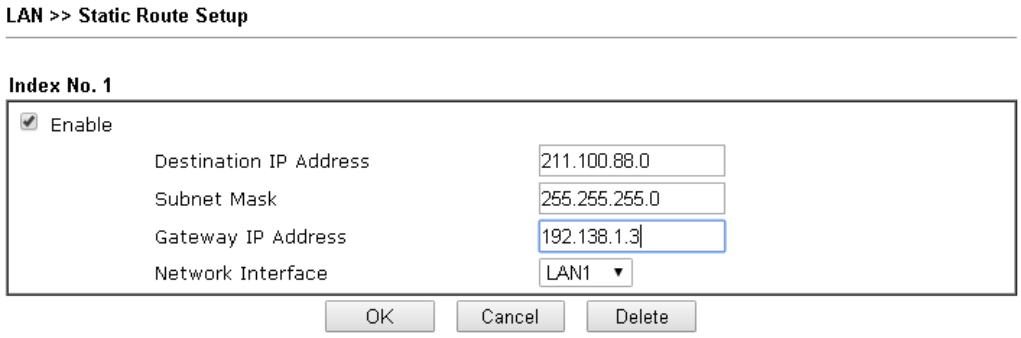
2. Click the **LAN >> Static Route** and click on the **Index Number 1.** Check the **Enable** box. Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click **OK**.



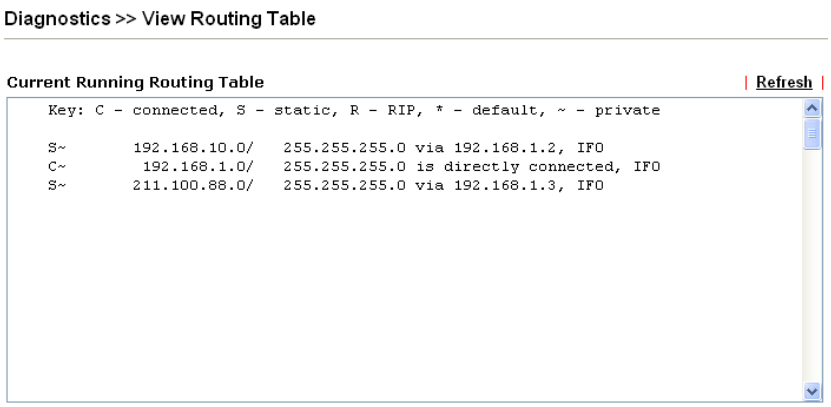
Available settings are explained as follows:

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. Click **OK**.



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



Part III Security

Firewall

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of the Vigor router helps to protect your local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet.

III-1 Firewall

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

Firewall Facilities

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

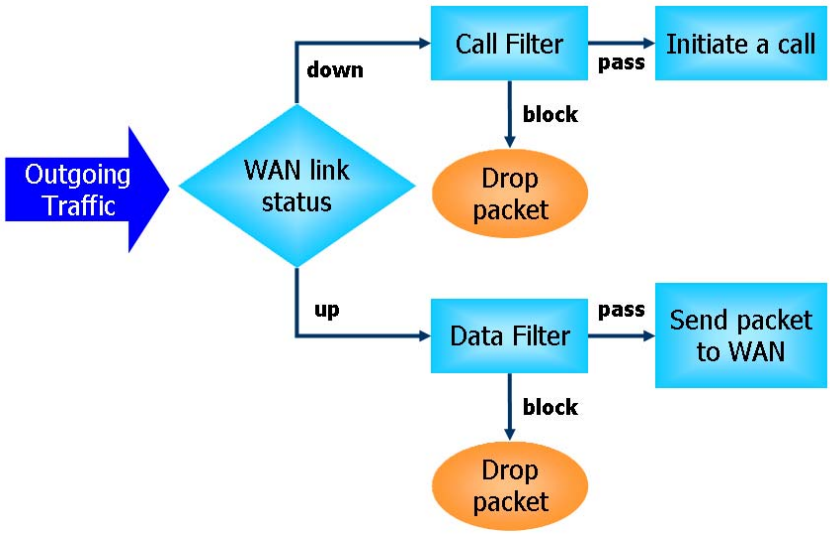
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

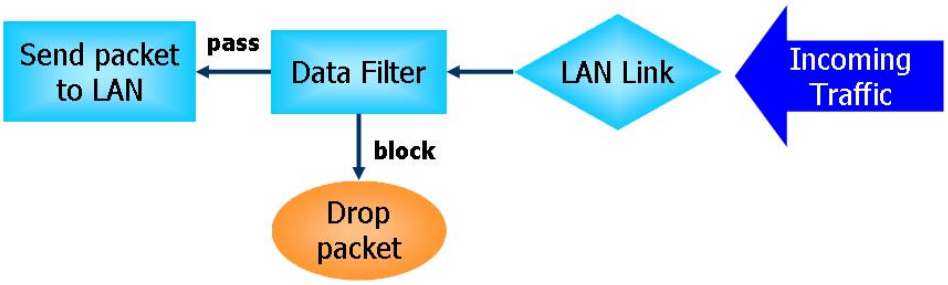
IP Filters

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 router will treat incoming traffic and outgoing traffic respectively.





Stateful Packet Inspection (SPI)

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

Denial of Service (DoS) Defense

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

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

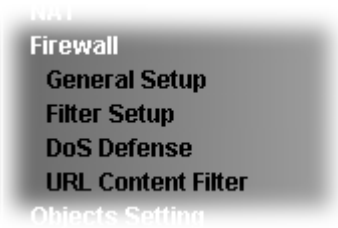
Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

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

1. SYN flood attack
2. UDP flood attack
3. ICMP flood attack
4. 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. Unassigned Numbers

Web User Interface

Below shows the menu items for Firewall.



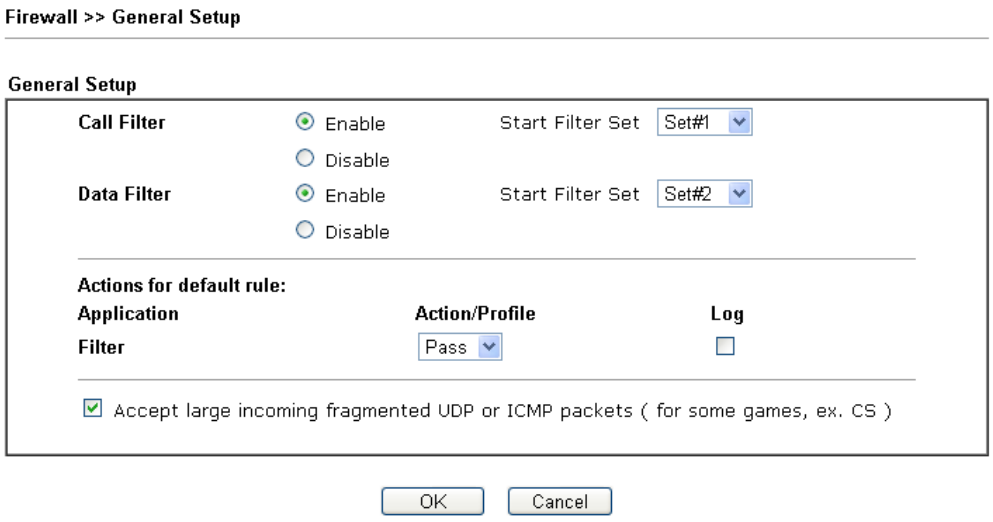
III-1-1 General Setup

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 **Accept large incoming fragmented UDP packets**.

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

General Setup Page

Such page allows you to enable / disable Call Filter and Data Filter, determine general rule for filtering the incoming and outgoing data.



Available settings are explained as follows:

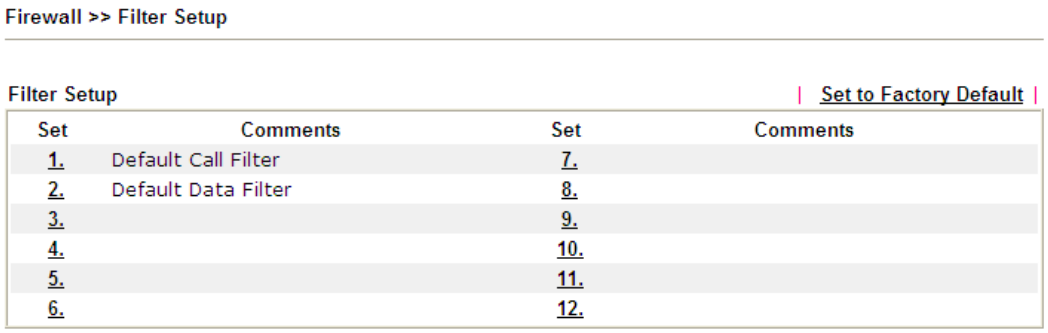
Item	Description
Call Filter	Check **Enable** to activate the Call Filter function. Assign a start filter set for the Call Filter.
Data Filter	Check **Enable** to activate the Data Filter function. Assign a start filter set for the Data Filter.
Accept large incoming...	Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable

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

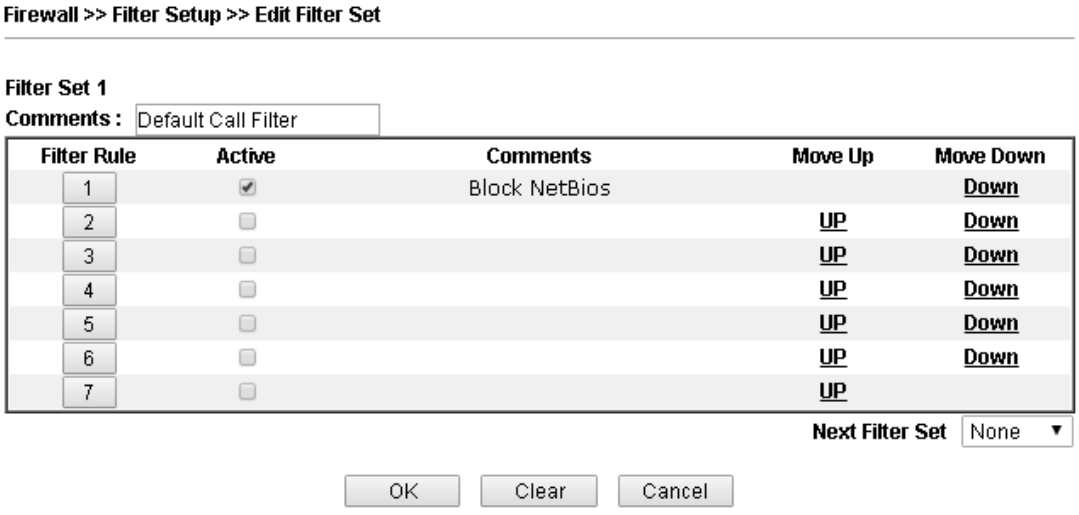
After finished the above settings, click **OK** to save the configuration.

III-1-2 Filter Setup

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



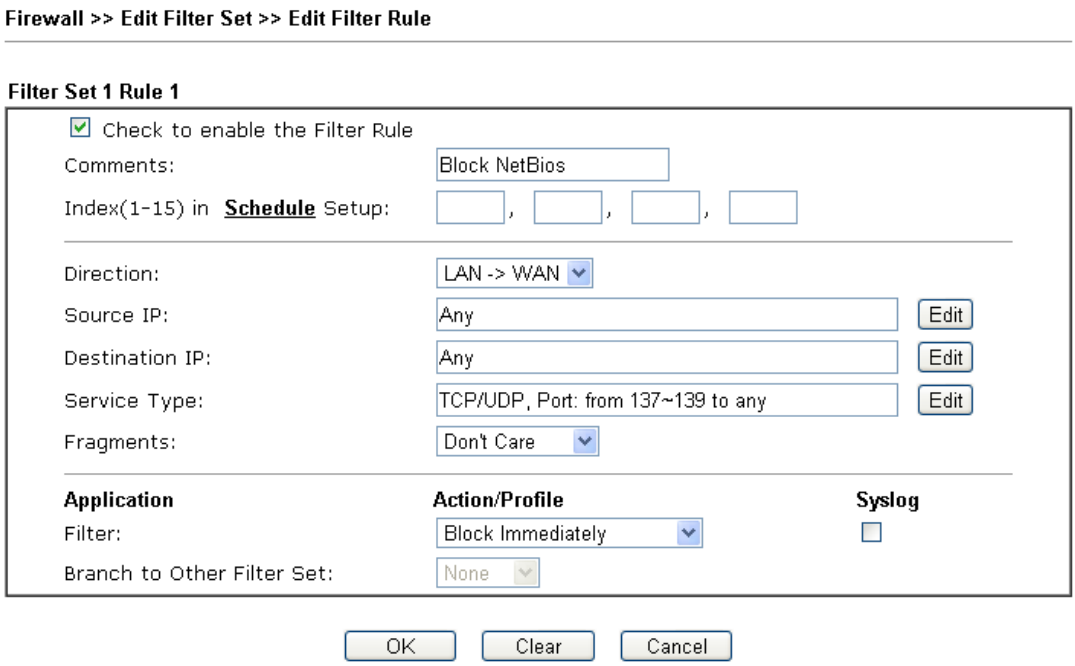
To edit or add a filter, click on the set number to edit the individual set. The following page will be shown. Each filter set contains up to 7 rules. Click on the rule number button to edit each rule. Check **Active** to enable the rule.



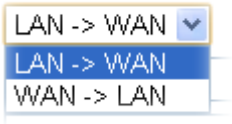
Available settings are explained as follows:

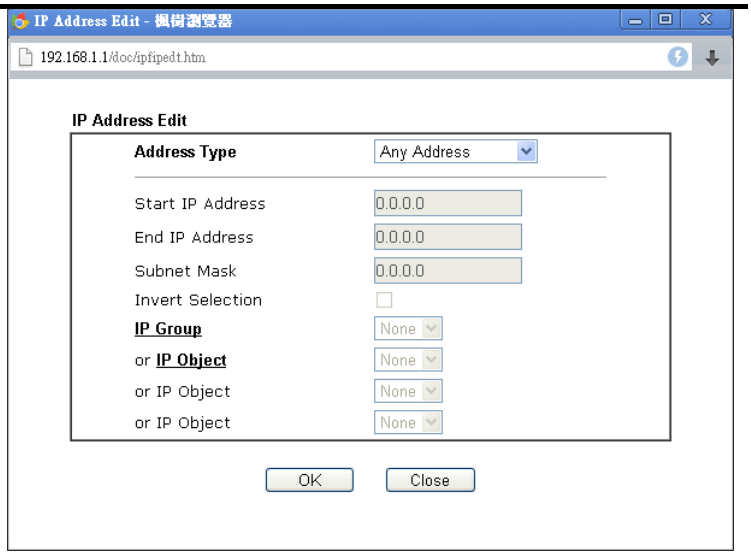
Item	Description
Filter Rule	Click a button numbered (1 ~ 7) to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.
Active	Enable or disable the filter rule.
Comment	Enter filter set comments/description. Maximum length 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.

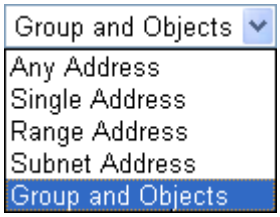


Available settings are explained as follows:

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



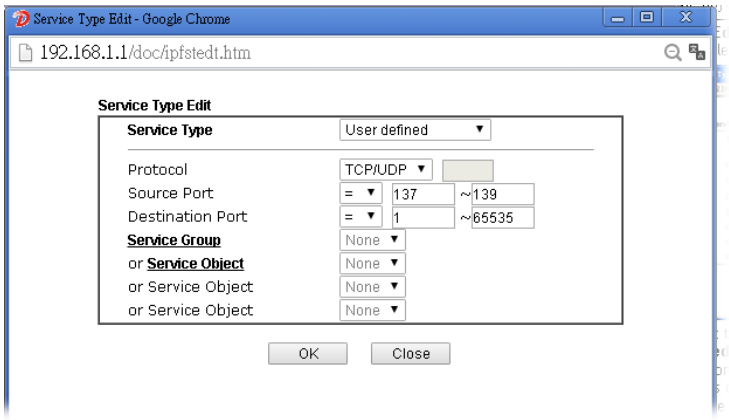
To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.



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.

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

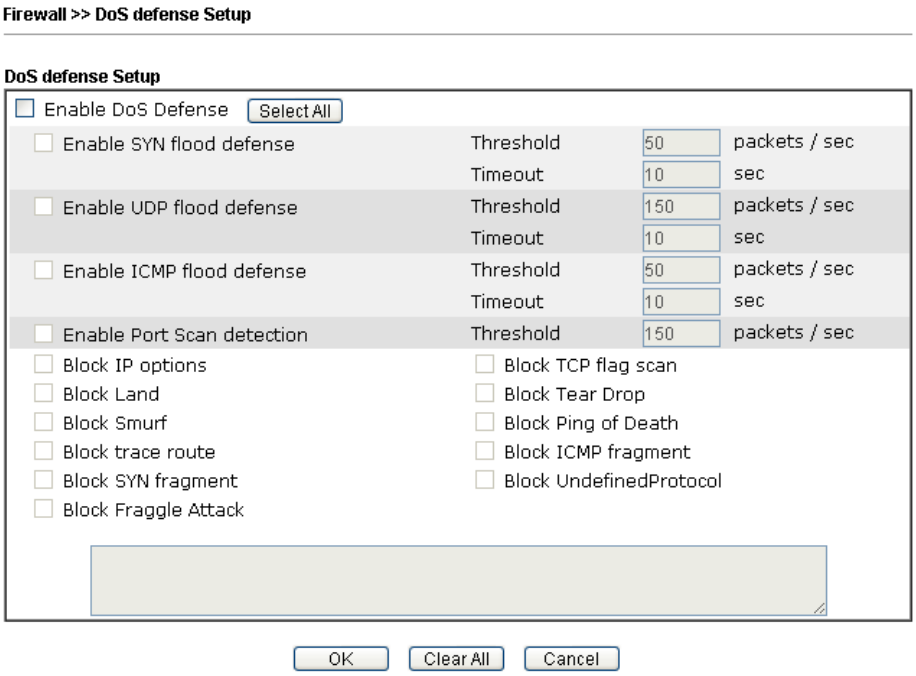
Example

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.

III-1-3 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.

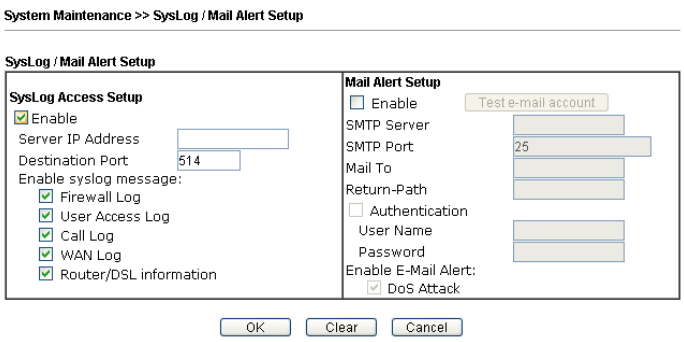
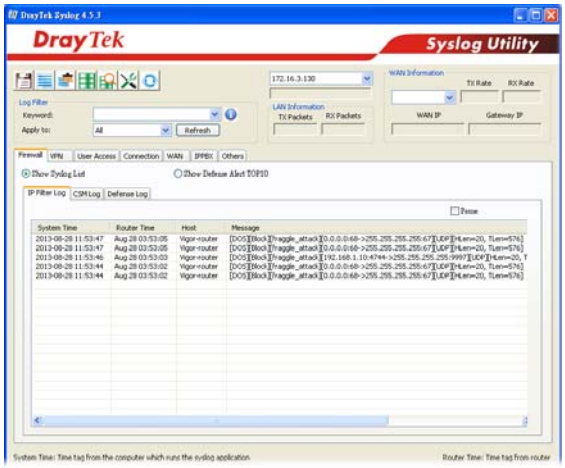
Click **Firewall** and click **DoS Defense** to open the setup page.



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 router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router. By default, the threshold and timeout values are set to 50 packets per second and 10 seconds, respectively. 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 router will start to randomly discard the subsequent UDP packets for a period defined in Timeout. The default setting for threshold and timeout are 150 packets per second and 10 seconds, respectively. 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 router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning. By default, the Vigor router sets the threshold as 150 packets per second. 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 router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages...etc. An eavesdropper outside might learn the details of your private networks.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.
Block trace route	Check the box to enforce the Vigor router not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.
Block Fraggle Attack	Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked. Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.
Block TCP flag scan	Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include *no flag scan*, *FIN without ACK scan*, *SYN FINscan*, *Xmas scan* and *full Xmas scan*.

Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.
Block Undefined Protocol	Check the box to activate the Block Undefined Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.
Warning Messages	We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client. All the warning messages related to **DoS Defense** will be sent to user and user can review it through Syslog daemon. Look for the keyword **DoS** in the message, followed by a name to indicate what kind of attacks is detected.  

This page is left blank.

Part IV Management

There are several items offered for the Vigor router system setup: System Status, TR-069, Administrator Password, Configuration Backup, Syslog /Mail Alert, Time and Date, Management, Reboot System, and Firmware Upgrade.

IV-1 System Maintenance

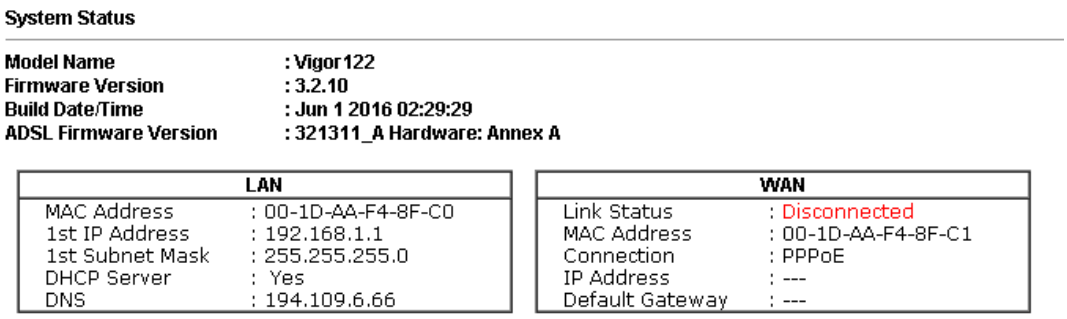
For the system setup, there are several items that you have to know the way of configuration: System Status, TR-069, Administrator Password, User Password, Login Page Greeting, Configuration Backup, Syslog /Mail Alert, Time and Date, Management, Reboot System, Firmware Upgrade, Activation and Internal Service User List.

Below shows the menu items for System Maintenance.

Web User Interface

IV-1-1 System Status

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

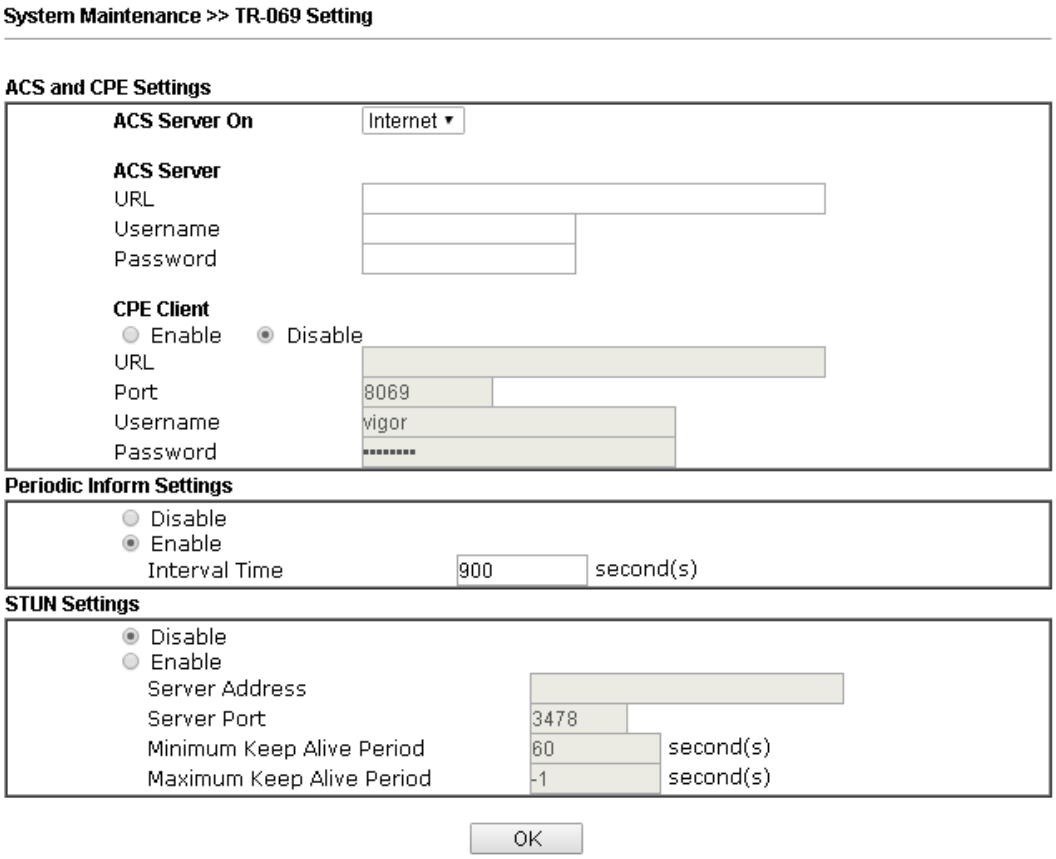


Available settings are explained as follows:

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.
ADSL Firmware Version	ADSL Firmware Version.
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.

IV-1-2 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:

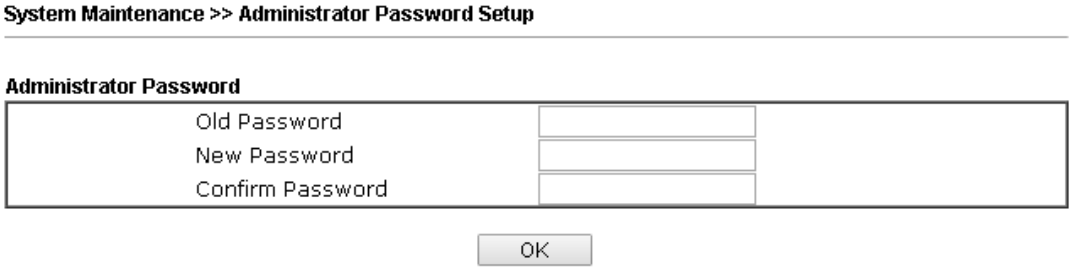
Item	Description
ACS Server On	Choose the interface for the modem connecting to ACS server.
ACS Server	**URL/Username/Password –** Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.
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. **Username** and **Password** – Type the username and password that VigorACS can use to access into such 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.

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

IV-1-3 Administrator Password

This page allows you to set new password.



Available settings are explained as follows:

Item	Description
Administrator Password	**Old Password** - Type in the old password. The factory default setting for password is **"admin"**. **New Password** -Type in new password in this field. The length of the password is limited to 23 characters. **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.

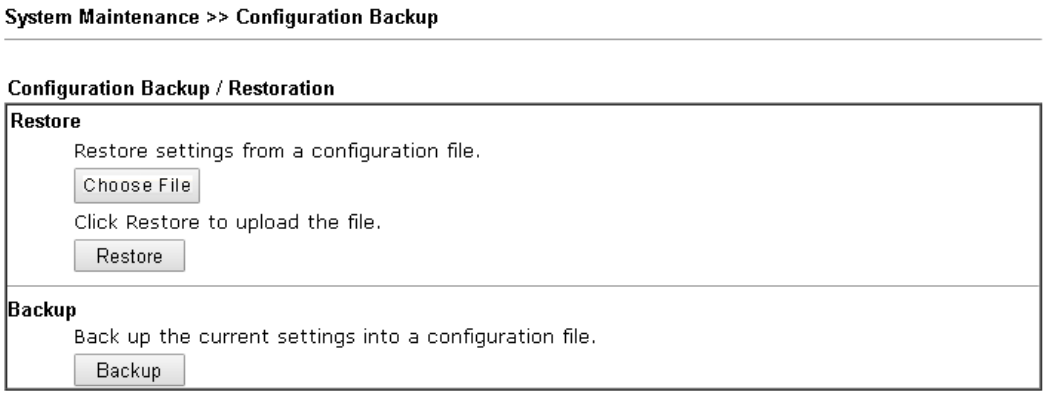
IV-1-4 Configuration Backup

Such function can be used to apply the modem settings configured by Vigor2820/ Vigor2830/ Vigor2850 to Vigor122.

Backup the Configuration

Follow the steps below to backup your configuration.

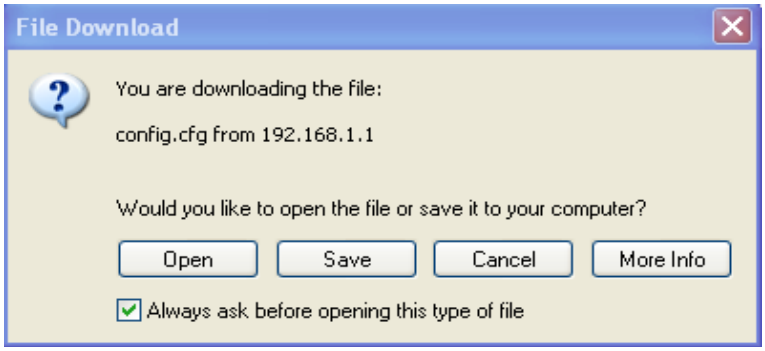
1. Go to **System Maintenance** >> **Configuration Backup**. The following page will be popped-up, as shown below.



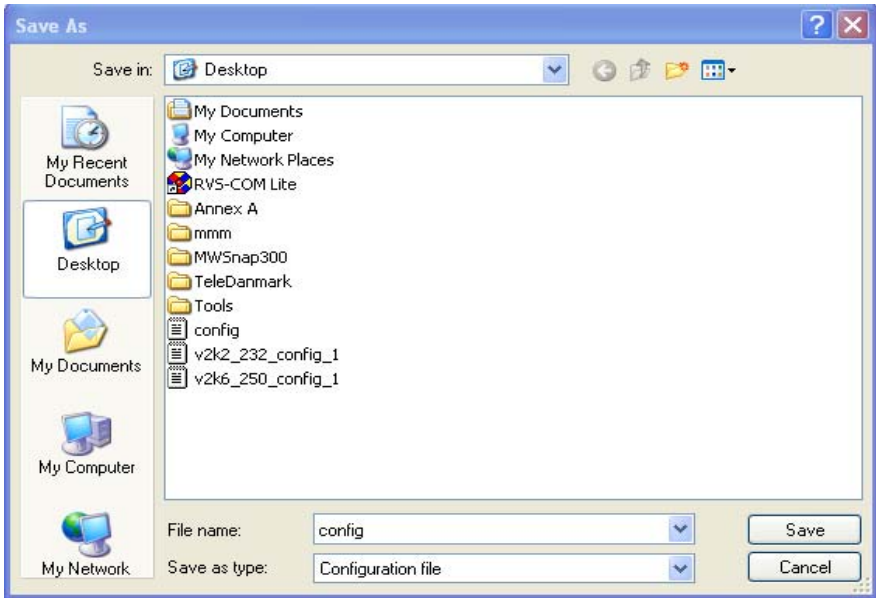
Available settings are explained as follows:

Item	Description
Restore	**Choose File** – Click it to specify a file to be restored. Click **Restore** to restore the configuration.
Backup	Click it to perform the configuration backup of this router.

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.



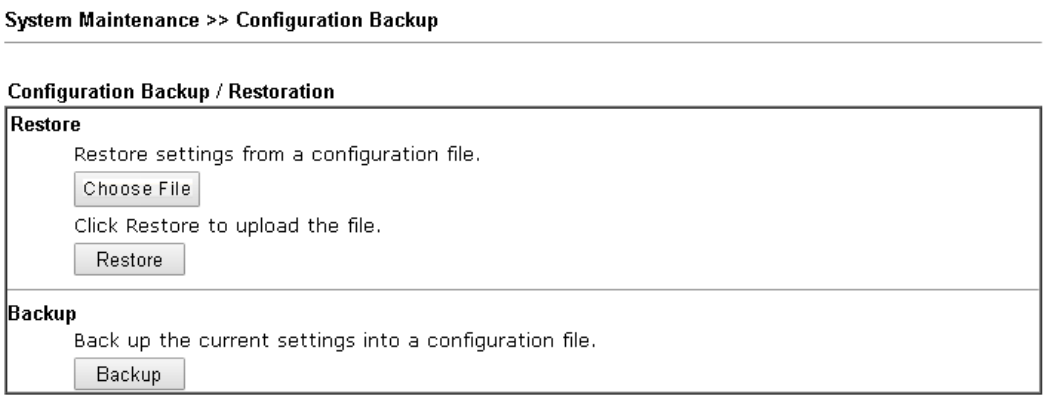
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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.

Info	Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

Restore Configuration

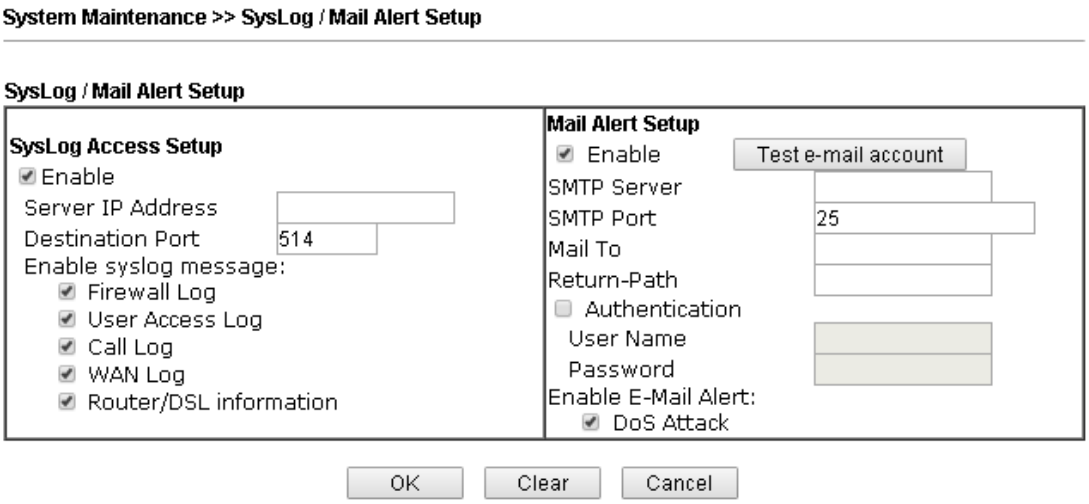
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.



2. Click **Choose File** 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.

IV-1-5 Syslog/Mail Alert

SysLog function is provided for users to monitor router.



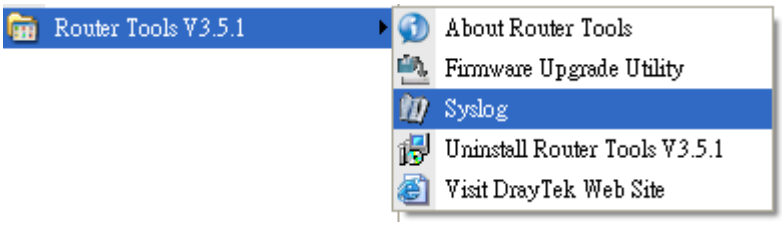
Available settings are explained as follows:

Item	Description
SysLog Access Setup	**Enable** - Check **Enable** to activate function of syslog. **Server IP Address -**The IP address of the Syslog server. **Destination Port -** Assign a port for the Syslog protocol. **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. **Test e-mail account -** 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/SMTP Port -** The IP address/Port number 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 detecting the item(s) you specify here.

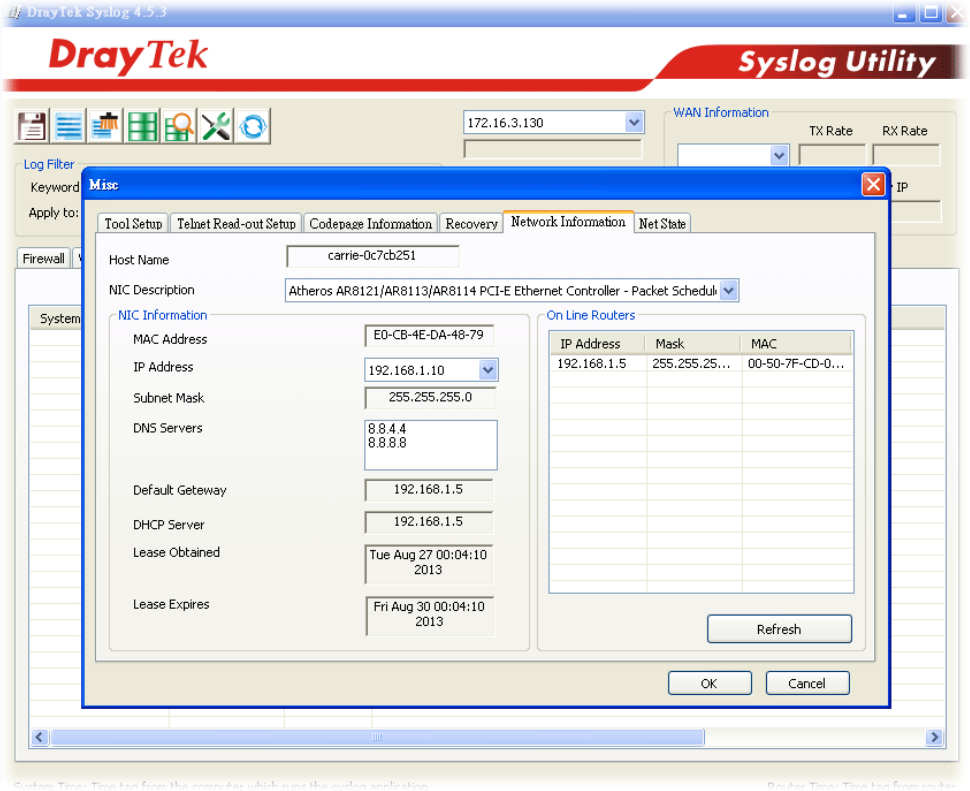
Click **OK** to save these settings.

For viewing the Syslog, please do the following:

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

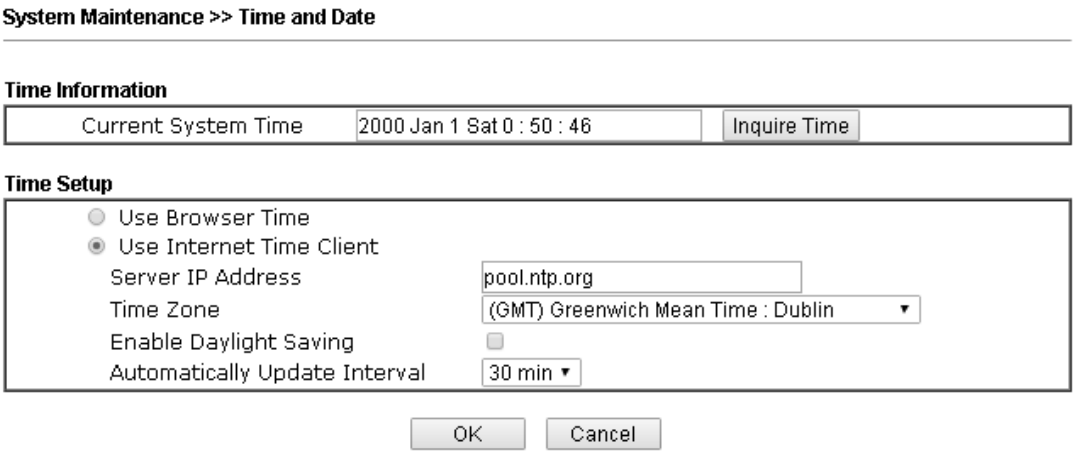


3. From the Syslog screen, select the modem you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the modem. Otherwise, you won't succeed in retrieving information from the modem.



IV-1-6 Time and Date

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



Available settings are explained as follows:

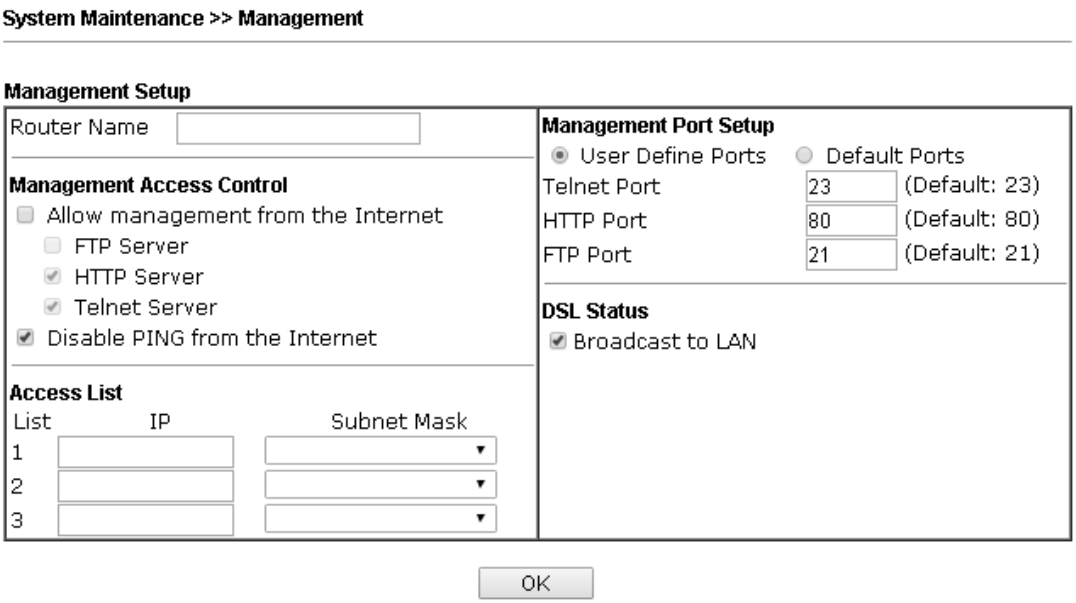
Item	Description
Current System Time	Click **Inquire Time** to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Server IP Address	Type the web site 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.

IV-1-7 Management

This page allows you to manage the settings for Internet/LAN Access Control, Access List from Internet, Management Port Setup, TLS/SSL Encryption Setup, CVM Access Control and Device Management.

The management pages for IPv4 and IPv6 protocols are different.



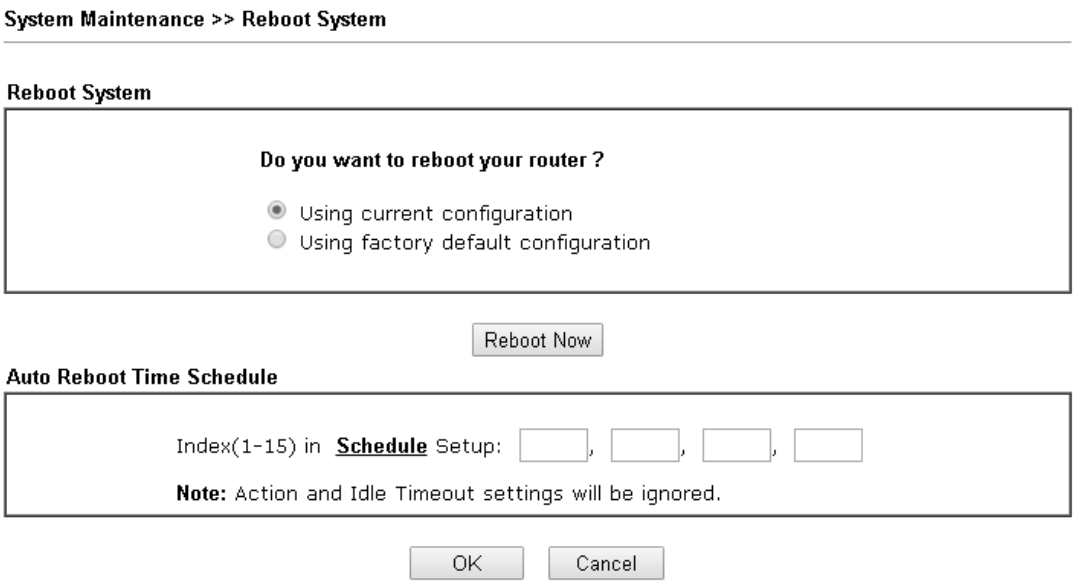
Available settings are explained as follows:

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.
Management Port Setup	**User Define Ports -** Check to specify user-defined port numbers for the Telnet, HTTP, HTTPS, and FTP ervers. **Default Ports -** Check to use standard port numbers for the Telnet and HTTP servers.
DSL Status	**Broadcast to LAN –** Check this box to send DSL status of Vigor122 to the device in LAN. If LAN device connecting to Vigor router/modem (e.g., Vigor2860, Vigor2925) supporting to display DSL information, such information can be viewed from the web page of that Vigor router/modem.

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

IV-1-8 Reboot System

The Web user interface may be used to restart your router. 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.

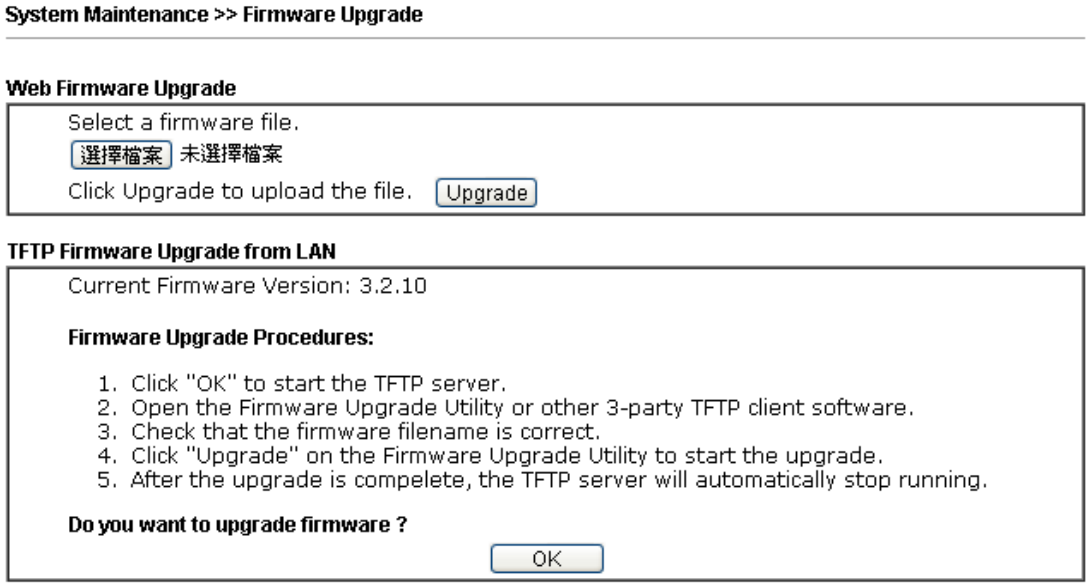
If you want to reboot the modem using the current configuration, check **Using current configuration** and click **Reboot Now**. To reset the modem settings to default values, check **Using factory default configuration** and click **Reboot Now**. The modem will take 5 seconds to reboot the system.

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

IV-1-9 Firmware Upgrade

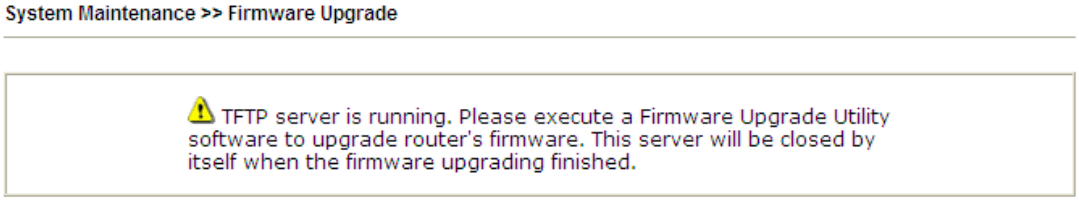
Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.DrayTek.com (or local DrayTek's web site) and FTP site is ftp.DrayTek.com.

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



Choose the right firmware by clicking **Select**. Then, click **Upgrade**. The system will upgrade the firmware of the modem automatically.

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



For the detailed information about firmware update, please go to Chapter 5.

This page is left blank.

Part V Others

Objects Settings

Define objects such as IP address, service type, and others. These pre-defined objects can be applied in Firewall.

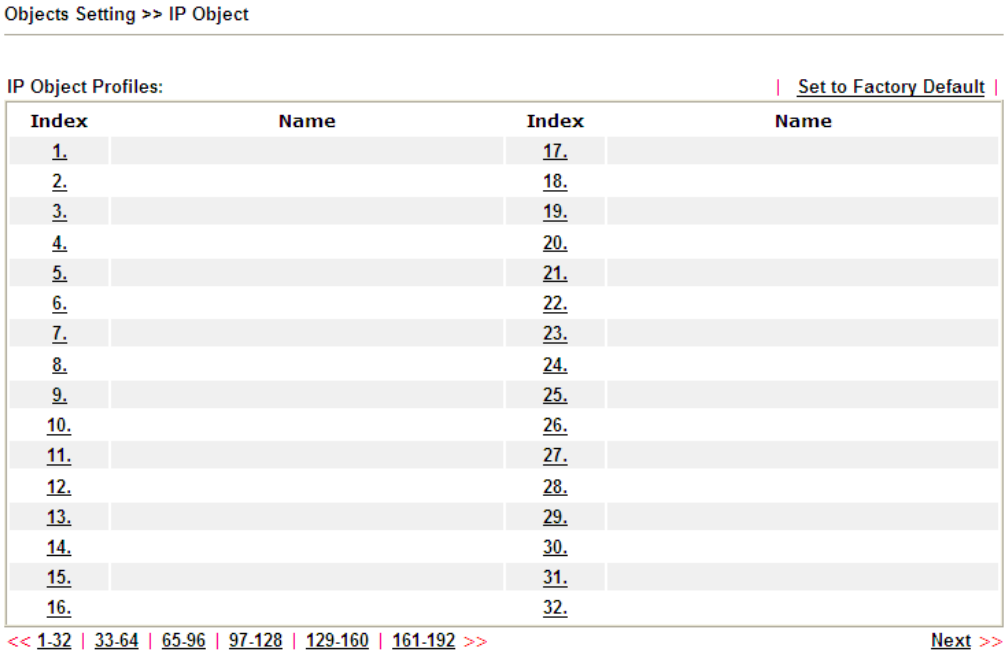
V-1 Objects Settings

For IPs in a range and service ports in a limited range usually will be applied in configuring router'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).

Web User Interface

V-1-1 IP Object

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

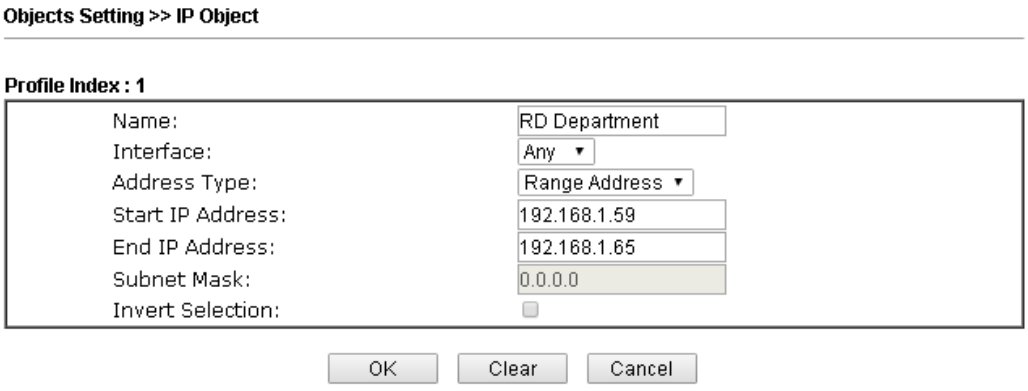


Available settings are explained as follows:

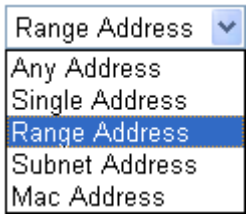
Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

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

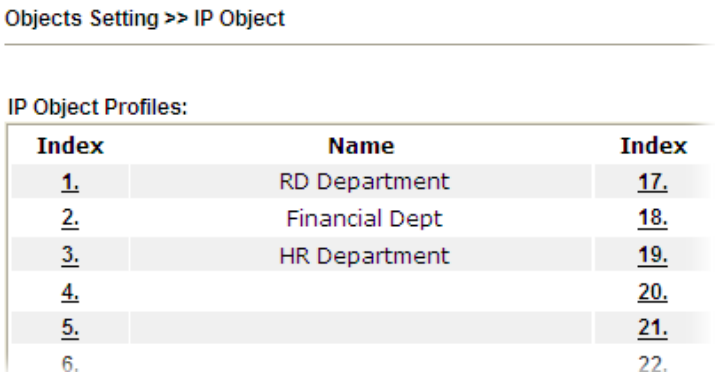
1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



Available settings are explained as follows:

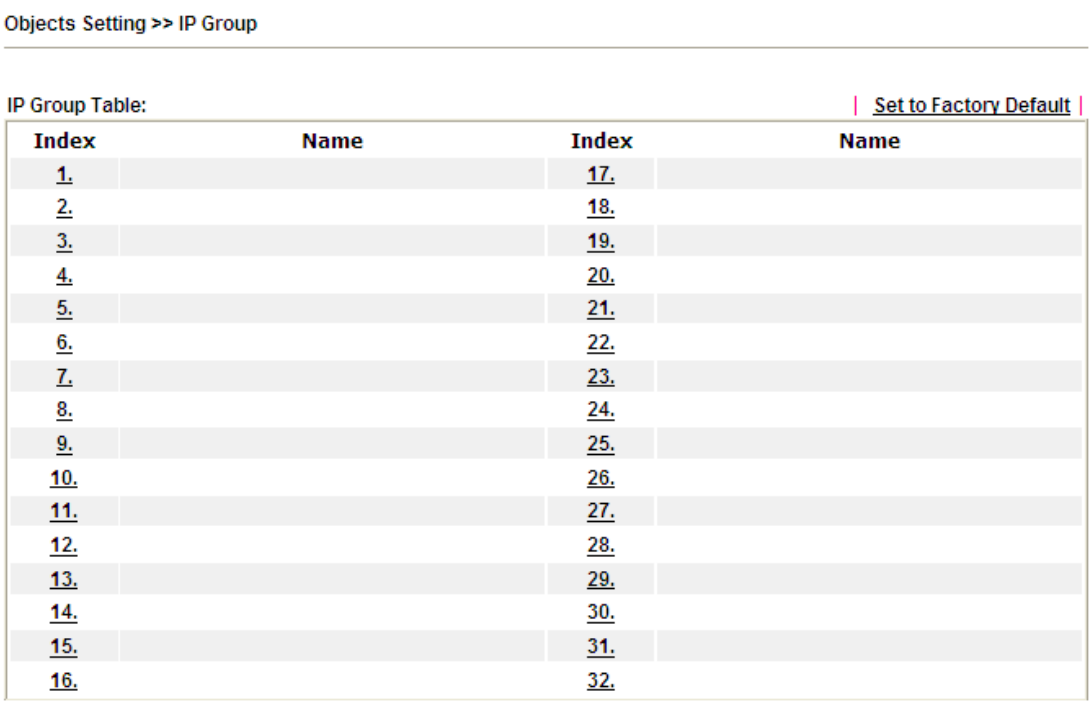
Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose a proper interface. For example, the **Direction** setting in **Edit Filter Rule** will ask you specify IP or IP range for WAN or LAN or any IP address. If you choose LAN/WAN/Any as the **Interface** here, and choose AN/WAN/Any as the direction setting in **Edit Filter Rule**, then all the IP addresses specified with AN/WAN/Any 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. 
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.



V-1-2 IP Group

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

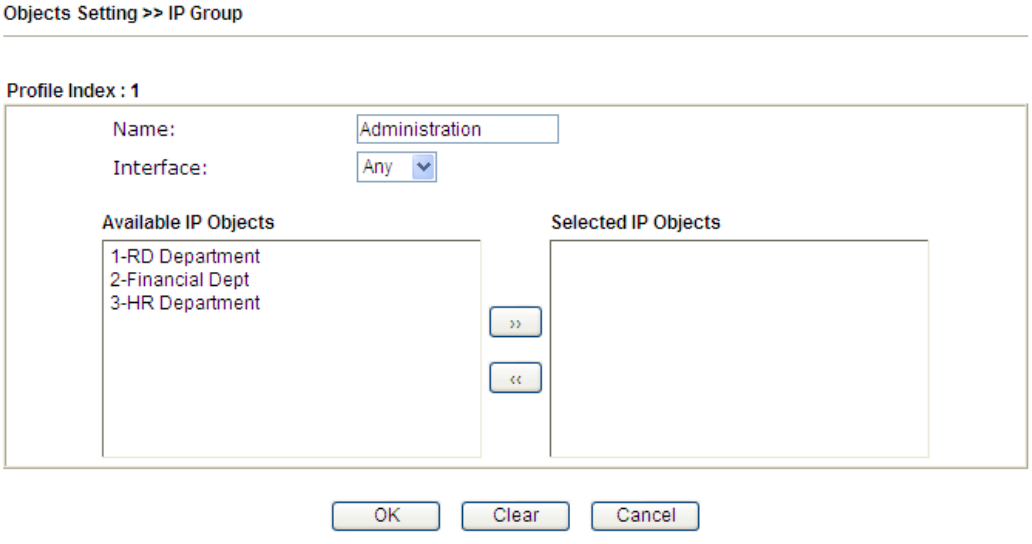


Available settings are explained as follows:

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:



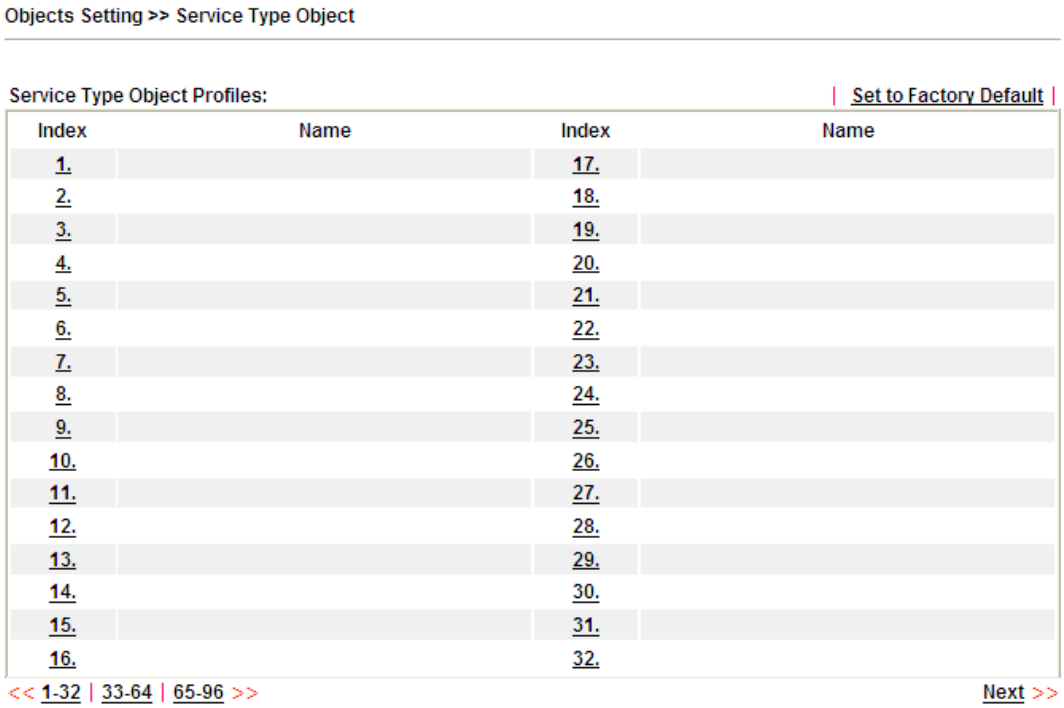
Available settings are explained as follows:

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.

V-1-3 Service Type Object

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

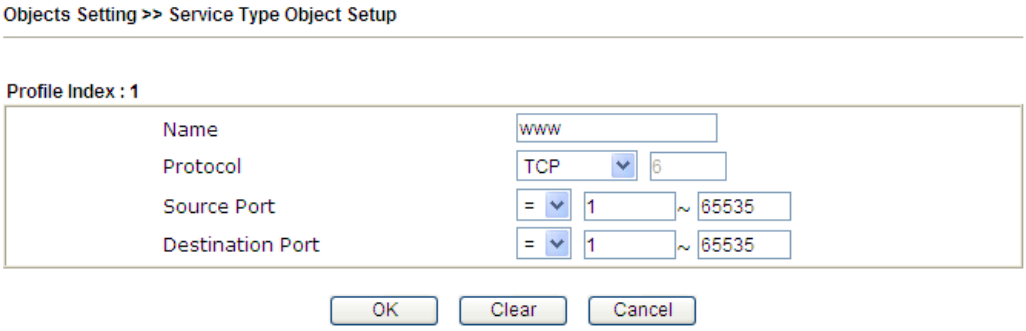


Available settings are explained as follows:

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:

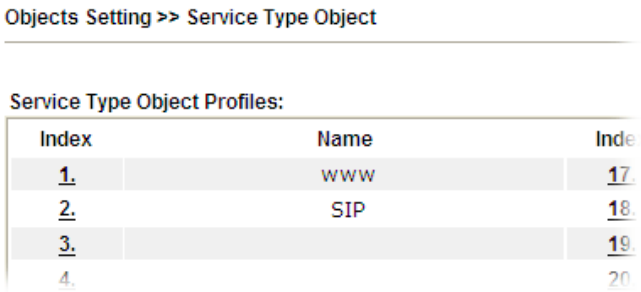
1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



Available settings are explained as follows:

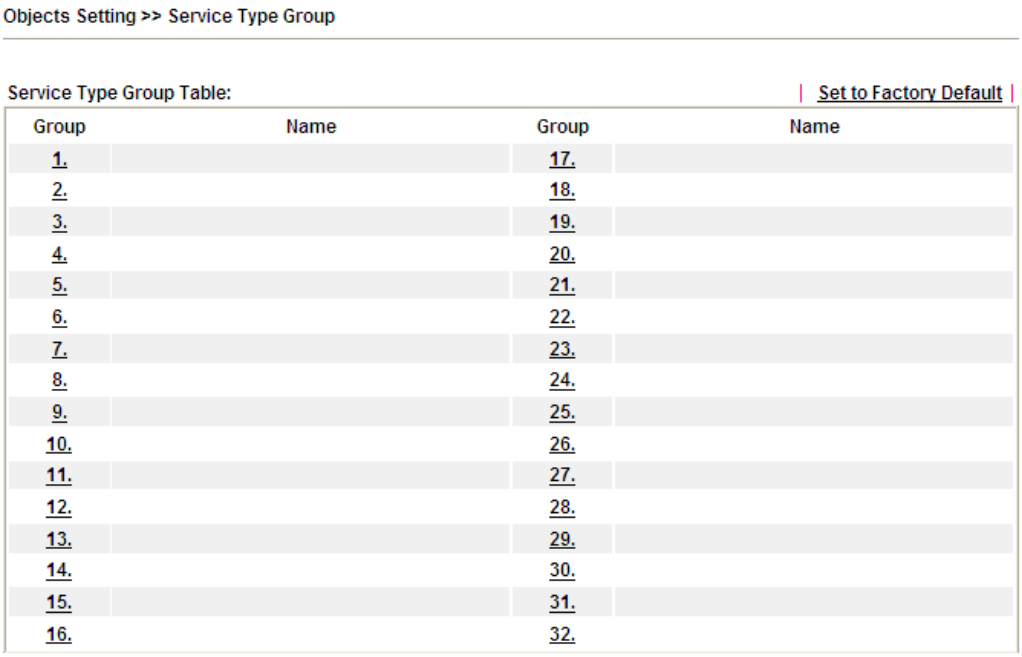
Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Protocol	Specify the protocol(s) which this profile will apply to. TCP 6 Any ICMP IGMP TCP UDP TCP/UDP Other
Source/Destination Port	**Source Port** and the **Destination Port** columns are available for TCP/UDP protocol. 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.



V-1-4 Service Type Group

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

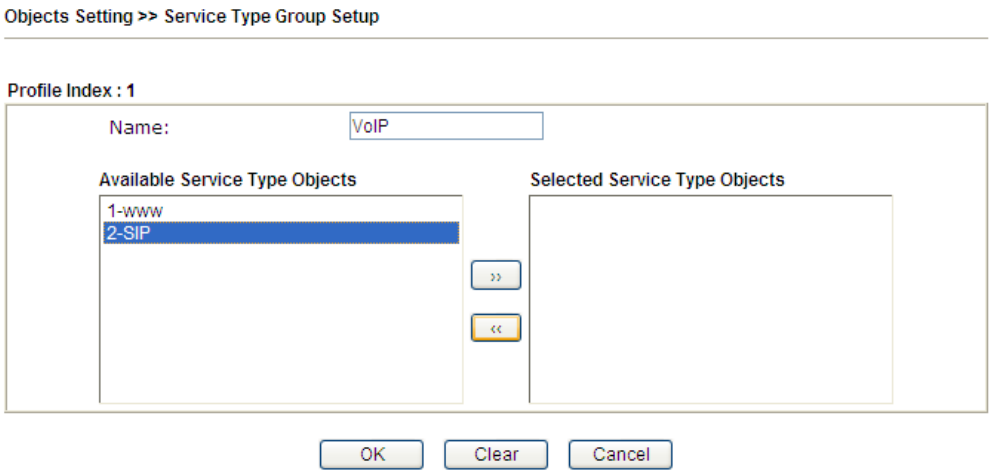


Available settings are explained as follows:

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.

This page is left blan.

Part VI Troubleshooting

This part will guide you to solve abnormal situations if you cannot access into the Internet after installing the modem and finishing the web configuration.

VI-1 Diagnostics

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.

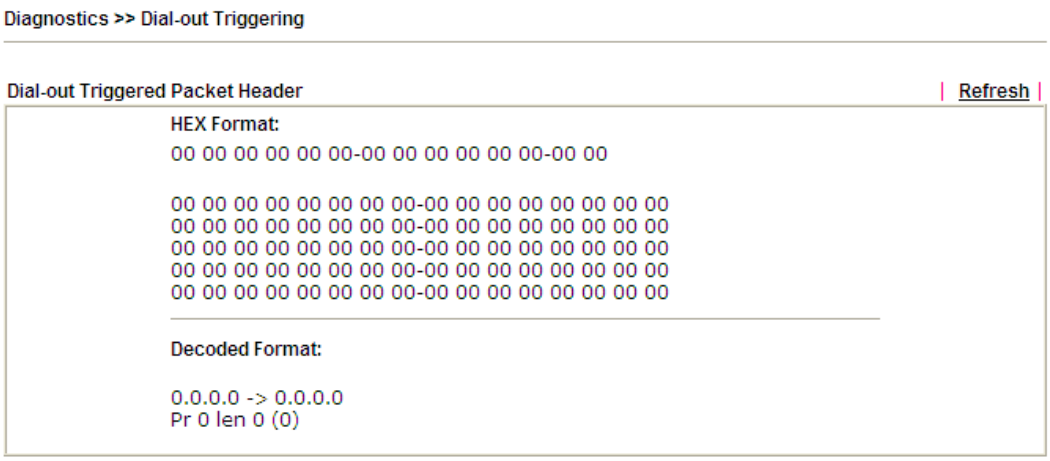
If all above stages are done and the modem still cannot run normally, it is the time for you to contact your dealer or DrayTek technical support for advanced help.

Web User Interface

Fisrt, take a look at the menu items under Diagnostics. Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router.

VI-1-1 Dial-out Triggering

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

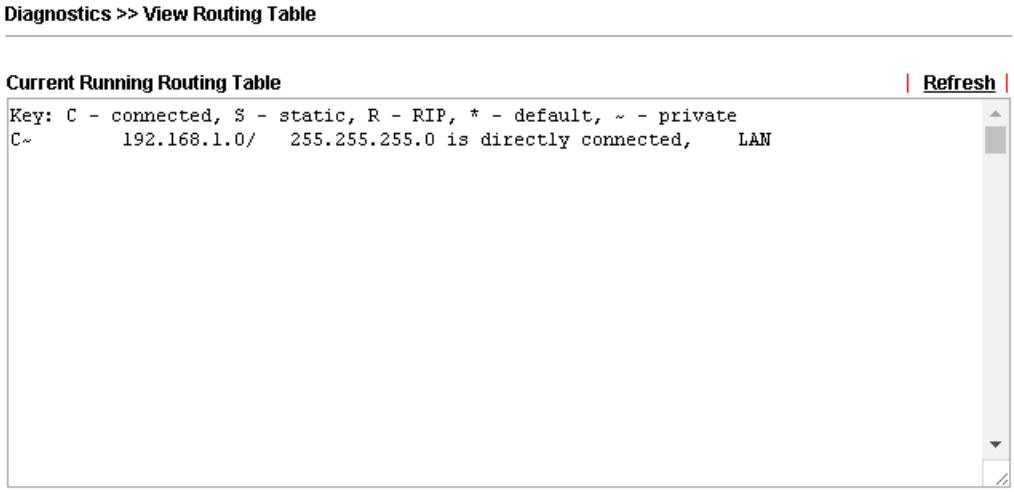


Available settings are explained as follows:

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.

VI-1-2 Routing Table

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



Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

VI-1-3 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.

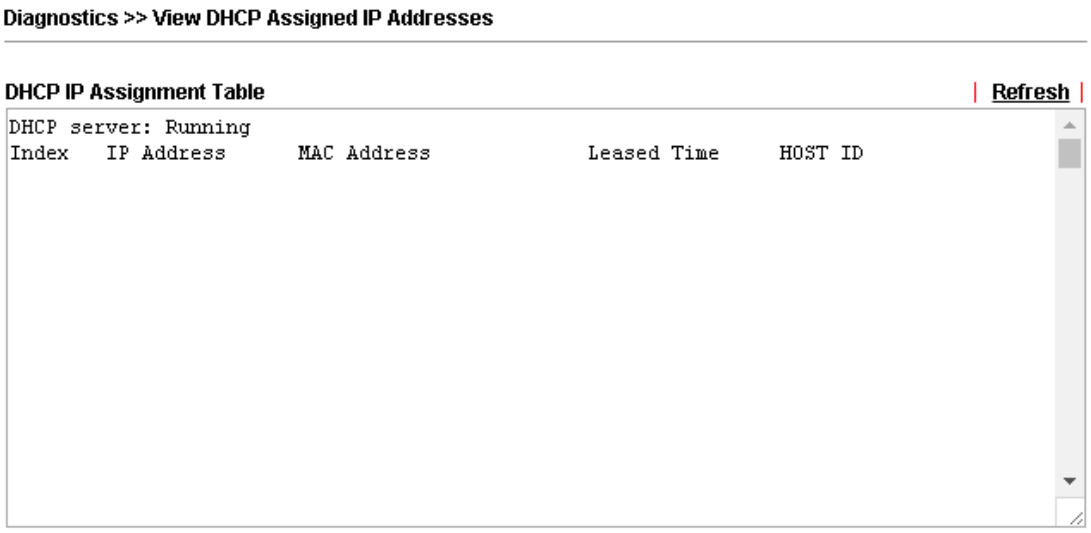
Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

VI-1-4 DHCP Table

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

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

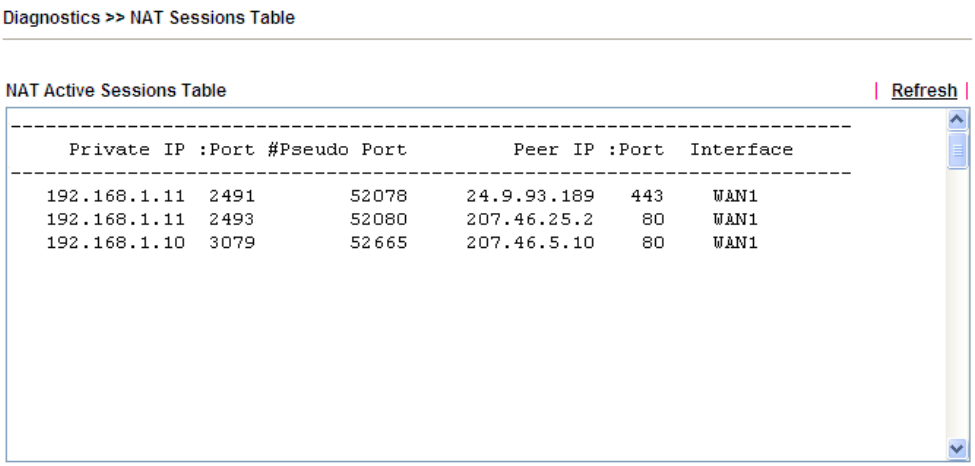


Available settings are explained as follows:

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

VI-1-5 NAT Sessions Table

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

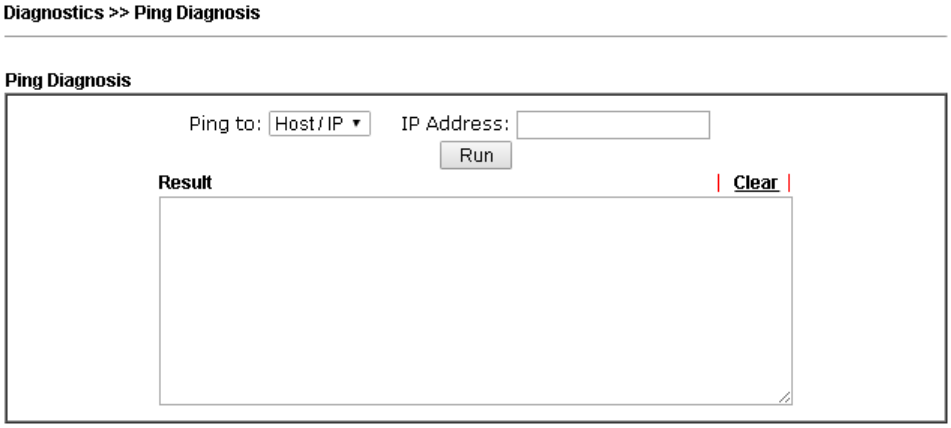


Available settings are explained as follows:

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.

VI-1-6 Ping Diagnosis

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



Available settings are explained as follows:

Item	Description
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.
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.

VI-1-7 Trace Route

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

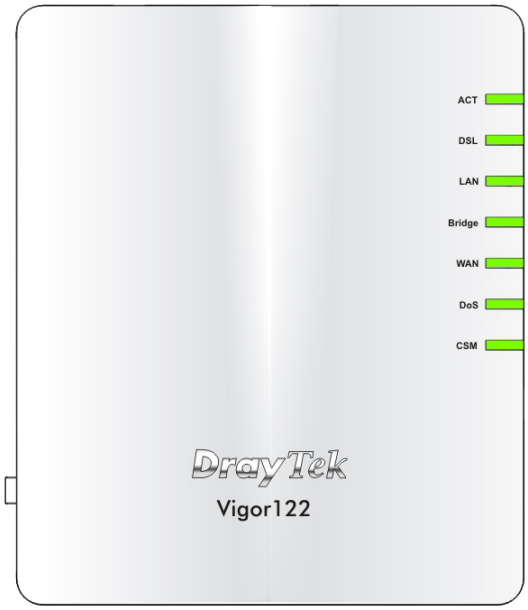
Available settings are explained as follows:

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

VI-2 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

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



3. If not, it means that there is something wrong with the hardware status. Simply back to **"I-2 Hardware Installation"** to execute the hardware installation again. And then, try again.

VI-3 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.

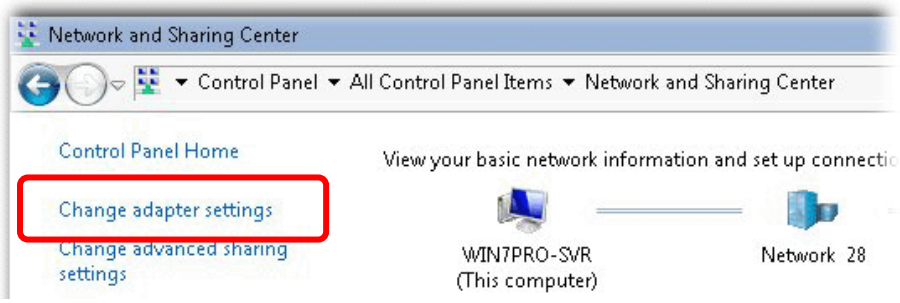
For Windows

Info

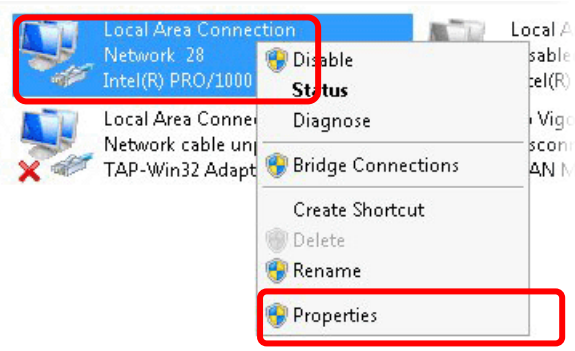
The example is based on Windows 7. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.DrayTek.com.

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

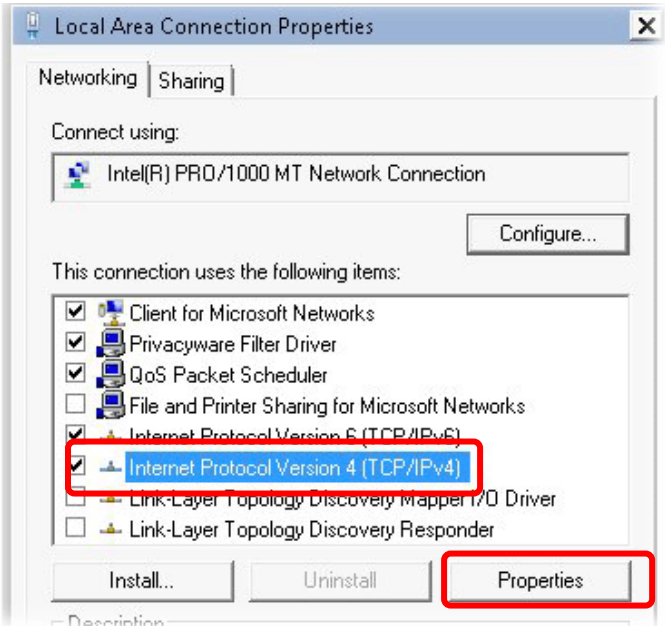
2. In the following window, click **Change adapter settings**.



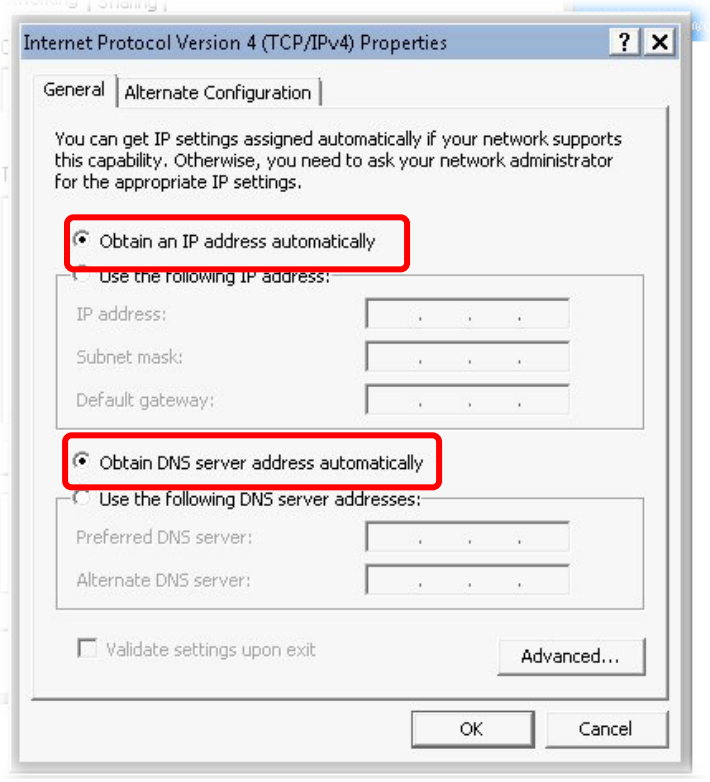
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



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

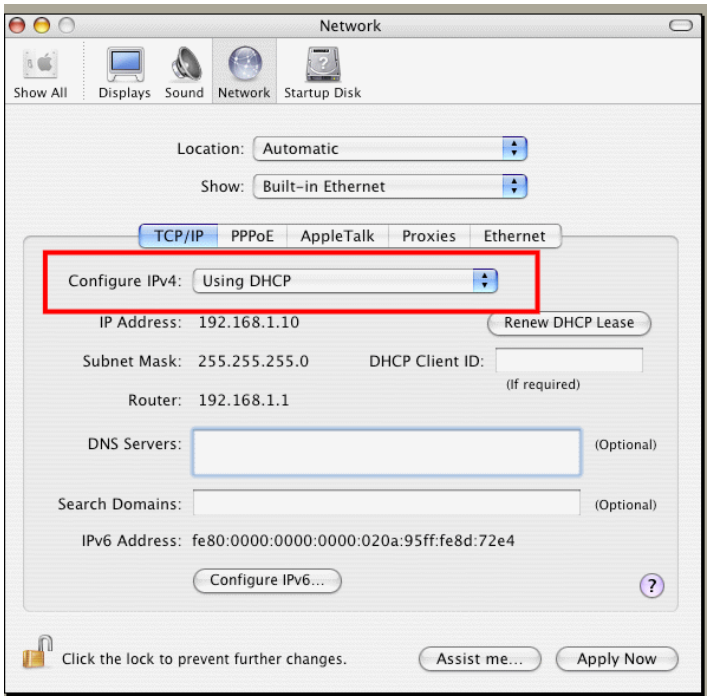


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



For Mac OS

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



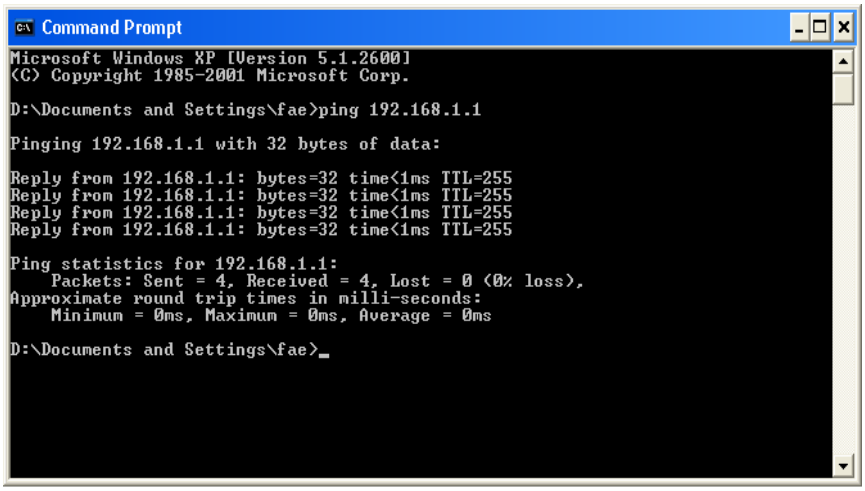
VI-4 Pinging the modem from Your Computer

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 VI-3)

Please follow the steps below to ping the modem correctly.

For Windows

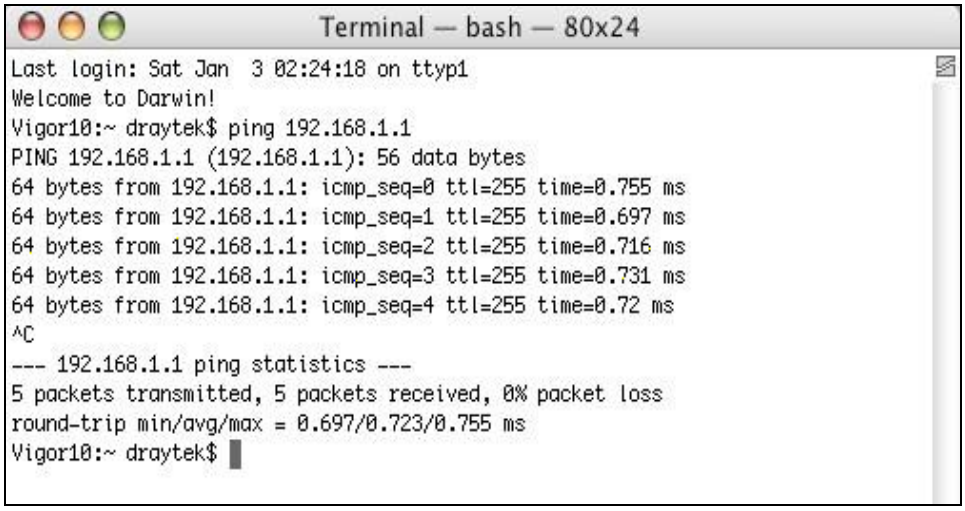
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista/7/8). The DOS command dialog will appear.



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

For Mac OS (Terminal)

1. Double click on the current used 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.


Terminal — bash — 80x24
Last login: Sat Jan 3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$

VI-5 Checking If the ISP Settings are OK or Not

If WAN connection cannot be up, check if the LEDs (according to the LED explanations listed on section I-1) are correct or not. If the LEDs are off, please:

When the LEDs are on and correct, yet the WAN connection still cannot be up, please:

Open **Internet Access** page and then check whether the ISP settings are set correctly.

VI-6 Backing to Factory Default Setting If Necessary

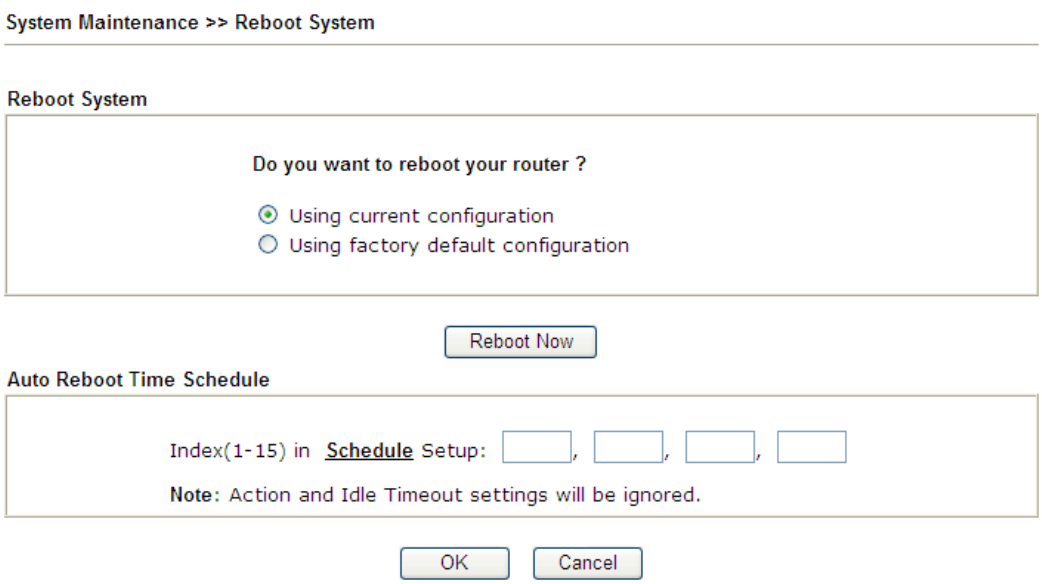
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the modem by software or hardware. Such function is available in **Admin Mode** only.

Info	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

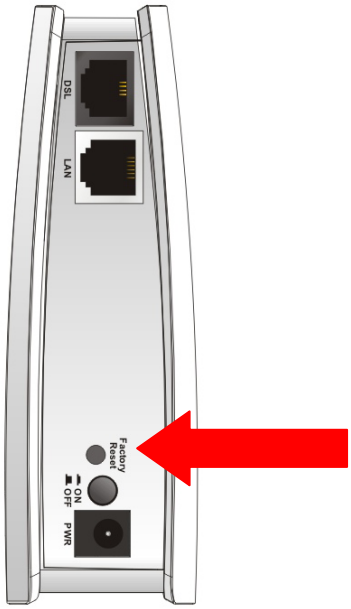
You can reset the modem to factory default via Web page. Such function is available in **Admin Mode** only.

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



Hardware Reset

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

VI-7 Contacting DrayTek

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.

This page is left blank.

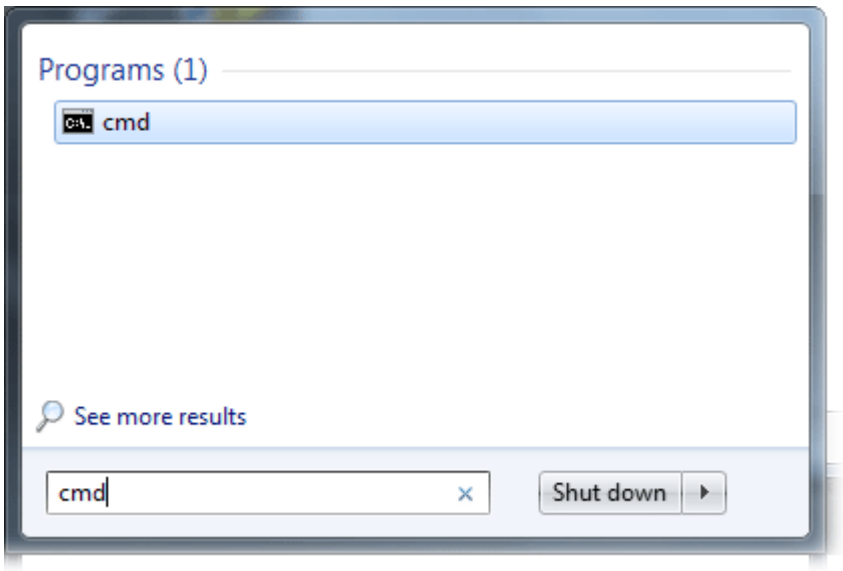
Part VII Telnet Commands

Accessing Telnet of Vigor122

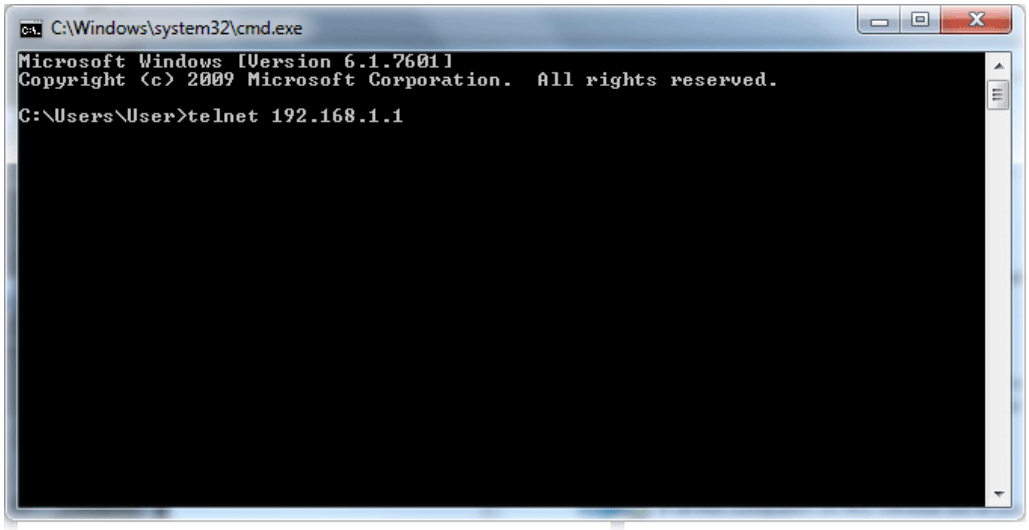
This chapter also gives you a general description for accessing telnet and describes the firmware versions for the modems explained in this manual.

Info	For Windows 7 user, please make sure the Windows Features of Telnet Client has been turned on under Control Panel>>Programs.

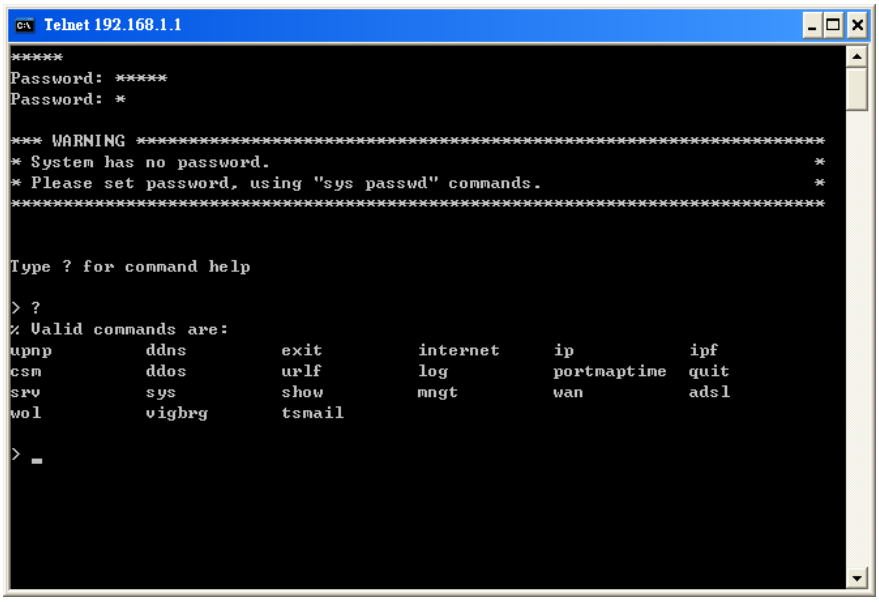
Type **cmd** and press Enter. The Telnet terminal will be open later.



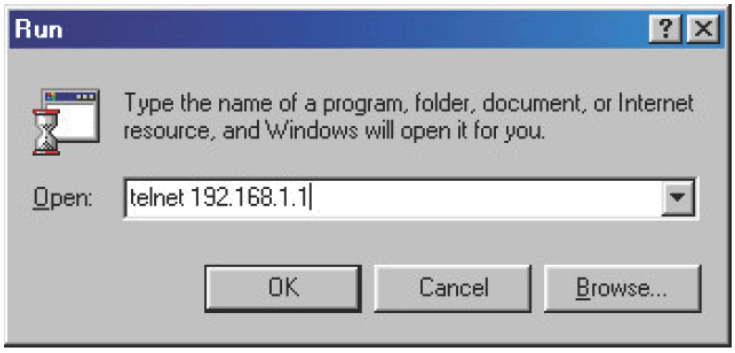
In the following window, type **Telnet 192.168.1.1** as below and press Enter. Note that the IP address in the example is the default address of the modem. If you have changed the default, enter the current IP address of the modem.



Next, type admin/admin for Account/Password. Then, type **?**. You will see a list of valid/common commands depending on the modem that your use.



For users using previous Windows system (e.g., 2000/XP), simply click **Start >> Run** and type **Telnet 192.168.1.1** in the Open box as below. Next, type admin/admin for Account/Password. And, type **?** to get a list of valid/common commands.



Telnet Command: upnp off

This command can close UPnP function.

Example

```
>upnp off
UPNP say bye-bye
```

Telnet Command: upnp on

This command can enable UPnP function.

Example

```
>upnp on
UPNP start.
```

Telnet Command: upnp nat

This command can display IGD NAT status.

Example

```
> upnp nat ?
*****************  IGD NAT Status  ****************

((0))
InternalClient >>192.168.1.10<<, RemoteHost >>0.0.0.0<<
InternalPort >>21<<, ExternalPort >>21<<
PortMapProtocol >>TCP<<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
Ftp Example [MICROSOFT]
((1))
InternalClient >>0.0.0.0<<, RemoteHost >>0.0.0.0<<
InternalPort >>0<<, ExternalPort >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
0<<

--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

Telnet Command: upnp service

This command can display the information of the UPnP service. UPnP service must be enabled first.

Example

```
> upnp on
UPNP start.
```

```
> upnp service
>>>>> SERVICE TABLE1 <<<<<
  serviceType urn:schemas-microsoft-com:service:OSInfo:1
  serviceId   urn:microsoft-com:serviceId:OSInfo1
  SCPDURL    /upnp/OSInfo.xml
  controlURL  /OSInfo1
  eventURL    /OSInfoEvent1
  UDN        uuid:774e9bbe-7386-4128-b627-001daa843464

>>>>> SERVICE TABLE2 <<<<<
  serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1
  serviceId   urn:upnp-org:serviceId:WANCommonIFC1
  SCPDURL    /upnp/WComIFCX.xml
  controlURL  /upnp?control=WANCommonIFC1
  eventURL    /upnp?event=WANCommonIFC1
  UDN        uuid:2608d902-03e2-46a5-9968-4a54ca499148
.
.
.
```

Telnet Command: upnp subscribe

This command can show all UPnP services subscribed.

Example

```
> upnp on
UPNP start.
> upnp subscribe
>>>> (1) serviceType urn:schemas-microsoft-com:service:OSInfo:1

>>>> (2) serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1

>>>> (3) serviceType urn:schemas-upnp-org:service:
WANDSLLinkConfig:1

>>>> (4) serviceType urn:schemas-upnp-org:service:WANPPPConnection:1

>
```

Telnet Command: upnp tmpvs

This command can display current status of temp Virtual Server of your router.

Example

```
Vigor> upnp tmpvs
******************  Temp virtual server status  ***************

((0))
```

```
real_addr  >>192.168.1.10<<, pseudo_addr >>172.16.3.229<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>TCP<<
time >>0<<

((1))
real_addr  >>0.0.0.0<<, pseudo_addr >>0.0.0.0<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>0<<
time >>0<<
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: ddns log

Displays the DDNS log.

Example

```
>ddns log
>
```

Telnet Command: exit

Type this command will leave telnet window.

Telnet Command: Internet

This command allows you to configure detailed settings for WAN connection.

Syntax

internet *-M n [-<command> <parameter> | …]*

Syntax Description

Parameter	Description
-M n	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 – 3) n=0: Offline n=1: PPPoE n=2: Dynamic IP n=3: Static IP
<command><parameter>|…]	The available commands with parameters are listed below. *[…]* means that you can type in several commands in one line.
-S <isp name>	Set ISP Name (max. 23 characters).
-u <username>	Set username (max. 49 characters) for Internet accessing.
-p <password>	Set password (max. 49 characters) for Internet accessing.
-a n	It means to set PPP Authentication Type and n means different types (represented by 0-1). n=0: PAP/CHAP (this is default setting) n=1: PAP Only

-t n	Set connection duration and n means different conditions. n=-1: Always-on n=1 ~ 999: Idle time for offline (default 180 seconds)
-i <ip address>	It means that *PPPoE server* will assign an IP address specified here for CPE (PPPoE client). If you type 0.0.0.0 as the <ip address>, ISP will assign suitable IP address for you. However, if you type an IP address here, the modem will use that one as a fixed IP.
-w <ip address>	It means to assign WAN IP address for such connection. Please type an IP address here for WAN port.
-n <netmask>	It means to assign netmask for WAN connection. You have to type 255.255.255.xxx (x is changeable) as the netmask for WAN port.
-g <gateway>	Assign gateway IP for such WAN connection.
-V	View Internet Access profile.

Example

```
> w > internet -M 1 -S tcom -u username -p password -a 0 -t -1  -i 0.0.0.0
> internet -V
Internet Mode: PPPoE
ISP Name: tcom
Username: username
Authentication: PAP/CHAP
Idle Timeout: -1
WAN IP: Dynamic IP

>
```

Telnet Command: ip aux

This command is used for configuring WAN IP Alias.

Syntax

ip aux add *[IP] [Join to NAT Pool]*

ip aux remove *[index]*

Syntax Description

Parameter	Description
add	Create a new WAN IP address.
remove	Delete an existed WAN IP address.
IP	It means the auxiliary WAN IP address.
Join to NAT Pool	0 (disable) or 1 (enable).
index	Type the index number of the table displayed on your screen.

Example

```
> ip aux add 192.168.1.65 1
% 192.168.1.65 has added in index 3.
```

When you type *ip aux*?, the current auxiliary WAN IP Address table will be shown as the following:

```
Index no.   Status  IP address      IP pool
-------------------------------------------
    1       Enable  172.16.3.229    Yes
    2       Enable  172.16.3.56     No
    3       Enable  172.16.3.113    No
```

Telnet Command: ip addr

This command allows users to set/add a specified LAN IP your router.

Syntax

ip addr *[IP address]*

Syntax Description

Parameter	Description
IP address	The LAN IP address.

Example

```
>ip addr 192.168.50.1
% Set IP address OK !!!
```

Info

When the LAN IP address is changed, the start IP address of DHCP server are still the same. To make the IP assignment of the DHCP server being consistent with this new IP address (they should be in the same network segment), the IP address of the PC must be fixed with the same LAN IP address (network segment) set by this command for accessing into the web user interface of the modem. Later, modify the start addresses for the DHCP server.

Telnet Command: ip nmask

This command allows users to set/add a specified netmask for your router.

Syntax

ip nmask *[IP netmask]*

Syntax Description

Parameter	Description
IP netmask	The netmask of LAN IP.

Example

```
> ip nmask 255.255.0.0
% Set IP netmask OK !!!
```

Telnet Command: ip arp

ARP displays the matching condition for IP and MAC address.

Syntax

ip arp add *[IP address] [MAC address] [LAN or WAN]*

ip arp del *[IP address] [LAN or WAN]*

ip arp flush

ip arp status

ip arp accept *[0/1/2/3/status]*

ip arp setCacheLife *[time]*

In which, **arp add** allows users to add a new IP address into the ARP table; **arp del** allows users to remove an IP address; **arp flush** allows users to clear arp cache; **arp status** allows users to review current status for the arp table; **arp accept** allows to accept or reject the source /destination MAC address; arp **setCacheLife** allows users to configure the duration in which ARP caches can be stored on the system. If **ip arp setCacheLife** is set with "60", it means you have an ARP cache at 0 second. Sixty seconds later without any ARP messages received, the system will think such ARP cache is expired. The system will issue a few ARP request to see if this cache is still valid.

Syntax Description

Parameter	Description
IP address	It means the LAN IP address.
MAC address	It means the MAC address of your router.
LAN or WAN	It indicates the direction for the arp function.
0/1/2/3/4/5	0: disable to accept illegal source mac address 1: enable to accept illegal source mac address 2: disable to accept illegal dest mac address 3: enable to accept illegal dest mac address status: display the setting status.
Time	Available settings will be 10, 20, 30,....2550 seconds.

Example

```
> i > ip arp status
[ARP Table]
 Index IP Address        MAC Address
   1   192.168.1.5       00-05-5D-E4-D8-EE

>
```

Telnet Command: ip dhcpc

This command is available for WAN DHCP.

Syntax

ip dhcpc *option*

ip dhcpc *release [1/2]*

ip dhcpc *renew [1/2]*

ip dhcpc *status*

Syntax Description

Parameter	Description
option	It is an optional setting for DHCP server.
Release [1/2]	It means to release current WAN IP address. 1: wan1 2: wan2
renew[1/2]	It means to renew the WAN IP address and obtain another new one. 1: wan1 2: wan2
status	It displays current status of DHCP client.

Example

```
> ip dhcpc status

DHCP Client Status: None active DHCP client!
```

Telnet Command: ip ping

This command allows users to ping IP address of WAN1/WAN2 for verifying if the WAN connection is OK or not.

Syntax

ip ping *[IP address]*

Syntax Description

Parameter	Description
IP address	It means the WAN IP address.

Example

```
>ip ping 172.16.3.229
Pinging 172.16.3.229 with 64 bytes of Data:
Receive reply from 172.16.3.229, time=0ms
Receive reply from 172.16.3.229, time=0ms
Receive reply from 172.16.3.229, time=0ms
Packets: Sent = 5, Received = 5, Lost = 0 <0% loss>
```

Telnet Command: ip tracert

This command allows users to trace the routes from the modem to the host.

Syntax

ip tracert *[Host/IP address] [WAN1/WAN2]*

Syntax Description

Parameter	Description
IP address	The target IP address.

WAN1/WAN2	It means the WAN port that the above IP address passes through.
Udp/Icmp	The UDP or ICMP.

Example

```
>ip tracert 22.128.2.62 WAN1
Traceroute to 22.128.2.62, 30 hops max
1   172.16.3.7  10ms
2   172.16.1.2  10ms
3   Request Time out.
4   168.95.90.66    50ms
5   211.22.38.134   50ms
6   220.128.2.62    50ms
Trace complete
```

Telnet Command: ip rip

This command allows users to set the RIP (routing information protocol) of IP.

Syntax

ip rip *[0/1/2]*

Syntax Description

Parameter	Description
0/1/2	0 means disable; 1 means first subnet and 2 means second subnet.

Example

```
> ip rip 1
%% Set RIP 1st subnet.%% Set RIP LAN1.
```

Telnet Command: ip route

This command allows users to set static route.

Syntax

ip route *add [dst] [netmask][gateway][ifno][rtype]*

ip route *del [dst] [netmask][rtype]*

ip route *status*

ip route *default [wan1/wan2/off/?]*

Syntax Description

Parameter	Description
add	It means to add an IP address as static route.
del	It means to delete specified IP address.
status	It means current status of static route.
dst	It means the IP address of the destination.
netmask	It means the netmask of the specified IP address.

gateway	It means the gateway of the connected router.
ifno	It means the connection interface. 3=WAN1, 4=WAN2, 5=WAN3, 6=WAN4
rtype	It means the type of the route. default : default route; static: static route.
cnc	It means current IP range for CNC Network.
default	Set WAN1/WAN2/off as current default route.
clean	Clean all of the route settings. 1: Enable the function. 0: Disable the function.

Example

```
> ip route add 172.16.2.0 255.255.255.0 172.16.2.4 3 static
> ip route status

Codes: C - connected, S - static, R - RIP, * - default, ~ - private
C~       192.168.1.0/   255.255.255.0 is directly connected, IF0
S         172.16.2.0/   255.255.255.0 via 172.16.2.4, IF3

>
```

Telnet Command: ip igmp_proxy

This command allows users to enable/disable igmp proxy server.

Syntax

ip igmp_proxy *set*

ip igmp_proxy *reset*

ip igmp_proxy *status*

Syntax Description

Parameter	Description
set	It means to enable proxy server.
reset	It means to disable proxy server.
status	It means to display current status for proxy server.

Example

```
This command is for setting IGMP General Query Interval
 The default value is 125000 ms
 Current Setting is:130000 ms
> ip igmp_proxy set
% ip igmp_proxy [set|reset|wan|status], IGMP Proxy is ON
> ip igmp_proxy status
%% ip igmp_proxy [set|reset|wan|status], IGMP Proxy is ON
%%% igmp_proxy WAN:
   239.255.255.250    state=1
   239.255.255.250    timer=0
```

Telnet Command: ip dmz

Specify MAC address of certain device as the DMZ host.

Syntax

ip dmz *[mac]*

Syntax Description

Parameter	Description
mac	It means the MAC address of the device that you want to specify.

Example

```
>ip dmz ?
% ip dmz <mac>,  now : 00-00-00-00-00-00
> ip dmz 11-22-33-44-55-66
> ip dmz ?
% ip dmz <mac>,  now : 11-22-33-44-55-66
>
```

Telnet Command: ip dmzswitch

This command is to enable /disable private IP DMZ or Active True IP DMZ for DMZ host.

Syntax

ip dmzswitch *off*

ip dmzswitch *private*

ip dmaswitch *active_trueip*

Syntax Description

Parameter	Description
off	Disable the function of DMZ host.
private	Enable private IP address of the DMZ host.
Active_trueip	Enable active true IP address of the DMZ host.

Example

```
> ip dmzswitch ?
%% ip dmzswitch [off|private|active_trueip], DMZ is OFF
> ip dmzswitch private
%% ip dmzswitch [off|private|trueip|active_trueip], PRIVATE IP DMZ is
ON
> ip dmzswitch trueip
> ip dmzswitch active_trueip
%% ip dmzswitch [off|private|trueip|active_trueip], ACTIVE TRUE IP DMZ
is ON
```

Telnet Command: ip bindmac

This command allows users to set IP-MAC binding for LAN host.

Syntax

ip bindmac *on*

ip bindmac *off*

ip bindmac *strict_on*

ip bindmac *show*

ip bindmac *add [IP][MAC]*

ip bindmac *del [IP]/all*

Syntax Description

Parameter	Description
on	Turn on IP bandmac policy. Even the IP is not in the policy table, it can still access into network.
off	Turn off all the bindmac policy.
strict_on	It means that only those IP address in IP bindmac policy table can access into network.
show	Display the IP address and MAC address of the pair of binded one.
add	Add one IP bindmac.
del	Delete one IP bindmac.
IP	Type the IP address for binding with specified MAC address.
MAC	Type the MAC address for binding with the IP address specified.
All	Delete all the IP bindmac settings.

Example

```
> ip bindmac add 192.168.1.46 00:50:7f:22:33:55
> ip bindmac show
ip bind mac function is turned ON
IP : 192.168.1.46 bind MAC : 00-50-7f-22-33-55
```

Telnet Command: ipf view

IPF users to view the version of the IP filter, to view/set the log flag, to view the running IP filter rules.

Syntax

ipf view *[-VcdhrtzZ]*

Syntax Description

Parameter	Description
-V	It means to show the version of this IP filter.
-c	It means to show the running call filter rules.
-d	It means to show the running data filter rules.
-h	It means to show the hit-number of the filter rules.
-r	It means to show the running call and data filter rules.
-t	It means to display all the information at one time.
-z	It means to clear a filter rule's statistics.
-Z	It means to clear IP filter's gross statistics.

Example

```
> > ipf view -V -c -d
------ Call Filter Rules ------
[Set 1 Rule 1]
  Schedule:
  Source IP: any
  Destination IP: any
  Service Type: TCP/UDP port from 137-139 to any
  Fragments: Don't Care
  Action: Block immediately
```

Telnet Command: ipf set

This command is used to set general rule for firewall.

Syntax

ipf set *[SET_NO] rule [RULE_NO] [Options]*

ipf set *[Options]*

Syntax Description

Parameter	Description
SET_NO	It means to specify the index number (from 1 to 12) of filter set.
RULE_NO	It means to specify the index number (from 1 to 7) of filter rule set.
Options	There are several options provided here, such as *-v*, *-c [SET_NO], -d [SET_NO],… and etc.*
-v	Type "-v" to view the configuration of general set.
-c [SET_NO]	It means to setup Call Filter, e.g., **-c 2**. The range for the index number you can type is "0" to "12" (0 means "disable).
-d [SET_NO]	It means to setup Data Filter, e.g., *-d 3*. The range for the index

	number you can type is “0” to “12” (0 means “disable).
-l [VALUE]	It means to setup Log Flag, e.g., *-l 2* Type “0” to disable the log flag. Type “1” to display the log of passed packet. Type “2” to display the log of blocked packet. Type “3” to display the log of non-matching packet.
- p [VALUE]	It means to setup actions for packet not matching any rule, e.g., *-p 1* Type “0” to let all the packets pass; Type “1” to block all the packets.

Example

```
> ipf set -c 1  #set call filter start from set 1

Setting saved.

> ipf set -v

Call Filter: Enable (Start Filter Set = 1)
Data Filter: Enable (Start Filter Set = 2)
Log Flag   : None

Actions for packet not matching any rule:
  Pass or Block    : Pass
  Content Management: None

Apply IP filter to VPN incoming packets           : Disable
Accept large incoming fragmented UDP or ICMP packets: Enable
>
```

Telnet Command: ipf flowtrack

This command is used to set and view flowtrack sessions.

Syntax

ipf flowtrack set *[-r]*

ipf flowtrack view *[-f]*

Syntax Description

Parameter	Description
-r	It means to refresh the flowtrack.
-t [value]	It means to specify a protocol (e.g., -t tcp). Available settings include: *tcp* *udp* *icmp*
-f	It means to show the sessions state of flowtrack. If you do not specify any IP address, then all the session state of flowtrack will be displayed.

Example

```
>ipf flowtrack set -r
Refresh the flowstate ok
> ipf flowtrack view -f
Start to show the flowtrack sessions state:
```

Telnet Command: ddos

This command allows users to configure the settings for DoS defense system.

Syntax

ddos *[-V | D | A]*

ddos *[-s ATTACK_F [THRESHOLD][TIMEOUT]]*

ddos *[-a | e [ATTACK_F][ATTACK_0] | d [ATTACK_F][ATTACK_0]]*

Syntax Description

Parameter	Description
-V	It means to view the configuration of DoS defense system.
-D	It means to deactivate the DoS defense system.
-A	It means to activate the DoS defense system.
-s	It means to enable the defense function for a specific attack and set its parameter(s).
ATTACK_F	It means to specify the name of flooding attack(s) or portscan, e.g., synflood, udpflood, icmpflood, or postscan.
THRESHOLD	It means the packet rate (packet/second) that a flooding attack will be detected. Set a value larger than 20.
TIMEOUT	It means the time (seconds) that a flooding attack will be blocked. Set a value larger than 5.
-a	It means to enable the defense function for all attacks listed in ATTACK_0.
-e	It means to enable defense function for a specific attack(s).
ATTACK_0	It means to specify a name of the following attacks: ip_option, tcp_flag, land, teardrop, smurf, pingofdeath, traceroute, icmp_frag, syn_frag, unknow_proto, fraggle.
-d	It means to disable the defense function for a specific attack(s).

Example

```
> ddos -A
The DoS Denfense system is Activated
> ddos -s synflood 50 10
synflood is enabled! Treshold=50 (pkt/sec)  timeout=10 (pkt/sec)
```

Telnet Command: urlf blist

This command allows users to set the URL access control.

Syntax

urlf blist *[noip]*

urlf blist *[on|off]*

urlf blist *[status]*

urlf blist *[INDEX –e |d [KEYWORD[SYMBOL KEYWORD]]*

urlf blist *[white | black]*

Syntax Description

Parameter	Description
noip	It means to prevent web access from the IP address.
on	It means to activate the functionality of the URL access control.
off	It means to deactivate the functionality of the URL access control.
status	It means to show the current configuration of the URL access control.
INDEX	It means the number of the specific item (e.g., 1-8).
-e	It means to enable the specific item with user's configuration.
-d	It means to disable the specific item for URL.
KEYWORD	It means the blocking keyword(s). The maximum length is 32.
SYMBOL	It means the space, comma or semicolon.
white	It means to block all packets except the ones that match the keyword in the list.
black	It means to pass all packets except the ones that match the keyword in the list.

Example

```
> urlf blist on
The functionality of the URL access control is activated!!
>urlf blist 1 –e news
The blocking keyword list valued with news and numbered with 1 has been
enabled.
```

Telnet Command: urlf setdefault

This command will reset all the configuration data for the contenet filtering.

Example

```
> urlf setdefault
All configuration data of the content filtering function is reset!!
```

Telnet Command: urlf esubnet

This command allows users to deal with the exempt subnets.

Syntax

urlf esubnet *[on|off]*

urlf esubnet *[status]*

urlf esubnet *[INDEX –e |d [IP_ADDRESS SUBNET_MASK]]*

Syntax Description

Parameter	Description
on	It means to activate the functionality of the exempt subnets.
off	It means to deactivate the functionality of the exempt sunbnets.
status	It means to show the current configuration of the exempt subnets.
INDEX	It means the number of the specific item (e.g., 1-4).
-e	It means to enable the specific item with the user's configuration.
-d	It means to disable the specific item.

Example

```
> urlf esubnet on
The functionality of the exceptional subnet is activated!!
> urlf esubnet 1 -e 192.168.1.55 255.255.255.0
The exceptional subnet list 192.168.1.55/255.255.255.0 and numberd
with 1 has be
en enabled

> urlf esubnet status
[V] Enable the functionality of the exceptional Subnets!!
  1. [V] 192.168.1.55/255.255.255.0
  2. [ ] 0.0.0.0/0.0.0.0
  3. [ ] 0.0.0.0/0.0.0.0
  4. [ ] 0.0.0.0/0.0.0.0
```

Telnet Command: urlf webf

This command allows users to restrict the web filter features.

Syntax

urlf webf *[on|off]*

urlf webf *[status]*

urlf webf *[-e|d [java][activex][zip][exe][mms][cookie][proxy]]*

Syntax Description

Parameter	Description
on	It means to activate the functionality of the restricted web features.
off	It means to deactivate the functionality of the restricted web features.
status	It means to show the current configuration of the restricted web features.
-e	It means to enable the specific item(s).
-d	It means to disable the specific item(s).

Example

```
> urlf webf on
The functionality of restricted web features is activated!!
```

```
> urlf webf -e java mms
java is enabled!

mms is enabled!
> urlf webf status
[V] Enable restrict web feature!!
  [V] java    [ ] activex    [ ] zip    [ ] exe    [V] mms
  [ ] cookie    [ ] proxy
```

Telnet Command: urlf tschedule

This command allows users to choose the call schedule for URL access control. You can choose up to four sets of call schedule profiles.

Syntax

urlf tschedule *Schedule1[Schedule2][Schedule3][Schedule4]*

Syntax Description

Parameter	Description
Schedule1~4	It means the index of the profile for the call schedule setup (1-15). You can set 4 schedules in this command from the 15 sets of call schedules. Action/Idle Timeout settings in the Call Schedule setting page will be ignored. Set "0" to clear current settings.

Example

```
> urlf tschedule 1
New URL Fitler time schedule:  1
>
```

Telnet Command: Log

This command allows users to view log for WAN interface such as call log, IP filter log, flush log buffer, etc.

Syntax

log *[-cfhiptwx?] [-F a| c | f | w]*

Syntax Description

Parameter	Description
-c	It means to show the latest call log.
-f	It means to show the IP filter log.
-F	It means to show the flush log buffer. a: flush all logs c: flush the call log f: flush the IP filter log w: flush the WAN log
-h	It means to show this usage help.
-p	It means to show PPP/MP log.

-t	It means to show all logs saved in the log buffer.
-w	It means to show WAN log.
-x	It means to show packet body hex dump.

Example

```
> log -w
0:00:07.190 DSL: DSL Channel = 0
0:00:07.190 DSL: VPI/VCI = 8/35
0:00:07.190 DSL: Mode = 0[PPPoA]
0:00:07.190 DSL: Encapsulation type = 0[VC_MUX]
0:00:07.190 DSL: Modulation type = 4[MULTI]
0:00:07.300 DSL: DSL_DRV_Init error code: 0
0:02:08.340 DSL: DSL Rebooting...IPLM
0:04:09.290 DSL: DSL Rebooting...IPLM
0:06:10.240 DSL: DSL Rebooting...IPLM
0:08:11.210 DSL: DSL Rebooting...IPLM
0:10:12.170 DSL: DSL Rebooting...IPLM
0:12:13.130 DSL: DSL Rebooting...IPLM
0:14:14.090 DSL: DSL Rebooting...IPLM
0:16:15.040 DSL: DSL Rebooting...IPLM
0:18:16.000 DSL: DSL Rebooting...IPLM
0:20:16.960 DSL: DSL Rebooting...IPLM
0:22:17.900 DSL: DSL Rebooting...IPLM
0:24:18.850 DSL: DSL Rebooting...IPLM
0:26:19.800 DSL: DSL Rebooting...IPLM
0:28:20.750 DSL: DSL Reboot    .
0:30:21.710 DSL: DSL Rebooting...IPLM
0:32:22.670 DSL: DSL Rebooting...IPLM
0:34:23.610 DSL: DSL Rebooting...IPLM
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: portmaptime

This command allows you to set a time of keeping the session connection for specified protocol.

Syntax

portmaptime *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
[<command> <parameter>|...]	The available commands with parameters are listed below. *[...]* means that you can type in several commands in one line.
-t <sec>	It means “TCP” protocol. <sec>: Type a number to set the TCP session timeout.
-u <sec>	It means “UDP” protocol. <sec>: Type a number to set the UDP session timeout.
-i <sec>	It means “IGMP” protocol. <sec>: Type a number to set the IGMP session timeout.

-l <List>	List all settings.

Example

```
> portmaptime -t 980
> portmaptime -u 300
> portmaptime -i 10
> portmaptime -l
-------Your    setting (min)------
-------TCP     Time: 980 ------
-------UDP     Time: 300 ------
-------IGMP    Time: 10 ------
>
```

Telnet Command: quit

This command can exit the telnet command screen.

Telnet Command: srv dhcp gateway

This command allows users to specify gateway address for DHCP server.

Syntax

srv dhcp gateway *[?]*

srv dhcp gateway *[Gateway IP]*

Syntax Description

Parameter	Description
?	It means to display current gateway that you can use.
Gateway IP	It means to specify a gateway address used for DHCP server.

Example

```
> srv dhcp gateway 192.168.2.1
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the modem.
```

Telnet Command: srv dhcp ipcnt

This command allows users to specify IP counts for DHCP server.

Syntax

srv dhcp ipcnt *[?]*

srv dhcp ipcnt *[IP counts]*

Syntax Description

Parameter	Description
?	It means to display current used IP count number.
IP counts	It means the number that you have to specify for the DHCP server.

Example

```
> srv dhcp ipcnt ?
% srv dhcp ipcnt <IP counts>
% Now: 50
```

Telnet Command: srv dhcp off

This function allows users to turn off DHCP server. It needs rebooting router, please type "sys reboot" command to reboot router.

Telnet Command: srv dhcp on

This function allows users to turn on DHCP server. It needs rebooting router, please type "sys reboot" command to reboot router.

Telnet Command: srv dhcp startip

Syntax

srv dhcp startip *[?]*

srv dhcp startip *[IP address]*

Syntax Description

Parameter	Description
?	It means to display current used start IP address.
IP address	It means the IP address that you can specify for the DHCP server as the starting point.

Example

```
> srv dhcp startip 192.168.1.53
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the modem.
```

Telnet Command: srv dhcp status

This command can display general information for the DHCP server, such as IP address, MAC address, leased time, host ID and so on.

Example

```
> srv dhcp status
DHCP server: Running
Default gateway: 192.168.1.1
Index   IP Address     MAC Address           Leased Time     HOST ID
1      192.168.1.113   00-05-5D-E4-D8-EE      17:20:08       A1000351
```

Telnet Command: srv dhcp leasetime

This command can set the lease time for the DHCP server.

Syntax

srv dhcp leasetime *[?]*

srv dhcp leasetime *[Lease Time (sec)]*

Syntax Description

Parameter	Description
?	It means to display current leasetime used for the DHCP server.
Lease Time (sec)	It means the lease time that DHCP server can use. The unit is second.

Example

```
> srv dhcp leasetime ?
% srv dhcp leasetime <Lease Time (sec.)>
% Now: 259200
>
```

Telnet Command: srv dhcp frcdnsmanl

This command can force the modem to invoke DNS Server IP address.

Syntax

srv dhcp frcdnsmanl *[on]*

srv dhcp frcdnsmanl *[off]*

Syntax Description

Parameter	Description
?	It means to display the current status.
on	It means to use manual setting for DNS setting.
Off	It means to use auto settings acquired from ISP.

Example

```
> srv dhcp frcdnsmanl on

% Domain name server now is using manual settings!

> srv dhcp frcdnsmanl off

% Domain name server now is using auto settings!
```

Telnet Command: srv dhcp dns1

This command allows users to set Primary IP Address for DNS Server in LAN.

Syntax

srv dhcp dns1 *[?]*

srv dhcp dns1 *[DNS IP address]*

Syntax Description

Parameter	Description
?	It means to display current IP address of DNS 1 for the DHCP server.
DNS IP address	It means the IP address that you want to use as DNS1. **Note:** The IP Routed Subnet DNS must be the same as NAT Subnet DNS).

Example

```
> srv dhcp dns1 168.95.1.1
% srv dhcp dns1 <DNS IP address>
% Now: 168.95.1.1
(IP Routed Subnet dns same as NAT Subnet dns)
```

Telnet Command: srv dhcp dns2

This command allows users to set Secondary IP Address for DNS Server in LAN.

Syntax

srv dhcp dns2 *[?]*

srv dhcp dns2 *[DNS IP address]*

Syntax Description

Parameter	Description
?	It means to display current IP address of DNS 2 for the DHCP server.
DNS IP address	It means the IP address that you want to use as DNS2. **Note:** The IP Routed Subnet DNS must be the same as NAT Subnet DNS).

Example

```
> srv dhcp dns2 10.1.1.1
% srv dhcp dns2 <DNS IP address>
% Now: 10.1.1.1
(IP Routed Subnet dns same as NAT Subnet dns)
```

Telnet Command: srv dhcp relay

This command allows users to set DHCP relay setting.

Syntax

srv dhcp relay servip *[server ip]*

srv dhcp relay subnet *[index]*

Syntax Description

Parameter	Description
server ip	It means the IP address that you want to used as DHCP server.
Index	It means subnet 1 or 2. Please type 1 or 2. The modem will invoke this function according to the subnet 1 or 2 specified here.

Example

```
> srv dhcp relay servip 192.168.1.46
> srv dhcp relay subnet 2
>srv dhcp relay servip ?
% srv dhcp relay servip <server ip>
% Now: 192.168.1.46
```

Telnet Command: srv dhcp badip

This command is reserved for future use.

Syntax

srv dhcp badip

Example

```
> srv dhcp badip
>
```

Telnet Command: srv dhcp public

This command allows users to configure DHCP server for second subnet.

Syntax

srv dhcp public *start [IP address]*

srv dhcp public *cnt [IP counts]*

srv dhcp public *status*

srv dhcp public *add [MAC Addr XX-XX-XX-XX-XX-XX]*

srv dhcp public *del [MAC Addr XX-XX-XX-XX-XX-XX/all/ALL]*

Syntax Description

Parameter	Description
start	It means the starting point of the IP address pool for the DHCP server.
IP address	It means to specify an IP address as the starting point in the IP address pool.
cnt	It means the IP count number.
IP counts	It means to specify the number of IP addresses in the pool. The maximum is 10.
status	It means the execution result of this command.
add	It means creating a list of hosts to be assigned.
del	It means removing the selected MAC address.

MAC Addr	It means to specify MAC Address of the host.
all/ALL	It means all of the MAC addresses.

Example

```
> srv dhcp start 192.168.1.100
 This function need rebooting router, please type "sys reboot" command
to reboot router.
```

Telnet Command: srv dhcp nodetype

This command can set the node type for the DHCP server.

Syntax

srv dhcp nodetype <*count*>

Syntax Description

Parameter	Description
count	It means to specify a type for node. 1. B-node 2. P-node 4. M-node 8. H-node

Example

```
> srv dhcp nodetype 1
> srv dhcp nodetype ?
%% srv dhcp nodetype <count>
%% 1. B-node 2. P-node 4. M-node 8. H-node
% Now: 1
```

Telnet Command: srv dhcp primWINS

This command can set the primary IP address for the DHCP server.

Syntax

srv dhcp primWINS *[WINS IP address]*

srv dhcp primWINS clear

Syntax Description

Parameter	Description
WINS IP address	It means the IP address of primary WINS server.
clear	It means to remove the IP address settings of primary WINS server.

Example

```
> srv dhcp primWINS 192.168.1.88
> srv dhcp primWINS ?
%% srv dhcp primWINS <WINS IP address>
%% srv dhcp primWINS clear
% Now: 192.168.1.88
```

Telnet Command: srv dhcp secWINS

This command can set the secondary IP address for the DHCP server.

Syntax

srv dhcp secWINS *[WINS IP address]*

srv dhcp secWINS clear

Syntax Description

Parameter	Description
WINS IP address	It means the IP address of secondary WINS server.
clear	It means to remove the IP address settings of second WINS server.

Example

```
> srv dhcp secWINS 192.168.1.180
> srv dhcp secWINS ?
%% srv dhcp secWINS <WINS IP address>
%% srv dhcp secWINS clear
% Now: 192.168.1.180
```

Telnet Command: srv dhcp tftp

This command can set the TFTP server as the DHCP server.

Syntax

srv dhcp tftp <*TFTP server name*>

Syntax Description

Parameter	Description
TFTP server name	It means to type the name of TFTP server.

Example

```
> srv dhcp tftp TF123
> srv dhcp tftp ?
%% srv dhcp tftp <TFTP server name>
% Now: TF123
```

Telnet Command: srv nat dmz

This command allows users to set DMZ host. Before using this command, please set WAN IP Alias first.

Syntax

srv nat dmz mapping *[wan1/wan2] [Private IP Address]*

srv nat dmz remove *[wan1/wan2]*

Syntax Description

Parameter	Description
wan1/wan2	Specify means to map selected WAN IP to certain host. wan1 wan2
private IP Address	Type the IP address to be mapped to specified WAN.
remove	Delete the settings for specified WAN interface.

Example

```
> srv nat dmz mapping wan2 192.168.1.25
%% Private IP address 192.168.1.25 was mapped on 128.31.217.248 (wan2)
```

Telnet Command: srv nat ipsecpass

This command allows users to enable or disable IPSec ESP tunnel passthrough and IKE source port (500) preservation.

Syntax

Srv nat ipsecpass *[options]*

Syntax Description

Parameter	Description
[options]	The available commands with parameters are listed below.
on	It means to enable IPSec ESP tunnel passthrough and IKE source port (500) preservation.
off	It means to disable IPSec ESP tunnel passthrough and IKE source port (500) preservation.
status	It means to display current status for checking.

Example

```
> srv nat ipsecpass status
%% Status: IPsec ESP pass-thru and IKE src_port:500 preservation is
OFF.
```

Telnet Command: srv nat openport

This command allows users to set open port settings for NAT server.

Syntax

srv nat openport list *<[All] | [Profile Index]>*

srv nat openport enable*<Index>*

srv nat openport disable *<Index>*

srv nat openport comment *<Index> <Comment>*

srv nat openport dstip *<Index> <Destination local IP address>*

srv nat openport add *<Profile index> <Subitem index> <WAN IP addr> <Pvt IP addr> <Protocol> <Start port> <End port>*

srv nat openport remove *<Profile index> [Subitem index]*

srv nat openport flush

Syntax Description

Parameter	Description
list <[All] | [Profile Index]>	Display status information for all of the profiles or specified profile.
enable <Index>	Enable the selected index profile. Index – Range from 1 to 20 (profile index number).
disable <Index>	Disable the selected index profile. Index – Range from 1 to 20 (profile index number).
comment <Index> <Comment>	Index – Range from 1 to 20 (profile index number). Comment – Type a description for such profile.
dstip <Index> <Destination local IP address>	It means to specify destination IP address for an open port profile. Index – Range from 1 to 20. Destination local IP address – Type the IP address of the destination.
add *<Profile index> <Subitem index> <WAN IP addr> <Pvt IP addr> <Protocol> <Start port> <End port>*	It means to create new open port profile. Profile index – Range from 1 to 20. Subitem index – Range form 1 to 10. Protocol – TCP or UDP. WAN IP Addr – Type the IP address of the WAN interface. Private IP Addr – Type the private IP address. Start port – Type a value as the starting port. End port – Type a value as the ending port.
Remove <Profile index> [Subitem index]	It means to remove specified profile. Profile index – Range from 1 to 20. Subitem index – Range form 1 to 10.
flush	It means to return to factory settings for all the open ports profiles.

Example

```
> srv nat openport enable 1
%% Open port profile 1 has enabled.

> srv nat openport comment 1 for_marketing
%% Ok.
```

```
> srv nat openport dstip 1 192.168.1.99
%% Ok.
```

Telnet Command: srv nat portmap

This command allows users to set port redirection table for NAT server.

Syntax

srv nat portmap *add [idx][serv name][proto][pub port][pri ip][pri port][wan1/wan2]*

srv nat portmap *del [idx]*

srv nat portmap *disable [idx]*

srv nat portmap *enable [idx] [proto]*

srv nat portmap *flush*

srv nat portmap *table*

Syntax Description

Parameter	Description
Add[idx]	It means to add a new port redirection table with an index number. Available index number is from 1 to 10.
serv name	It means to type one name as service name.
proto	It means to specify TCP or UDP as the protocol.
pub port	It means to specify which port can be redirected to the specified Private IP and Port of the internal host.
pri ip	It means to specify the private IP address of the internal host providing the service.
pri port	It means to specify the private port number of the service offered by the internal host.
wan1/wan2	It means to specify WAN interface for the port redirection.
del [idx]	It means to remove the selected port redirection setting.
disable [idx]	It means to inactivate the selected port redirection setting.
enable [idx]	It means to activate the selected port redirection setting.
flush	It means to clear all the port mapping settings.
table	It means to display Port Redirection Configuration Table.

Example

```
> srv nat portmap add 1 game tcp 80 192.168.1.11 100 wan1
> srv nat portmap table

NAT Port Redirection Configuration Table:

Index  Service Name   Protocol  Public Port  Private IP     Private
Port ifno
 1    game            6         80   192.168.1.11       100
-1
 2                    0          0                    0     -2
 3                    0          0                    0     -2
 4                    0          0                    0     -2
 5                    0          0                    0     -2
```

```
 6                    0          0                    0      -2
 7                    0          0                    0      -2
 8                    0          0                    0      -2
 9                    0          0                    0      -2
10                    0          0                    0      -2
11                    0          0                    0      -2
12                    0          0                    0      -2
13                    0          0                    0      -2
14                    0          0                    0      -2
15                    0          0                    0      -2
16                    0          0                    0      -2
17                    0          0                    0      -2
18                    0          0                    0      -2

19                    0          0                    0      -2

20                    0          0                    0      -2


Protocol: 0 = Disable, 6 = TCP, 17 = UDP
```

Telnet Command: srv nat status

This command allows users to view NAT Port Redirection Running Table.

Example

```
> srv nat status
NAT Port Redirection Running Table:

Index  Protocol  Public Port   Private IP       Private Port
 1          6          80   192.168.1.11            100
 2          0           0   0.0.0.0                   0
 3          0           0   0.0.0.0                   0
 4          0           0   0.0.0.0                   0
 5          0           0   0.0.0.0                   0
 6          0           0   0.0.0.0                   0
 7          0           0   0.0.0.0                   0
 8          0           0   0.0.0.0                   0
 9          0           0   0.0.0.0                   0
10          0           0   0.0.0.0                   0
11          0           0   0.0.0.0                   0
12          0           0   0.0.0.0                   0
13          0           0   0.0.0.0                   0
14          0           0   0.0.0.0                   0
15          0           0   0.0.0.0                   0
16          0           0   0.0.0.0                   0
17          0           0   0.0.0.0                   0
18          0           0   0.0.0.0                   0
19          0           0   0.0.0.0                   0

20          0           0   0.0.0.0                   0
```

```
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: srv nat showall

This command allows users to view a summary of NAT port redirection setting, open port and DMZ settings.

Example

```
>  srv nat showall ?
Index   Proto   WAN IP:Port              Private IP:Port           Act
****************************************************************************
****
R01     TCP     0.0.0.0:80               192.168.1.11:100          Y

O01     TCP     0.0.0.0:23~83             192.168.1.100:23~83        Y

D01     All     0.0.0.0                  192.168.1.96              Y

R:Port Redirection, O:Open Ports, D:DMZ
> sys tr069 get Int. nextlevel
Total number of parameter is 24
Total content length of parameter is 915
InternetGatewayDevice.LANDeviceNumberOfEntries
InternetGatewayDevice.WANDeviceNumberOfEntries
InternetGatewayDevice.DeviceInfo.
InternetGatewayDevice.ManagementServer.
InternetGatewayDevice.Time.
InternetGatewayDevice.Layer3Forwarding.
InternetGatewayDevice.LANDevice.
InternetGatewayDevice.WANDevice.
InternetGatewayDevice.Services.
InternetGatewayDevice.X_00507F_InternetAcc.
InternetGatewayDevice.X_00507F_LAN.
InternetGatewayDevice.X_00507F_NAT.
InternetGatewayDevice.X_00507F_Firewall.
InternetGatewayDevice.X_00507F_Bandwidth.
InternetGatewayDevice.X_00507F_Applications.
InternetGatewayDevice.X_00507F_VPN.
InternetGatewayDevice.X_00507F_VoIP.
InternetGatewayDevice.X_00507F_WirelessLAN.
InternetGatewayDevice.X_00507F_System.
InternetGatewayDevice.X_00507F_Status.

InternetGatewayDevice.X_00507F_Diagnostics.
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
```

Telnet Command: sys sip_alg

This command can turn on/off SIP ALG (Application Layer Gateway) for traversal.

Syntax

sys sip_alg *[1]*

sys sip_alg *[0]*

Syntax Description

Parameter	Description
1	It means to turn on SIP ALG.
0	It means to turn off SIP ALG.

Example

```
> sys sip_alg ?
usage: sys sip_alg [value]
 0 - disable SIP ALG
 1 - enable SIP ALG
 current SIP ALG is disabled
```

Telnet Command: sys admin

This command is used for RD engineer to access into test mode of Vigor router.

Telnet Command: sys cfg

This command reset the modem with factory default settings. When a user types this command, all the configuration will be reset to default setting.

Syntax

sys cfg default

sys cfg status

Syntax Description

Parameter	Description
default	It means to reset current settings with default values.
status	It means to display current profile version and status.

Example

```
> sys cfg status
Profile version: 3.0.0   Status: 1 (0x491e5e6c)
> sys cfg default
>
```

Telnet Command: sys cmdlog

This command displays the history of the commands that you have typed.

Example

```
> sys cmdlog
% Commands Log: (The lowest index is the newest !!!)
   [1] sys cmdlog
   [2] sys cmdlog ?
   [3] sys ?
   [4] sys cfg status
   [5] sys cfg ?
```

Telnet Command: sys ftpd

This command displays current status of FTP server.

Syntax

sys ftpd *on*

sys ftpd *off*

Syntax Description

Parameter	Description
on	It means to turn on the FTP server of the system.
off	It means to turn off the FTP server of the system.

Example

```
> sys ftpd on
% sys ftpd turn on !!!
```

Telnet Command: sys domainname

This command can set and remove the domain name of the system when DHCP mode is selected for WAN.

Syntax

sys domainname *[wan1/wan2] [Domain Name Suffix]*

sys domainname *[wan1/wan2] clear*

Syntax Description

Parameter	Description
wan1/wan2	It means to specify WAN interface for assigning a name for it.
Domain Name Suffix	It means the name for the domain of the system. The maximum number of characters that you can set is 40.
clear	It means to remove the domain name of the system.

Example

```
> sys domainname wan1 clever
> sys domainname wan2 intellegent
> sys domainname ?
% sys domainname <wan1/wan2> <Domain Name Suffix (max. 40 characters)>
% sys domainname <wan1/wan2> clear
% Now: wan1 == clever, wan2 ==intelligent
>
```

Telnet Command: sys iface

This command displays the current interface connection status (UP or Down) with IP address, MAC address and Netmask for the modem.

Example

```
> sys iface
Interface 0 Ethernet:
Status: UP
IP Address: 192.168.1.1      Netmask: 0xFFFFFF00 (Private)
IP Address: 0.0.0.0          Netmask: 0xFFFFFFFF
MAC: 00-50-7F-00-00-00
Interface 4 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-02
Interface 5 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-03
Interface 6 Ethernet:
Status: DOWN
IP Address: 0.0.0.0          Netmask: 0x00000000
MAC: 00-50-7F-00-00-04
```

```
Interface 7 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-05
Interface 8 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-06

Interface 9 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-07
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
---
>
```

Telnet Command: sys name

This command can set and remove the name for the modem when DHCP mode is selected for WAN.

Syntax

sys name *[wan1/wans=2] [ASCII string]*

sys name *[wan1/wan2]* **clear**

Syntax Description

Parameter	Description
wan1/wan2	It means to specify WAN interface for assigning a name for it.
ASCII string	It means the name for router. The maximum character that you can set is 20.

Example

```
> sys name wan1 drayrouter
> sys name ?
% sys name <wan1/wan2> <ASCII string (max. 20 characters)>
% sys name <wan1/wan2> clear
% Now: wan1 == drayrouter, wan2 ==
```

Note: Such name can be used to recognize router's identification in SysLog dialog.

Telnet Command: sys passwd

This command allows users to set password for the administrator.

Syntax

sys passwd *[ASCII string]*

Syntax Description

Parameter	Description
ASCII string	It means the password for administrator. The maximum character that you can set is 23.

Example

```
> sys passwd admin123
>
```

Telnet Command: sys reboot

This command allows users to restart the modem immediately.

Example

```
> sys reboot
>
```

Telnet Command: sys autoreboot

This command allows users to restart the modem automatically within a certain time.

Syntax

sys autoreboot *[on/off/hour(s)]*

Syntax Description

Parameter	Description
on/off	On – It means to enable the function of auto-reboot. Off – It means to disable the function of auto-reboot.
hours	It means to set the time schedule for router reboot. For example, if you type "2" in this field, the modem will reboot with an **interval** of two hours.

Example

```
> sys autoreboot on
 autoreboot is ON
> sys autoreboot 2
 autoreboot is ON
 autoreboot time is 2 hour(s)
```

Telnet Command: sys commit

This command allows users to save current settings to FLASH. Usually, current settings will be saved in SRAM. Yet, this command will save the file to FLASH.

Example

```
> sys commit
>
```

Telnet Command: sys tftpd

This command can turn on TFTP server for upgrading the firmware.

Example

```
> sys tftpd
% TFTP server enabled !!!
```

Telnet Command: sys cc

This command can display current country code and wireless region of this device.

Example

```
> sys cc
Country Code       : 0x 0 [International]
Wireless Region Code: 0x30
>
```

Telnet Command: sys version

This command can display current version for the system.

Example

```
> sys version
Router Model: Vigor122   Version: 3.2.10_RC1 English
Profile version: 3.0.0   Status: 1 (0x273d3001)
Router IP: 192.168.1.1   Netmask: 255.255.255.0
Firmware Build Date/Time: Apr 28 2016 05:33:14
Revision: 56444 v120
ADSL Firmware Version: 321311_A  Annex A
```

Telnet Command: sys qrybuf

This command can display the system memory status and leakage list.

Example

```
> > sys qrybuf
System Memory Status and Leakage List

# of free L-Buffer=154, total=448, port num:0
# of free M-Buffer=32, total=32
# of sk head queue buffer=139
# of sk freelink queue buffer=293

FLOWTRACK Memory Status
# of free = 5500
# of maximum = 0
# of flowstate = 5500
# of lost by siganture = 0
# of lost by list = 0
```

Telnet Command: sys pollbuf

This command can turn on or turn off polling buffer for the modem.

Syntax

sys pollbuf *[on]*

sys pollbuf *[off]*

Syntax Description

Parameter	Description
on	It means to turn on pulling buffer.
off	It means to turn off pulling buffer.

Example

```
> sys pollbuf on
% Buffer polling is on!

> sys pollbuf off
% Buffer polling is off!
```

Telnet Command: sys tr069

This command can set CPE settings for applying in VigorACS.

Syntax

sys tr069 get *[parm] [option]*

sys tr069 set *[parm] [value]*

sys tr069 save

Syntax Description

Parameter	Description
get [parm] [option]	It means to get parameters for tr-069. option=<nextlevel>: only gets nextlevel for GetParameterNames.
set [parm] [value]	It means to set parameters for tr-069.
save	It means to save the parameters to the flash memory of the modem.

Example

Telnet Command: sys sip_log

This command is used for enable/disable SIP ALG.

Syntax

sys sip_log *[value]*

Parameter	Description
[value]	0 – Disable SIP ALG. 1 – Enable SIP ALG.

Example

```
> sys sip_alg 1
>
```

Telnet Command: show lan1/lan2

This command displays current status of LAN IP address settings.

Example

```
> show lan1
%% 1st subnet settings:
%%     IP address: 192.168.1.1
%%     Subnet mask: 255.255.255.0
%%     RIP : [1st Subnet]
> show lan2
%% 2nd subnet settings:
%%     Status: [Inactive]
%%     IP address: 192.168.2.1
%%     Subnet mask: 255.255.255.0
%%     RIP : [1st Subnet]
```

Telnet Command: show dhcp

This command displays current status of DHCP server.

Example

```
> show dhcp
%% DHCP settings:
%%     Status: [Active]
%%     Start IP address for offering: 192.168.1.100
%%     Maximus offer IP address count: 50
%%     Default gateway: 192.168.1.1

%%     DHCP Relay: [Inactive]
```

Telnet Command: show dmz

This command displays current status of DMZ host.

Example

```
> show dmz
%%     DMZ mapping status:
 Index  Status  WAN aux IP     Private IP
-------------------------------------------
   1    Disable 172.16.3.221
   2    Disable 192.168.1.65
```

Telnet Command: show dns

This command displays current status of DNS setting.

Example

```
> show dns
%%     Domain name server settings:
%            Primary DNS: [Not set]
%            Secondary DNS: [Not set]
```

Telnet Command: show openport

This command displays current status of open port setting.

Example

```
> show openport
%%     Openport settings:
Index   Status  Comment        Local IP Address
*****************************************************
  1.    Enable  for_marketing   192.168.1.99
Total 1 items listed.
```

Telnet Command: show nat

This command displays current status of NAT.

Example

```
> show nat
NAT Port Redirection Running Table:

Index  Protocol  Public Port   Private IP      Private Port
 1          0          0   0.0.0.0                  0
 2          0          0   0.0.0.0                  0
 3          0          0   0.0.0.0                  0
 4          0          0   0.0.0.0                  0
 5          0          0   0.0.0.0                  0
 6          0          0   0.0.0.0                  0
 7          0          0   0.0.0.0                  0
 8          0          0   0.0.0.0                  0
 9          0          0   0.0.0.0                  0
10          0          0   0.0.0.0                  0
11          0          0   0.0.0.0                  0
12          0          0   0.0.0.0                  0
13          0          0   0.0.0.0                  0
14          0          0   0.0.0.0                  0
15          0          0   0.0.0.0                  0
16          0          0   0.0.0.0                  0
17          0          0   0.0.0.0                  0
18          0          0   0.0.0.0                  0
19          0          0   0.0.0.0                  0
20          0          0   0.0.0.0                  0
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
```

Telnet Command: show session

This command displays current status of current session.

Example

```
> show session
% Maximum Session Number: 5000
% Maximum Session Usage: 0
% Current Session Usage: 0
```

Telnet Command: show status

This command displays current status of LAN and WAN connections.

Example

```
> show status
System Uptime:64:25:1
LAN Status
Primary DNS:194.109.6.66     Secondary DNS:168.95.1.1
IP Address:192.168.1.1       Tx Rate:38805    Rx Rate:1139

WAN 1 Status:Disconnected
```

```
Enable:Yes      Line:ADSL       Name:tcom
Mode:PPPoA      Up Time:0:00:00    IP:---          GW IP:---
TX Packets:0         TX Rate:0   RX Packets:0         RX Rate:0
Message [PPP Shutdown]

WAN 2 Status:Disconnected
Enable:Yes      Line:ADSL       Name:
Mode:---        Up Time:0:00:00    IP:---          GW IP:---
TX Packets:0         TX Rate:0   RX Packets:0         RX Rate:0

ADSL Information:     ADSL Firmware Version:321311_A
Mode:-----           State:READY     TX Block:0    RX Block:0
Corrected Blocks:0    Uncorrected Blocks:0
UP Speed:0         Down Speed:0         SNR Margin:0   Loop Att.:0
```

Telnet Command: show adsl

This command displays current status of ADSL.

Example

```
> show adsl
  -------------------------- ATU-R Info (hw: annex A, f/w: annex A) -----------
   Running Mode          :   T1.413      State              : TRAINING
   DS Actual Rate        :       0 bps   US Actual Rate     :       0 bps
   DS Attainable Rate    :       0 bps   US Attainable Rate :       0 bps
   DS Path Mode          :       Fast    US Path Mode       :       Fast
   DS Interleave Depth   :       0       US Interleave Depth :       0
   NE Current Attenuation :       0 dB    Cur SNR Margin     :       0  dB
   DS actual PSD         :    0. 0 dB    US actual PSD      :    0. 0   dB
   ADSL Firmware Version   : 05-04-04-04-00-01
  ------------------------------ ATU-C Info --------------------------------
   Far Current Attenuation :       0 dB    Far SNR Margin     :       0  dB
   CO ITU Version[0]      : 00000000      CO ITU Version[1]   : 00000000
   DSLAM CHIPSET VENDOR   : < ADI >
```

Telnet Command: mngt ftpport

This command allows users to set FTP port for management.

Syntax

mngt ftpport *[FTP port]*

Syntax Description

Parameter	Description
FTP port	It means to type the number for FTP port. The default setting is 21.

Example

```
> mngt ftpport 21
% Set FTP server port to 21 done.
```

Telnet Command: mngt httpport

This command allows users to set HTTP port for management.

Syntax

mngt httpport *[Http port]*

Syntax Description

Parameter	Description
Http port	It means to enter the number for HTTP port. The default setting is 80.

Example

```
> mngt httpport 80
% Set web server port to 80 done.
```

Telnet Command: mngt telnetport

This command allows users to set telnet port for management.

Syntax

mngt telnetport *[Telnet port]*

Syntax Description

Parameter	Description
Telnet port	It means to type the number for telnet port. The default setting is 23.

Example

```
> mngt telnetport 23
% Set Telnet server port to 23 done.
```

Telnet Command: mngt ftpserver

This command can enable/disable FTP server.

Syntax

mngt ftpserver *[enable]*

mngt ftpserver *[disable]*

Syntax Description

Parameter	Description
enable	It means to activate FTP server function.
disable	It means to inactivate FTP server function.

Example

```
> mngt ftpserver enable
%% FTP server has been enabled.
```

```
> mngt ftpserver disable
%% FTP server has been disabled.
```

Telnet Command: mngt noping

This command is used to pass or block Ping from LAN PC to the internet.

Syntax

mngt noping *[on]*

mngt noping *[off]*

mngt noping *[viewlog]*

mngt noping *[clearlog]*

Syntax Description

Parameter	Description
on	All PING packets will be forwarded from LAN PC to Internet.
off	All PING packets will be blocked from LAN PC to Internet.
viewlog	It means to display a log of ping action, including source MAC and source IP.
clearlog	It means to clear the log of ping action.

Example

```
> mngt noping off
No Ping Packet Out is OFF!!
```

Telnet Command: mngt defenseworm

This command can block specified port for passing through the modem.

Syntax

mngt defenseworm *[on]*

mngt defenseworm *[off]*

mngt defenseworm *[add port]*

mngt defenseworm *[del port]*

mngt defenseworm *[viewlog]*

mngt defenseworm *[clearlog]*

Syntax Description

Parameter	Description
on	It means to activate the function of defense worm packet out.
off	It means to inactivate the function of defense worm packet out.
add port	It means to add a new TCP port for block.
del port	It means to delete a TCP port for block.
viewlog	It means to display a log of defense worm packet, including source MAC and source IP.
clearlog	It means to remove the log of defense worm packet.

Example

```
> mngt defenseworm add 21
Add TCP port 21
Block TCP port list: 135, 137, 138, 139, 445, 21, 21
```

Telnet Command: mngt rmtcfg

This command can allow the system administrators to login from the Internet. By default, it is not allowed.

Syntax

mngt rmtcfg *[status]*

mngt rmtcfg *[enable]*

mngt rmtcfg *[disable]*

mngt rmtcfg *[http/https/ftp/telnet/ssh] [on/off]*

Syntax Description

Parameter	Description
status	It means to display current setting for your reference.
enable	It means to allow the system administrators to login from the Internet.
disable	It means to deny the system administrators to login from the Internet.
http/https/ftp/telnet/ssh/tr069	It means to specify one of the servers/protocols for enabling or disabling.

on/off	on – enable the function. off – disable the function.

Example

```
> mngt rmtcfg enable
%% Remote configure function has been enabled.

> mngt rmtcfg ftp on
%% FTP server has been enabled.
```

Telnet Command: mngt echoicmp

This command allows users to reject or accept PING packets from the Internet.

Syntax

mngt echoicmp *[enable]*

mngt echoicmp *[disable]*

Syntax Description

Parameter	Description
enable	It means to accept the echo ICMP packet.
disable	It means to drop the echo ICMP packet.

Example

```
> mngt echoicmp enable
%% Echo ICMP packet enabled.
```

Telnet Command: mngt accesslist

This command allows you to specify that the system administrator can login from a specific host or network. A maximum of three IPs/subnet masks is allowed.

Syntax

mngt accesslist *list*

mngt accesslist *add [index][ip addr][mask]*

mngt accesslist *remove [index]*

mngt accesslist *flush*

Syntax Description

Parameter	Description
list	It can display current setting for your reference.
add	It means adding a new entry.
index	It means to specify the number of the entry.
ip addr	It means to specify an IP address.
mask	It means to specify the subnet mask for the IP address.
remove	It means to delete the selected item.

flush	It means to remove all the settings in the access list.

Example

```
> mngt accesslist add 1 192.168.1.89 255.255.255.0
%% Set OK.
> mngt accesslist list
%% Access list :
  Index IP address     Subnet mask
========================================
  1    192.168.1.89    255.255.255.0
```

Telnet Command: wan ppp_mss

This command allows users to adjust the size of MTU for WAN interface.

Syntax

wan ppp_mss <*Value*>

Syntax Description

Parameter	Description
<*Value*>	It means the number of MTU for PPP. The available range is from 1000 to 1500.

Example

```
> wan ppp_mss 1450
> wan ppp_mss
% wan ppp_mss <MSS size: 1000 ~ 1500>

> wan ppp_mss ?
% wan ppp_mss <MSS size: 1000 ~ 1500>
% Now: 1450
```

Telnet Command: wan DF_check

This command allows you to enable or disable the function of DF (Don't fragment)

Syntax

wan DF_check *[on]*

wan DF_check *[off]*

Syntax Description

Parameter	Description
on/off	It means to enable or disable DF.

Example

```
> wan DF_check on
%DF bit check enable!
```

Telnet Command: wan disable

This command allows you to disable WAN connection.

Example

```
> wan disable WAN
%WAN disabled.
```

Telnet Command: wan forward

This command allows you to enable or disable the function of WAN forwarding. The packets are allowed to be transmitted between different WANs.

Syntax

wan forward *[on]*

wan forward *[off]*

Syntax Description

Parameter	Description
on/off	It means to enable or disable WAN forward.

Example

```
> wan forward ?
%WAN forwarding is Disable!

> wan forward on
%WAN forwarding is enable!
```

Telnet Command: wan detect

This command allows you to Ping a specified IP to detect the WAN connection (static IP or PPPoE mode).

Syntax

wan detect *[wan1/wan2][on/off/always_on]*

wan detect *[wan1/wan2]***target** *[ip addr]*

wan detect *[wan1/wan2]***ttl** *[1-255]*

wan detect status

Syntax Description

Parameter	Description
on	It means to enable ping detection. The IP address of the target shall be set.
off	It means to enable ARP detection (default).
always_on	disable link detect, always connected(only support static IP)
target	It means to set the ping target.
ip addr	It means the IP address used for detection. Type an IP address in this field.
ttl	It means to set the ping TTL value (work as trace route) If you do not set any value for ttl here or just type 0 here, the

	system will use default setting (255) as the ttl value.
status	It means to show the current status.

Example

```
> wan detect status
 WAN1: off
 WAN2: off
> wan detect wan1 target 192.168.1.78
 Set OK

> wan detect wan1 on
 Set OK

> wan detect status
 WAN1: on, Target=192.168.1.78, TTL=255
 WAN2: off
>
```

Telnet Command: adsl status

This command is used to display current status of ADSL setting.

Syntax

adsl status

Example

```
> adsl status
  ------------------------- ATU-R Info (hw: annex A, f/w: annex A) -----------
   DSL Modulation         : T1.413
   State                :    READY
   DS Actual Rate         :       0 bps   US Actual Rate      :       0 bps
   DS Attainable Rate     :       0 bps   US Attainable Rate   :       0 bps
   DS Path Mode          :       Fast    US Path Mode        :       Fast
   DS Interleave Depth    :       0      US Interleave Depth  :       0
   NE Current Attenuation  :       0 dB    Cur SNR Margin      :       0  dB
   DS actual PSD         :    0. 0 dB    US actual PSD       :    0. 0   dB
   ADSL Firmware Version   : 321311_A
  ------------------------------- ATU-C Info
--------------------------------
   Far Current Attenuation :       0 dB    Far SNR Margin      :       0  dB
   CO ITU Version[0]      : 00000000      CO ITU Version[1]    : 00000000
   DSLAM CHIPSET VENDOR    : < ADI >
>
```

Telnet Command: adsl ppp

This command can set the Internet Access mode for the router.

Syntax

adsl ppp *[? | pvc_no vci vpi Encap Proto modu acqIP idle [Username Password]*

Syntax Description

Parameter	Description

?	Display the command syntax of “adsl ppp”.
pvc_no	It means the PVC number and the adjustable range is from 0 (Channel-1) to 3(Channel-4).
Encap	Different numbers represent different modes. 0 : VC_MUX, 1: LLC/SNAP, 2: LLC_Bridge, 3: LLC_Route, 4: VCMUX_Bridge 5: VCMUX_Route, 6: IPoE.
Proto	It means the protocol used to connect Internet. Different numbers represent different protocols. 0: PPPoA, 1: PPPoE, 2: MPoA.
Modu	0: T1.413, 2: G.dmt, 4: Multi, 5: ADSL2, 7:ADSL2_AnnexM 8:ADSL2+ 14:ADSL2+_AnnexM.
acqIP	It means the way to acquire IP address. Type the number to determine the IP address by specifying or assigned dynamically by DHCP server. 0 : fix_ip, 1: dhcp_client/PPPoE/PPPoA.(acquire IP method)
idle	Type number to determine the network connection will be kept for always or idle after a certain time. -1: always on, else idle timeout secs. Only for PPPoE/PPPoA.
Username	This parameter is used only for PPPoE/PPPoA.
Password	This parameter is used only for PPPoE/PPPoA.

You have to reboot the system when you set it on Route mode.

Example

```
> adsl ppp o 35 8 1 1 4 1 -1 draytek draytek
pvc no.=0
vci=35
vpi=8
encap=LLC(1)
proto=PPPoE(1)
modu=MULTI(4)
AcquireIP: Dhcp_client(1)
```

```
Idle timeout:-1
Username=draytek
Password=draytek
```

Telnet Command: adsl idle

This command can make the router accessing into the idle status. If you want to invoke the router again, you have to reboot the router by using “reboot” command.

Example

```
> adsl idle
%ADSL Enter IDLE Mode!
% Use 'adsl reboot' to restart dsl to normal mode.
```

Telnet Command: adsl drivermode

This command is useful for laboratory to measure largest power of data transmission. Please follow the steps below to set adsl drivermode.

1. Please connect dsl line to the DSLAM.
2. Waiting for dsl SHOWTIME.
3. Drop the dsl line.
4. Now, it is on continuous sending mode, and adsl2/2+ led is always ON.
5. Use 'adsl reboot' to restart dsl to normal mode.

Telnet Command: adsl reboot

This command can wake up the idle router.

Example

```
> adsl reboot
% Adsl is Rebooting...
```

Telnet Command: adsl oamlb

This command is used to test if the connection between CPE and CO is OK or not.

adsl oamlb *[n][type]*

adsl oamlb chklink *[on/off]*

adsl oamlb *[log_on/log_off]*

Syntax Description

Parameter	Description
n	It means the total number of transmitted packets.
type	It means the protocol that you can use. 1 – for F4 Seg-to-Seg (VP level) 2 – for F4 End-to-End (VP level) 4 – for F5 Seg-to-Seg (VC level) 5 – for F5 End-to-End (VC level)
chklink	Check the DSL connection.
Log_on/log_off	Enable or disable the OAM log for debug.

Example

```
> adsl oamlb chklink on
 OAM checking dsl link is ON.
> adsl oamlb F5 4
Tx cnt=0
Rx Cnt=0
>
```

Telnet Command: adsl vcilimit

This command can cancel the limit for vci value.

Some ISP might set the vci value under 32. In such case, we can cancel such limit manually by using this command. Do not set the number greater than 254.

adsl vcilimit *[n]*

Syntax Description

Parameter	Description
n	The number shall be between 1 ~ 254.

Example

```
> adsl vcilimit 33
change VCI limitation from 32 to 33.
```

Telnet Command: adsl automode

This command is used to add or remove ADSL modes (such as ANNEXL, ANNEXM and ANNEXJ) supported by Multimode.

adsl automode *[add|remove|set|default|show] [adsl_mode]*

Syntax Description

Parameter	Description

add	Add ADSL mode.
remove	Remove ADSL mode.
set	Use default settings plus the new added ADSL mode.
default	Use default settings.
show	Display current setting.
adsl_mode	There are three modes to be choose, ANNEXL, ANNEXM and ANNEXJ. T1413, GDMT, GLITE, ADSL2, ADSL2+, ANNEXL are enabled on default.

Example

```
> adsl automode set ANNEXJ
 Automode supported :  T1.413, G.DMT, G.LITE, ADSL2, ADSL2+, ANNEXJ,
```

Telnet Command: adsl annex

This command can display the annex interface of this router.

Example

```
> adsl annex
% hardware is annex A.
% modem code is annex A
```

Telnet Command: adsl showbins

This command can display the allocation for each Bin (Tone) SNR, Gain, and Bits.

Syntax

adsl showbins *[startbin endbin |up]*

Syntax Description

Parameter	Description
startbin	The number is between 0 ~ 517.
endbin	The number is between 4 ~ 511.
up	Show upstream information.

Example

```
> adsl showbins 2 30
DOWNSTREAM :
--------------------------------------------------------------------------------
Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi
     dB  .1dB ts        dB  .1dB ts        dB  .1dB ts        dB  .1dB ts
--- ----- ---- -- - --- ----- ---- -- - --- ----- ---- -- - --- ----- ---- --
--- ----- ---- -- - --- ----- ---- -- - --- ----- ---- -- - --- ----- ---- --
Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi - Bin  SNR  Gain Bi
     dB  .1dB ts        dB  .1dB ts        dB  .1dB ts        dB  .1dB ts
>
```

Telnet Command: adsl savecfg

This command can save the configuration into FLASH with a file format of cfg.

Example

```
> adsl savecfg
% Xdsl Cfg Save OK!
```

Telnet Command: adsl vendorid

This command allows you to configure user-defined CPE vendor ID.

adsl vendorid *[status/on/off/ set vid0 vid1]*

Syntax Description

Parameter	Description
status	Display current status of user-defined vendor ID.
on	Enable the user-defined function.
off	Disable the user-defined function.
set vid0 vid1	It means to set user-defined vendor ID with vid0 and vid1. The vendor ID shall be set with HEX format, ex: 00fe7244: 79612f21.

Example

```
> adsl vendorid status
% User define CPE Vendor ID is OFF
% vid0:vid1 = 0x00fe7244:79612f21
> adsl vendorid on set vid0 vid1
% User define CPE Vendor ID is ON
```

Telnet Command: adsl atm

This command can set QoS parameter for ATM.

adsl atm *pcr [pvc_no][PCR][max][status]*

adsl atm *scr [pvc_no][SCR][status]*

adsl atm *mbs [pvc_no][MBS][status]*

adsl atm *status*

Syntax Description

Parameter	Description
pvc_no	It means *pvc* number and must be between 0(Channel 1) to 7(Channel 8).
PCR	It means Peak Cell Rate for upstream. The range for the number is “1” to “2539”.
max	Get the highest speed for the upstream.
SCR	Mean Sustainable Cell Rate. The range for the number is “1” to “2539”.
MBS	Maximum Burst Size. The range for the number is “1” to “2539”.
status	Display PCR/SCR/MBS setting.

Example

```
> adsl atm pcr 1 200 max
% PCR is 0 for pvc 1.
> adsl atm pcr status
  pvc   channel       PCR
 ---------------------------
   0      1          0
   1      2          0
   2      3          0
   3      4          0
```

Telnet Command: wol

This command allows Administrator to set the white list of WAN IP addresses/Subnets, that the magic packet from these IP addresses/Subnets will be eligible to pass through NAT and wake up the LAN client. You also need to set NAT rule for LAN client.

Syntax

wol up *[MAC Address]/[IP Address]*

Syntax Description

Parameter	Description
MAC Address	It means the MAC address of the host.
IP address	It means the LAN IP address of the host. If you want to wake up LAN host by using IP address, be sure that that IP address has been bound with the MAC address (IP BindMAC).

Example

```
> wol fromWan on
> wol fromWan_Setting 1 192.168.1.45 255.255.255.0
>
```

Telnet Command: vigbrg on

This command can make the modem to be regarded as a modem but not a router.

Example

```
> vigbrg on
%Enable Vigor Bridge Function!
```

Telnet Command: vigbrg off

This command can disable vigor bridge function.

Example

```
> vigbrg off
%Disable Vigor Bridge Function!
```

Telnet Command: vigbrg status

This command can show whether the Vigor Bridge Function is enabled or disabled.

Example

```
> vigbrg status
%Vigor Bridge Function is enable!

%Wan1 management is disable!
```

Telnet Command: vigbrg cfgip

This command allows users to transfer a bridge modem into ADSL router by accessing into and adjusting specified IP address. Users can access into Web UI of the modem to manage the modem through the IP address configured here.

Syntax

vigbrg cfgip *[IP Address]*

Syntax Description

Parameter	Description
IP Address	It means to type an IP address for users to manage the modem.

Example

```
> vigbrg cfgip 192.168.1.15
> vigbrg cfgip ?
% Vigor Bridge Config IP,
% Now: 192.168.1.15
```

Telnet Command: vigbrg wan1on

This command is used to enable the bridge WAN1 management.

Example

```
> vigbrg wan1on
%Enable Vigor Bridge Wan1 management!
```

Telnet Command: vigbrg wan1off

This command is used to disable the bridge WAN1 management.

Example

```
> vigbrg wan1off

%Disable Vigor Bridge Wan1 management!
```

Telnet Command: tsmail

This command is used to display current settings for sending test mail.

Example

```
> testmail
Send out test mail
```