

DrayTek

Vigor130

VDSL2/ADSL2/2+ Modem



Your reliable networking solutions partner

User's Guide

V1.0

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

Version: 1.0

Firmware version: V3.7.1

(For future update, please visit DrayTek web site)

Date: 5/06/2013

Copyright Information

Copyright Declarations

Copyright 2013 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

Trademarks

The following trademarks are used in this document:

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

Safety Instructions and Approval

Safety Instructions

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

Warranty

We warrant to the original end user (purchaser) that the modem will be free from any defects in workmanship or materials for a period of one (1) year from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary to restore the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Be a Registered Owner

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

Firmware & Tools Updates

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

<http://www.draytek.com>

European Community Declarations

Manufacturer: DrayTek Corp.
Address: No. 26, Fu Shing Road, HuKou Township, HsinChu Industrial Park, Hsin-Chu, Taiwan 303
Product: Vigor130

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

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

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

Federal Communication Commission Interference Statement

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

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

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

- (1) This device may not cause harmful interference, and
- (2) This device may accept any interference received, including interference that may cause undesired operation.

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



Table of Contents

1

Introduction1

- 1.1 Web Configuration Buttons Explanation 1
- 1.2 LED Indicators and Connectors 2
- 1.3 Hardware Installation 4

2

Basic Configuration5

- 2.1 Accessing Web Page 5
- 2.2 Changing Password 6
- 2.3 Quick Start Wizard 7
 - 2.3.1 Setting PPPoE/PPPoA Connection 7
 - 2.3.2 Setting MPoA/Static or Dynamic Connection 10
- 2.4 Introducing Dashboard 13
 - 2.4.1 Virtual Panel 13
 - 2.4.2 Name with a Link 14
 - 2.4.3 Quick Access for Common Used Menu 14
 - 2.4.4 GUI Map 15
 - 2.4.5 Web Console 15
 - 2.4.6 Config Backup 16
- 2.5 Online Status 17
 - 2.5.1 Physical Connection 17
 - 2.5.2 Virtual WAN 19
- 2.6 Saving Configuration 20
- 2.7 Registering Vigor Router 20

3

Advanced Configuration23

- 3.1 Internet Access 23
 - 3.1.1 Basics of Internet Protocol (IP) Network 23
 - 3.1.2 General Setup 24
 - 3.1.3 PPPoE/PPPoA 26
 - 3.1.4 MPoA /Static or dynamic IP 28
 - 3.1.5 IPv6 31
 - 3.1.6 Multi-PVCs 36
 - 3.1.7 Multi-VLAN 40
- 3.2 LAN 42
 - 3.2.1 Basics of LAN 42
 - 3.2.2 General Setup 44
 - 3.2.3 Static Route 49

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

4

Application and Examples.....132

4.1 LAN – Created by Using NAT	132
--------------------------------------	-----

5

Trouble Shooting.....135

5.1 Checking If the Hardware Status Is OK or Not.....	135
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	136
5.3 Pinging the Modem from Your Computer.....	138
5.4 Checking If the ISP Settings are OK or Not.....	139
5.5 Backing to Factory Default Setting If Necessary	139
5.6 Contacting Your Dealer	140

1


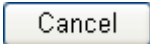
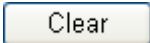
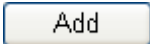

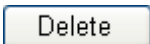
Introduction

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

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

1.1 Web Configuration Buttons Explanation

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

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

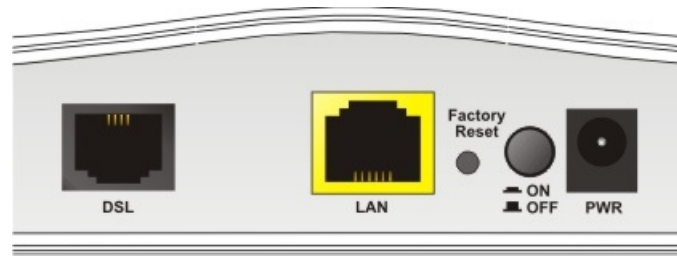
Note: For the other buttons shown on the web pages, please refer to Chapter 4 for detailed explanation.



1.2 LED Indicators and Connectors

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



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



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

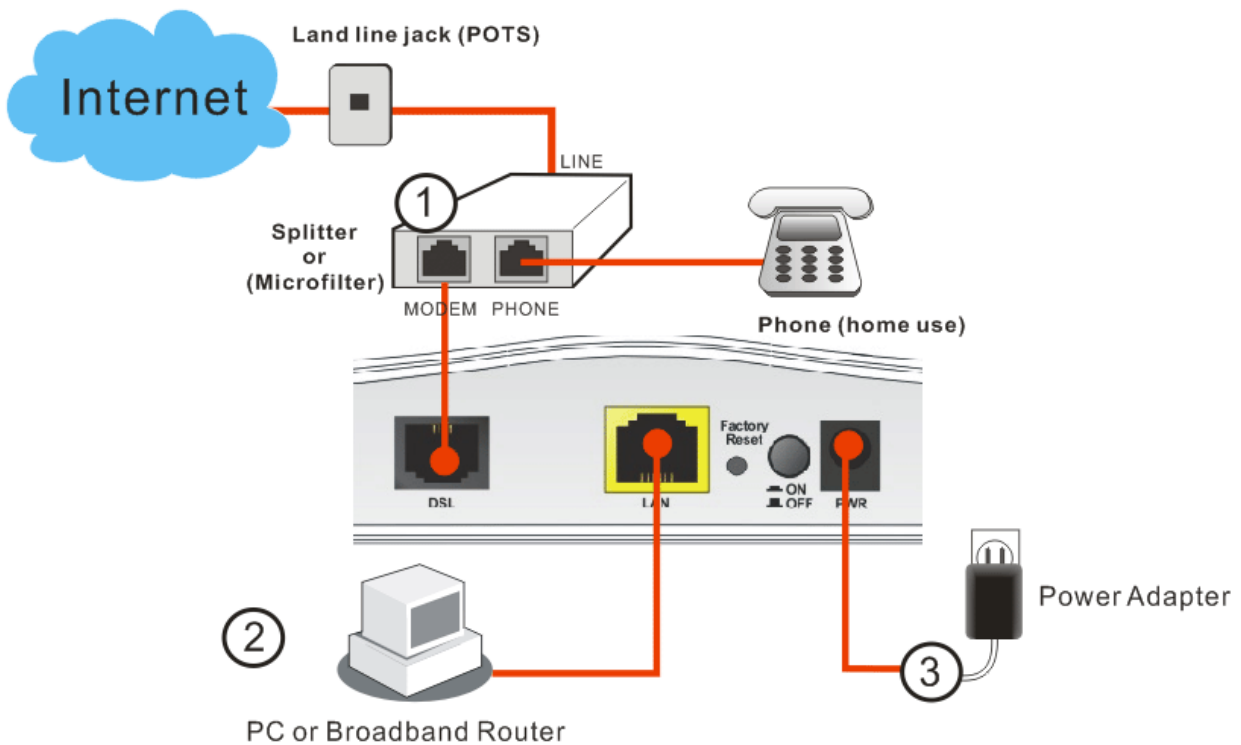
1.3 Hardware Installation

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

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

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

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



2

Basic Configuration

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

2.1 Accessing Web Page

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



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

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

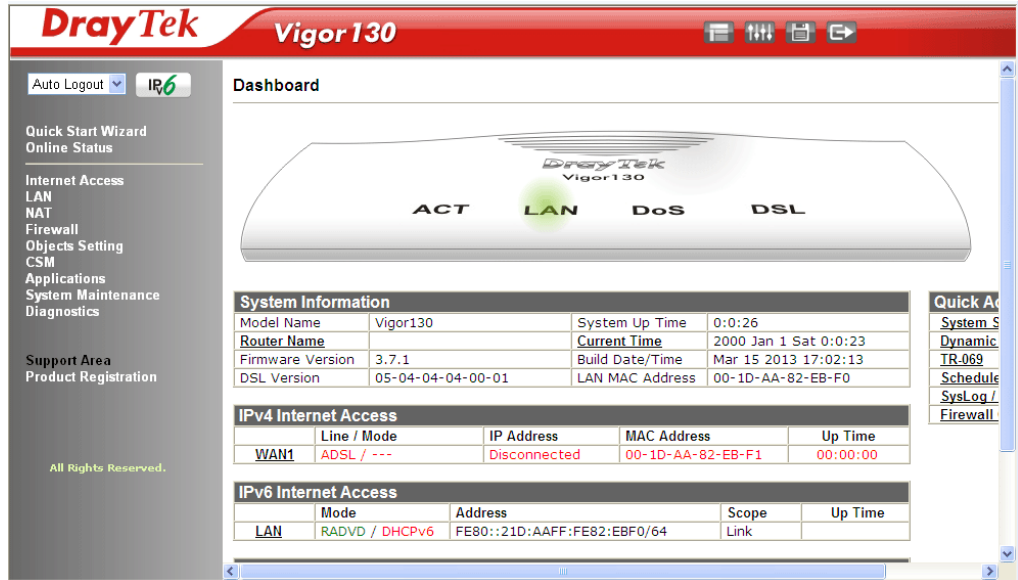


Notice: If you fail to access to the web configuration, please go to “Trouble Shooting” for detecting and solving your problem.

2.2 Changing Password

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

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



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

System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	<input type="text"/>
New Password	<input type="text"/>
Confirm Password	<input type="text"/>

Note: Password can contain only a-z A-Z 0-9 , ; . " < > * + = \ | ? @ # ^ ! ()

OK

3. Enter the login password (the default is blank) on the field of **Old Password**. Type **New Password**. Then click **OK** to continue.
4. Now, the password has been changed. Next time, use the new password to access the Web User Interface for this modem.



2.3 Quick Start Wizard



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

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

2.3.1 Setting PPPoE/PPPoA Connection

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

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

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

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

Quick Start Wizard

Enter login password

Please enter an alpha-numeric string as your **Password** (Max 23 characters).

Old Password

New Password

Confirm Password

< Back

Next >

Finish

Cancel

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

Quick Start Wizard

Connect to Internet

Protocol	PPPoE / PPPoA
For ADSL Only:	MPoA / Static or Dynamic IP
Encapsulation	PPPoA VC MUX
VPI	8 <input type="button" value="Auto detect"/>
VCI	35
Fixed IP	<input type="radio"/> Yes <input checked="" type="radio"/> No(Dynamic IP)
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Default Gateway	<input type="text"/>
Primary DNS	8.8.8.8
Second DNS	8.8.4.4

Available parameters are listed below:

Item	Description
For ADSL Only	You have to select an appropriate WAN connection type for connecting to the Internet through this modem according to the settings that your ISP provided. Auto detect – Click it to detect suitable values below by the modem automatically.
Encapsulation	Select an IP mode for this WAN interface. There are several available modes for Internet access such as PPPoE , PPPoA .
VPI	Stands for Virtual Path Identifier . It is an 8-bit header inside each ATM cell that indicates where the cell should be routed. The ATM, is a method of sending data in small packets of fixed sizes. It is used for transferring data to client computers.
VCI	Stands for Virtual Channel Identifier . It is a 16-bit field inside ATM cell's header that indicates the cell's next destination as it travels through the network. A virtual channel is a logical connection between two end devices on the network.
Fixed IP	Click Yes to specify a fixed IP for the modem. Otherwise, click No (Dynamic IP) to allow the modem choosing a dynamic IP. If you choose No , the following IP Address, Subnet Mask and Default Gateway will not be changed.
IP Address	Assign an IP address for the protocol that you select.
Subnet Mask	Assign a subnet mask value for the protocol of

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

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

Quick Start Wizard

Set PPPoE / PPPoA

User Name	<input type="text" value="carrie"/>
Password	<input type="password" value="••••"/>
Confirm Password	<input type="password" value="•••"/>

Available parameters are listed below:

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

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

Quick Start Wizard

Please confirm your settings:

VPI:	8
VCI:	35
Protocol / Encapsulation:	PPPoA / VCMUX
Fixed IP:	No
Primary DNS:	8.8.8.8
Secondary DNS:	8.8.4.4

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

Quick Start Wizard

Quick Start Wizard Setup OK!

2.3.2 Setting MPoA/Static or Dynamic Connection

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

Quick Start Wizard

Enter login password

Please enter an alpha-numeric string as your **Password** (Max 23 characters).

Old Password	<input type="password" value="•••••"/>
New Password	<input type="password" value="••••"/>
Confirm Password	<input type="password" value="••••"/>

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

Quick Start Wizard

Connect to Internet

Protocol MPoA / Static or Dynamic IP

For ADSL Only:

Encapsulation 1483 Bridged IP LLC

VPI 8 Auto detect

VCI 35

Fixed IP Yes No(Dynamic IP)

IP Address

Subnet Mask

Default Gateway

Primary DNS 8.8.8.8

Second DNS 8.8.4.4

< Back Next > Finish Cancel

Available parameters are listed below:

Item	Description
For ADSL Only	You have to select an appropriate WAN connection type for connecting to the Internet through this modem according to the settings that your ISP provided. Auto detect – Click it to detect suitable values below by the modem automatically.
Encapsulation	Select an IP mode for this WAN interface. There are several available modes for Internet access such as PPPoE , PPPoA .
VPI	Stands for Virtual Path Identifier . It is an 8-bit header inside each ATM cell that indicates where the cell should be routed. The ATM, is a method of sending data in small packets of fixed sizes. It is used for transferring data to client computers.
VCI	Stands for Virtual Channel Identifier . It is a 16-bit field inside ATM cell's header that indicates the cell's next destination as it travels through the network. A virtual channel is a logical connection between two end devices on the network.
Fixed IP	Click Yes to specify a fixed IP for the modem. Otherwise, click No (Dynamic IP) to allow the modem choosing a dynamic IP. If you choose No , the following IP Address, Subnet Mask and Default Gateway will not be changed.
IP Address	Assign an IP address for the protocol that you select.
Subnet Mask	Assign a subnet mask value for the protocol of

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

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

Quick Start Wizard

Please confirm your settings:

VPI:	8
VCI:	35
Protocol / Encapsulation:	1483 Bridge LLC
Fixed IP:	No
Primary DNS:	8.8.8.8
Secondary DNS:	8.8.4.4

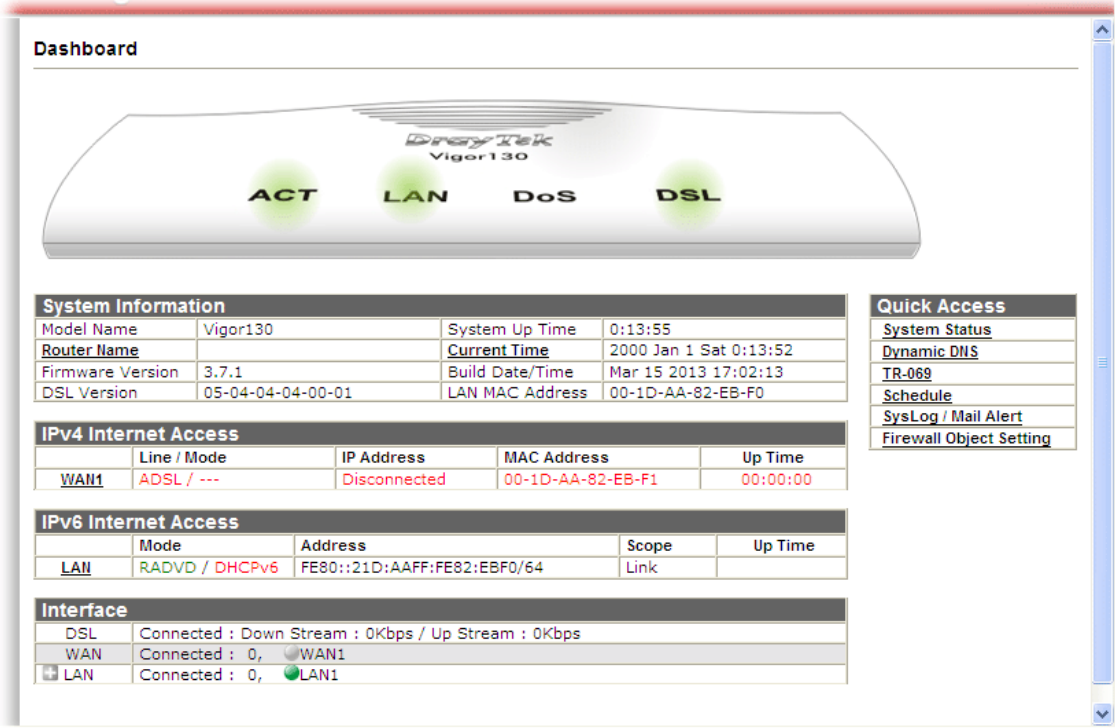
- Click **Finish**. The Quick Start Wizard Setup OK page will be displayed.

Quick Start Wizard

Quick Start Wizard Setup OK!

2.4 Introducing Dashboard

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



The screenshot shows the DrayTek Vigor130 Dashboard. At the top, there is a virtual panel of the modem with four LEDs labeled ACT, LAN, DoS, and DSL, all of which are illuminated in green. Below this panel are several sections:

- System Information:**

Model Name	Vigor130	System Up Time	0:13:55
Router Name		Current Time	2000 Jan 1 Sat 0:13:52
Firmware Version	3.7.1	Build Date/Time	Mar 15 2013 17:02:13
DSL Version	05-04-04-04-00-01	LAN MAC Address	00-1D-AA-82-EB-F0
- Quick Access:**
 - System Status
 - Dynamic DNS
 - TR-069
 - Schedule
 - SysLog / Mail Alert
 - Firewall Object Setting
- IPv4 Internet Access:**

	Line / Mode	IP Address	MAC Address	Up Time
WAN1	ADSL / ---	Disconnected	00-1D-AA-82-EB-F1	00:00:00
- IPv6 Internet Access:**

	Mode	Address	Scope	Up Time
LAN1	RADVD / DHCPv6	FE80::21D:AAFF:FE82:EBF0/64	Link	
- Interface:**

DSL	Connected : Down Stream : 0Kbps / Up Stream : 0Kbps
WAN	Connected : 0, WAN1
LAN	Connected : 0, LAN1

2.4.1 Virtual Panel

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



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

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

2.4.2 Name with a Link

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

System Information			
Model Name	Vigor130	System Up Time	0:13:55
Router Name		Current Time	2000 Jan 1 Sat 0:13:52
Firmware Version	3.7.1	Build Date/Time	Mar 15 2013 17:02:13
DSL Version	05-04-04-04-00-01	LAN MAC Address	00-1D-AA-82-EB-F0

IPv4 Internet Access				
	Line / Mode	IP Address	MAC Address	Up Time
WAN1	ADSL / ---	Disconnected	00-1D-AA-82-EB-F1	00:00:00

IPv6 Internet Access				
	Mode	Address	Scope	Up Time
LAN	RADVD / DHCPv6	FE80::21D:AAFF:FE82:EBF0/64	Link	

2.4.3 Quick Access for Common Used Menu

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

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

Quick Access
System Status
Dynamic DNS
TR-069
Schedule
SysLog / Mail Alert
Firewall Object Setting

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

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

Interface	
DSL	Connected : Down Stream : 0Kbps / Up Stream : 0Kbps
WAN	Connected : 0, WAN1
LAN	Connected : 1, LAN1

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

Interface			
DSL	Connected : Down Stream : 0Kbps / Up Stream : 0Kbps		
WAN	Connected : 0, WAN1		
LAN	Connected : 1, LAN1		
	Host ID	IP Address	MAC
	CARRIE-0C7CB251	192.168.1.10	E0-CB-4E-DA-48-79

2.4.4 GUI Map



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

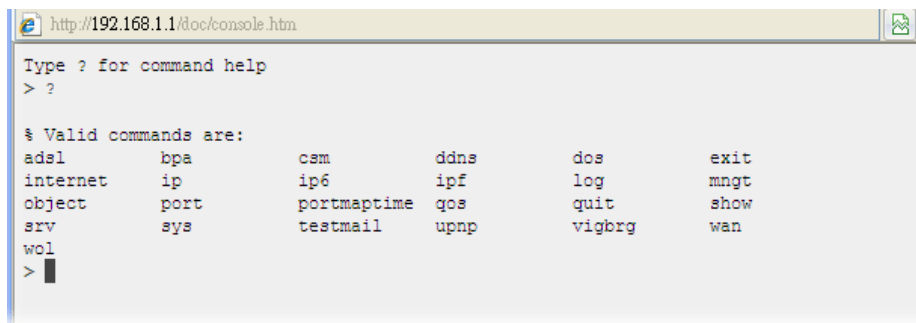
GUI Map			
Wizard	Quick Start Wizard	Applications	Dynamic DNS
Online Status	Physical Connection		Schedule
	Virtual WAN		UPnP
Internet Access	General Setup	System Maintenance	IGMP
	PPPoE/PPPoA		System Status
	MPoA / Static or dynamic IP		TR-069
	IPv6		Administrator Password
	Multi-PVCs		Configuration Backup
	Multi-VLAN		SysLog / Mail Alert
LAN	General Setup		Time and Date Management
	Static Route		Reboot System
	Bind IP to MAC	Diagnostics	Firmware Upgrade
NAT	Port Redirection		Dial-out Triggering
	DMZ Host		Routing Table
	Open Ports		ARP Cache Table
Firewall	General Setup		IPv6 Neighbour Table
	Filter Setup		DHCP Table
	DoS Defense		NAT Sessions Table
Objects Setting	IP Object		Ping Diagnosis
	IP Group		Data Flow Monitor
	IPv6 Object		Trace Route
	IPv6 Group		IPv6 TSPC Status
	Service Type Object		
	Service Type Group		
	Keyword Object		
	Keyword Group		
	File Extension Object		
CSM	URL Content Filter Profile		

2.4.5 Web Console



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

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

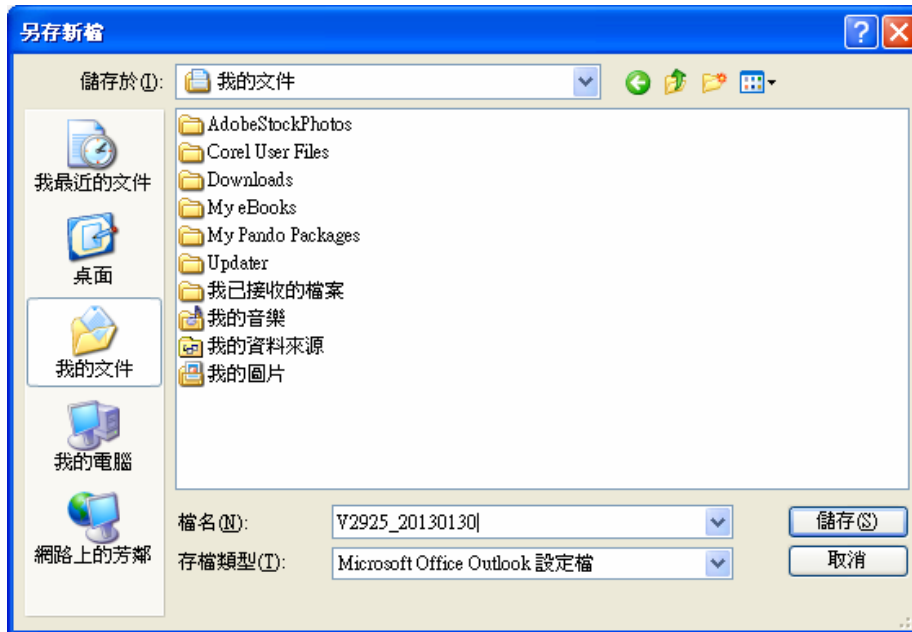


2.4.6 Config Backup



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

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



Click **Save** to store the setting.

2.4.7 Logout



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

2.5 Online Status



2.5.1 Physical Connection

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

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

Physical Connection for IPv4 Protocol

Online Status

Physical Connection				System Uptime: 0:2:57		
IPv4		IPv6				
LAN Status		Primary DNS: 8.8.8.8		Secondary DNS: 8.8.4.4		
IP Address	TX Packets	RX Packets				
192.168.1.1	0	1851				
WAN Status						>> Renew
Enable	Line	Name	Mode	Up Time		
Yes	ADSL		DHCP Client	00:00:00		
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
---	---	0	0	0	0	
ADSL Information (ADSL Firmware Version: 05-04-04-04-00-01)						
ATM Statistics	TX Cells	RX Cells	TX CRC errs	RX CRC errs		
	0	0	0	0		
ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
		TRAINING	0	0	0	0

Detailed explanation is shown below:

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

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

Physical Connection for IPv6 Protocol

Online Status

Physical Connection		System Uptime: 0:6:50	
IPv4		IPv6	
LAN Status			
IP Address			
FE80::21D:AAFF:FE82:EBF0/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
5	0	390	0
WAN IPv6 Status			
Enable	Mode	Up Time	
No	Offline	---	
IP			Gateway IP
---			---

Detailed explanation (for IPv6) is shown below:

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

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

2.5.2 Virtual WAN

Such page displays the virtual WAN connection information.

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

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

Online Status

Virtual WAN						System Uptime: 0:4:36
WAN 3 Status						
Enable	Line	Name	Mode	Up Time	Application	
No	Ethernet		---	00:00:00	Management	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
---	---	0	0	0	0	
WAN 4 Status						
Enable	Line	Name	Mode	Up Time	Application	
No	Ethernet		---	00:00:00	Management	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
---	---	0	0	0	0	
WAN 5 Status						
Enable	Line	Name	Mode	Up Time	Application	
No	Ethernet		---	00:00:00	Management	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
---	---	0	0	0	0	

Detailed explanation is shown below:

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

2.6 Saving Configuration

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



Status: Ready

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

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

2.7 Registering Vigor Router

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

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




The image shows the login page for a DrayTek Vigor130 router. The page has a red header with the DrayTek logo on the left and 'Vigor130' on the right. Below the header, the word 'Login' is written in white on a black background. The main content area is white and contains two input fields: 'Username' with the text 'admin' and 'Password' with five dots. A 'Login' button is positioned below the password field. At the bottom of the page, there is a small copyright notice: 'Copyright © 2012 DrayTek Corp. All Rights Reserved.'

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



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



LOGIN

UserName :

Password :

Auth Code : t x x h d d

If you cannot read the word, [click here](#)

[Forgotten password?](#)

Don't have a MyVigor Account ? [Create an account now](#)

If you are having difficulty logging in, contact our customer service.
Customer Service : (886) 3 597 2727 or

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



My

Home
Search

- D About Us
- P Product
- M My Information
- VigorACS SI
- Vigor Series
- Management
- Product Registration
- Customer Survey

My Information

Welcome, james_fae

Last Login Time : 2011-08-24 09:39:13

Last Login From : 123.110.144.220

Current Login Time : 2011-08-24 23:01:15

Current Login From : 114.37.142.184

RowNo : PageNo : Add

Your Device List

Serial Number / Host ID	Device Name	Model	Note
104001703857	Vigor2710	Vigor2710	-
200807100001	VigorPro5300	VigorPro5300	-
200911030001	ryan	VigorPro5300	-

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

The screenshot shows the 'My Product' registration page on the MyVigor website. The page has a red header with the DrayTek logo and 'MyVigor' text. A navigation menu on the left includes 'Home', 'About Us', 'Product', 'My Information', 'VigorACS SI', 'Vigor Series', 'Management', 'Product Registration', and 'Customer Survey'. The main content area is titled 'My Product' and 'Registration Device'. The form contains the following fields: Serial number (2011082214320301), Nickname (vigor130), Registration Date (04-24-2013), Usage (dropdown), Product Rating (dropdown), No. of Employees (dropdown), Supplier (text), Date of Purchase (text), and Internet Connection (checkboxes for Cable, ADSL, VDSL, Fiber, 3G, WIMAX, LTE). The 'Submit' button is highlighted with a red box.

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

Your device has been successfully added to the database.



- 7 Now, you have finished the product registration.
- 8 After clicking **OK**, you will see the following page. Your modem has been registered to *myvigor* website successfully.

3

Advanced Configuration

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

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

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

The screenshot displays the DrayTek Vigor 130 web management interface. The top navigation bar includes the DrayTek logo and 'Vigor 130'. A left sidebar contains menu items such as 'Quick Start Wizard', 'Internet Access', 'Firewall', and 'System Maintenance'. The main content area features a 'Dashboard' with a router image and several data tables.

System Information			
Model Name	Vigor130	System Up Time	0:0:26
Router Name		Current Time	2000 Jan 1 Sat 0:0:23
Firmware Version	3.7.1	Build Date/Time	Mar 15 2013 17:02:13
DSL Version	05-04-04-04-00-01	LAN MAC Address	00-1D-AA-82-EB-F0

IPv4 Internet Access				
	Line / Mode	IP Address	MAC Address	Up Time
WAN1	ADSL / ---	Disconnected	00-1D-AA-82-EB-F1	00:00:00

IPv6 Internet Access				
	Mode	Address	Scope	Up Time
LAN	RADVD / DHCPv6	FE80::21D:A AFF:FE82:EBF0/64	Link	

3.1 Internet Access

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

3.1.1 Basics of Internet Protocol (IP) Network

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

From 10.0.0.0 to 10.255.255.255

From 172.16.0.0 to 172.31.255.255

From 192.168.0.0 to 192.168.255.255

What are Public IP Address and Private IP Address

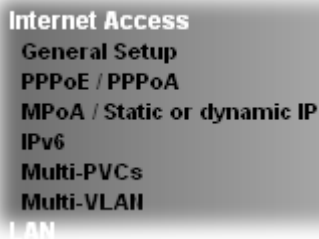
As the modem plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor modem. The modem itself will also use the default **private IP** address: 192.168.1.1 to communicate with the local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

Get Your Public IP Address from ISP

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

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

Below shows the menu items for Internet Access.



3.1.2 General Setup

This section will introduce some general settings of Internet.

Internet Access >> General Setup

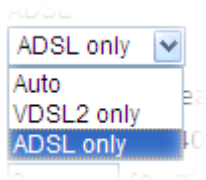
WAN 1

Display Name:	<input type="text"/>
Physical Mode:	ADSL
DSL Mode:	Auto <input type="button" value="v"/>
VLAN Tag insertion :	Disable <input type="button" value="v"/> (Please configure Internet Access setting first)
Tag value:	<input type="text" value="0"/> (0~4095)
Priority:	<input type="text" value="0"/> (0~7)

Note : In DSL auto mode, the router will reboot automatically while switching between VDSL2 and ADSL lines.

Available settings are explained as follows:

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

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

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

3.1.3 PPPoE/PPPoA

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

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

Internet Access >> PPPoE / PPPoA

PPPoE / PPPoA Client Mode

PPPoE/PPPoA Client Enable Disable

DSL Modem Settings (for ADSL mode only)

Multi-PVC channel: Channel 1

VPI: 8

VCI: 35

Encapsulating Type: VC MUX

Protocol: PPPoA

Modulation: Multimode

PPPoE Pass-through

For Wired LAN

Note: If this box is checked while using the PPPoA protocol, the router will behave like a modem which only serves the PPPoE client on the LAN.

VLAN Enable

VID: 0 (0~4095)

Priority: 0 (0~7)

WAN Connection Detection

Mode: ARP Detect

Ping IP:

TTL:

MTU: 1442 (Max: 1492)

ISP Access Setup

ISP Name:

Username:

Password:

PPP Authentication: PAP or CHAP

Always On

Idle Timeout: -1 second(s)

IP Address From ISP: WAN IP Alias

Fixed IP: Yes No (Dynamic IP)

Fixed IP Address:

Default MAC Address

Specify a MAC Address

MAC Address: 00 . 1D . AA : 82 . EB . F1

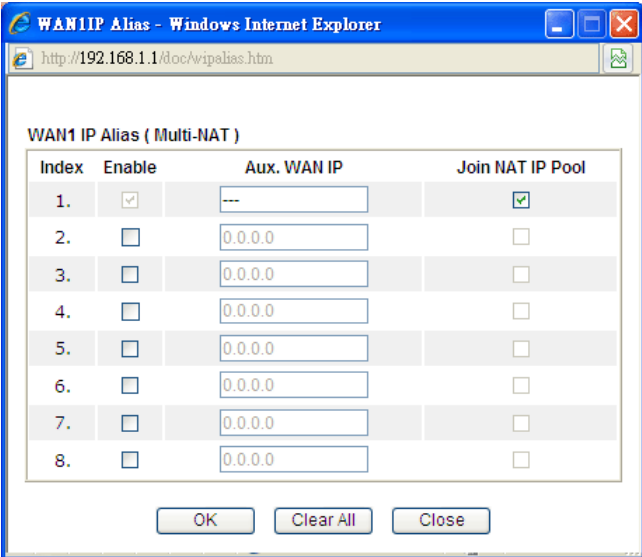
Index(1-15) in Schedule Setup:

=> , , ,

Available settings are explained as follows:

Item	Description
Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
DSL Modem Settings	Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP. Multi-PVC channel - The selections displayed here are determined by the page of Internet Access – Multi PVCs . VPI - Type in the value provided by ISP. VCI - Type in the value provided by ISP. Encapsulating Type - Drop down the list to choose the type

	<p>provided by ISP.</p> <p>Protocol - Drop down the list to choose the protocol, PPPoE or PPPoA.</p> <p>Modulation – Choose a suitable method for PPPoE/PPoA connection.</p>
PPPoE Pass-through	<p>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.</p> <p>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.</p> <p>VLAN Enable - Enable the function of VLAN with tag. The modem will add specific VLAN number to all packets while sending them out. Please type the tag value and specify the priority for the packets sent by the modem.</p> <p>VLAN ID –Type the value as the VLAN ID number. The range is form 1 to 4095.</p> <p>Priority (802.1p) - Type the packet priority number for such VLAN. The range is from 0 to 7.</p>
WAN Connection Detection	<p>Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.</p> <p>Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection.</p> <p>Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.</p> <p>TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.</p>
MTU	<p>It means Max Transmit Unit for packet. The default setting will be 1442.</p>
ISP Access Setup	<p>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.</p> <p>ISP Name – Type the name of the ISP if required.</p> <p>Username – Type in the username provided by ISP in this field.</p> <p>Password – Type in the password provided by ISP in this field.</p> <p>PPP Authentication – Select PAP only or PAP or CHAP for PPP.</p> <p>Always On - If you want to connect to Internet all the time, check the Always On box.</p> <p>Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action. This setting</p>

	<p>is active only when the Active on demand option for Active Mode is selected in WAN>> General Setup page.</p>
<p>IP Address From ISP</p>	<p>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.</p> <p>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.</p>  <p>Fixed IP – Click Yes to use this function and type in a fixed IP address in the box of Fixed IP Address.</p> <p>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.</p> <p>Specify a MAC Address – Type the MAC address for the modem manually.</p> <p>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.</p>

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

3.1.4 MPoA /Static or dynamic IP

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

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

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

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

Internet Access >> MPoA / Static or dynamic IP

MPoA / Static or dynamic IP

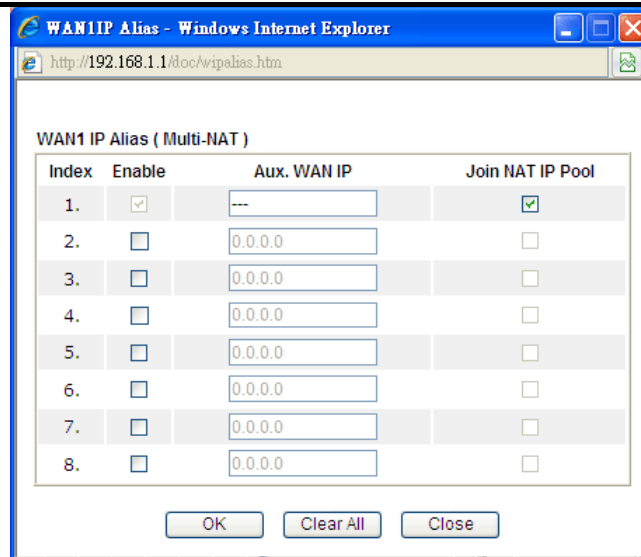
<p>MPoA (RFC1483/2684) <input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <p>DSL Modem Settings (for ADSL mode only)</p> <p>Multi-PVC channel: Channel 2</p> <p>Encapsulation: 1483 Bridged IP LLC</p> <p>VPI: 8</p> <p>VCI: 88</p> <p>Modulation: Multimode</p> <p><input type="checkbox"/> VLAN Enable</p> <p>VID: 0 (0~4095)</p> <p>Priority: 0 (0~7)</p> <p>WAN Connection Detection</p> <p>Mode: ARP Detect</p> <p>Ping IP: </p> <p>TTL: </p> <p>MTU: 1442 (Max:1500)</p> <p>RIP Protocol</p> <p><input type="checkbox"/> Enable RIP</p> <p>Bridge Mode</p> <p><input type="checkbox"/> Enable Bridge Mode</p>	<p>WAN IP Network Settings</p> <p><input type="radio"/> Obtain an IP address automatically</p> <p>Router Name: Vigor</p> <p>Domain Name: </p> <p>*: Required for some ISPs</p> <p>DHCP Client Identifier for some ISP</p> <p><input type="checkbox"/> Enable</p> <p>Username: </p> <p>Password: </p> <p><input checked="" type="radio"/> Specify an IP address: WAN IP Alias</p> <p>IP Address: 0.0.0.0</p> <p>Subnet Mask: 0.0.0.0</p> <p>Gateway IP Address: 0.0.0.0</p> <p><input checked="" type="radio"/> Default MAC Address</p> <p><input type="radio"/> Specify a MAC Address</p> <p>MAC Address: 00 . 1D . AA . 82 . EB . F1</p> <p>DNS Server IP Address</p> <p>Primary IP Address: 8.8.8.8</p> <p>Secondary IP Address: 8.8.4.4</p>
--	---

OK

Available settings are explained as follows:

Item	Description
Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
DSL Modem Settings	<p>Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP.</p> <p>Multi-PVC channel - The selections displayed here are determined by the page of Internet Access – Multi PVCs.</p> <p>VPI - Type in the value provided by ISP.</p> <p>VCI - Type in the value provided by ISP.</p> <p>Encapsulating Type - Drop down the list to choose the type provided by ISP.</p> <p>Protocol - Drop down the list to choose the protocol, PPPoE or</p>

	<p>PPPoA.</p> <p>Modulation – Choose a suitable method for PPPoE/PPoA connection.</p>
VLAN Enable	<p>Enable the function of VLAN with tag. The modem will add specific VLAN number to all packets while sending them out. Please type the tag value and specify the priority for the packets sending by the modem.</p> <p>VLAN ID –Type the value as the VLAN ID number. The range is form 1 to 4095.</p> <p>Priority (802.1p) - Type the packet priority number for such VLAN. The range is from 0 to 7.</p>
WAN Connection Detection	<p>Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.</p> <p>Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection.</p> <p>Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.</p> <p>TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.</p>
MTU	<p>It means Max Transmit Unit for packet. The default setting will be 1442.</p>
RIP Protocol	<p>Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how modems exchange routing tables information. Click Enable RIP for activating this function.</p>
Bridge Mode	<p>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.</p>
WAN IP Network Settings	<p>This group allows you to obtain an IP address automatically and allows you type in IP address manually.</p> <p>Obtain an IP address automatically – Click this button to obtain the IP address automatically.</p> <p>Modem Name – Type in the modem name provided by ISP.</p> <p>Domain Name – Type in the domain name that you have assigned.</p>
DHCP Client Identifier for some ISP	<p>This feature is offered for certain ISP with special request.</p> <p>Enable – Check this box to enable the function of DHCP client identifier for some ISP.</p> <p>Username – Type a username used for such function.</p> <p>Password – Type a password used for such function.</p>
Specify an IP address	<p>Click this radio button to specify some data.</p> <p>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.</p>



IP Address – Type in the private IP address.

Subnet Mask – Type in the subnet mask.

Gateway IP Address – Type in gateway IP address.

Default MAC Address

Type in MAC address for the modem. You can use **Default MAC Address** or specify another MAC address for your necessity.

MAC Address – Type in the MAC address for the modem manually.

DNS Server IP Address

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

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

3.1.5 IPv6

Offline

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

Internet Access >> IPv6

WAN 1

Internet Access Mode	
Connection Type	Offline

OK Cancel

PPP

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

No need to type any other information for PPP mode.

Internet Access >> IPv6

WAN 1

Internet Access Mode	
Connection Type	PPP
Note : IPv4 WAN setting should be PPPoE client.	

OK Cancel

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

Online Status

Physical Connection		System Uptime: 0:0:30	
IPv4	IPv6		
LAN Status			
IP Address			
2001:B010:7300:200:21D:AAFF:FE7A:3E58/64 (Global)			
FE80::21D:AAFF:FE7A:3E58/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
7	8	618	672
WAN2 IPv6 Status			
Enable	Mode	Up Time	
Yes	PPP	0:00:11	
IP			
2001:B010:7300:200:21D:AAFF:FE7A:3E5A/128 (Global)		Gateway IP	
FE80::1D:AAFF:FE7A:3E5A/128 (Link)		FE80::90:1A00:242:AD52	
DNS IP			
2001:B000:168::1			
2001:B000:168::2			
TX Packets	RX Packets	TX Bytes	RX Bytes
7	4	544	616

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

TSPC

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

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

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

WAN 1

Internet Access Mode	
Connection Type	TSPC
TSPC Configuration	
Username	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>
Tunnel Broker	<input type="text"/>

OK Cancel

Available settings are explained as follows:

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

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

AICCU

WAN 1

Internet Access Mode	
Connection Type	AICCU
AICCU Configuration	
<input checked="" type="checkbox"/> Always On	
Username	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>
Tunnel Broker	tic.sixxs.net
Subnet Prefix	<input type="text"/> / <input type="text"/>

Note : If "Always On" is not enabled,AICCU connection would only retry three times.

OK Cancel

Available settings are explained as follows:

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

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

DHCPv6 Client

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

Internet Access >> IPv6

WAN 1

Internet Access Mode

Connection Type DHCPv6 Client ▾

DHCPv6 Client Configuration

Identity Association Prefix Delegation Non-temporary Address

IAID (Identity Association ID)

Available settings are explained as follows:

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

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

Static IPv6

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

WAN 1

Internet Access Mode
 Connection Type: Static IPv6

Static IPv6 Address configuration
 IPv6 Address: / Prefix Length:

Current IPv6 Address Table

Index	IPv6 Address/Prefix Length	Scope

Static IPv6 Gateway configuration
 IPv6 Gateway Address:

Available settings are explained as follows:

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

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

3.1.6 Multi-PVCs

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

General

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

Internet Access >> Multi-PVCs

Enable Multi-PVCs Setup

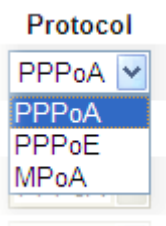
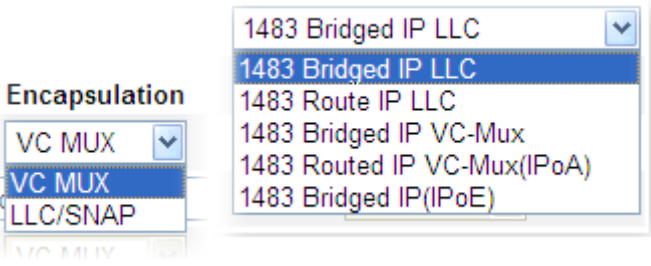
General			ATM QoS			
Channel	Enable	VPI	VCI	QoS Type	Protocol	Encapsulation
1.	<input checked="" type="checkbox"/>	8	35	UBR	PPPoA	VC MUX
2.	<input checked="" type="checkbox"/>	8	88	UBR	MPoA	1483 Bridged IP LLC
3.	<input type="checkbox"/>	1	43	UBR	PPPoA	VC MUX
4.	<input type="checkbox"/>	1	44	UBR	PPPoA	VC MUX
5.	<input type="checkbox"/>	1	45	UBR	PPPoA	VC MUX

Note:VPI/VCI must be unique for each channel!

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Enable Multi-PVCs Setup	Check it to enable the multi-PVCs function.
Enable	Check this box to enable that channel. The channels that you enabled here will be shown in the Multi-PVC channel drop down list on the web page of Internet Access . Though you can enable eight channels in this page, yet only one channel can be chosen on the web page of Internet Access .
VPI	Type in the value provided by your ISP.
VCI	Type in the value provided by your ISP.
QoS Type	Select a proper QoS type for the channel. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>QoS Type</p> <p>UBR ▾</p> <p>UBR</p> <p>CBR</p> <p>ABR</p> <p>ntVBR</p> <p>rtVBR</p> </div>

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

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

WAN for Router-borne Application: Management

Enable Disable

DSL Modem Settings

VPI: 1 QoS Type: UBR PVC Redirect: Disable

VCI: 43 Protocol: PPPoA Add Tag: 0

Encapsulation: VC MUX

WAN Connection Detection

Mode: ARP Detect

Ping IP:

TTL:

<p>PPPoE/PPPoA Client</p> <p>ISP Access Setup</p> <p>ISP Name: <input type="text"/></p> <p>Username: <input type="text"/></p> <p>Password: <input type="text"/></p> <p>PPP Authentication: PAP or CHAP</p> <p><input checked="" type="checkbox"/> Always On</p> <p>Idle Timeout: -1 second(s)</p> <p>IP Address From ISP</p> <p>Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)</p> <p>Fixed IP Address: <input type="text"/></p>	<p>MPoA (RFC1483/2684)</p> <p><input type="radio"/> Obtain an IP address automatically</p> <p>Router Name: Vigor</p> <p>Domain Name: <input type="text"/></p> <p><small>*: Required for some ISPs</small></p> <p><input checked="" type="radio"/> Specify an IP address</p> <p>IP Address: <input type="text"/></p> <p>Subnet Mask: <input type="text"/></p> <p>Gateway IP Address: <input type="text"/></p> <p>DNS Server IP Address</p> <p>Primary IP Address: 8.8.8.8</p> <p>Secondary IP Address: 8.8.4.4</p>
---	---

Available settings are explained as follows:

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

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

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

ATM QoS

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

Enable Multi-PVCs Setup


General		ATM QoS		
Channel	QoS Type	PCR	SCR	MBS
1.	UBR	0	0	0
2.	UBR	0	0	0
3.	UBR	0	0	0
4.	UBR	0	0	0
5.	UBR	0	0	0

Note: 1.Set 0 means default value.

2.PCR(max) = ADSL Up Speed / 53 / 8.

OK Clear Cancel

Available settings are explained as follows:

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

3.1.7 Multi-VLAN

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

Internet Access >> Multi-VLAN

Enable Multi-VLAN Setup

General

Channel	Enable		Add Tag	Priority
1.	<input type="checkbox"/>		<input type="text" value="0"/>	<input type="text" value="0"/>
2.	<input type="checkbox"/>		<input type="text" value="0"/>	<input type="text" value="0"/>
3.	<input type="checkbox"/>	WAN	<input type="text" value="0"/>	<input type="text" value="0"/>
4.	<input type="checkbox"/>	WAN	<input type="text" value="0"/>	<input type="text" value="0"/>
5.	<input type="checkbox"/>	WAN	<input type="text" value="0"/>	<input type="text" value="0"/>

- Note:**
1. Tag value must be set between 1 ~ 4095 and unique for each channel.
 2. Only one channel can be untagged (equal to 0) at a time.
 3. Channel 1 and channel 2 are reserved for NAT/Route application.
 4. Channel 3 to channel 5 can be used for Router-borne application.

Available settings are explained as follows:

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

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

WAN for Router-borne Application: Management ▼

PPPoE/PPPoA Client <input type="radio"/> Enable <input checked="" type="radio"/> Disable	Static or Dynamic IP <input type="radio"/> Enable <input checked="" type="radio"/> Disable
ISP Access Setup ISP Name <input type="text"/> Username <input type="text"/> Password <input type="text"/> PPP Authentication PAP or CHAP ▼ <input checked="" type="checkbox"/> Always On Idle Timeout <input type="text" value="-1"/> second(s)	WAN IP Network Settings <input type="radio"/> Obtain an IP address automatically Router Name <input type="text" value="Vigor"/> * Domain Name <input type="text"/> * *: Required for some ISPs <input checked="" type="radio"/> Specify an IP address IP Address <input type="text"/> Subnet Mask <input type="text"/> Gateway IP Address <input type="text"/>
IP Address From ISP Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/>	DNS Server IP Address Primary IP Address <input type="text" value="8.8.8.8"/> Secondary IP Address <input type="text" value="8.8.4.4"/>

Available settings are explained as follows:

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

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

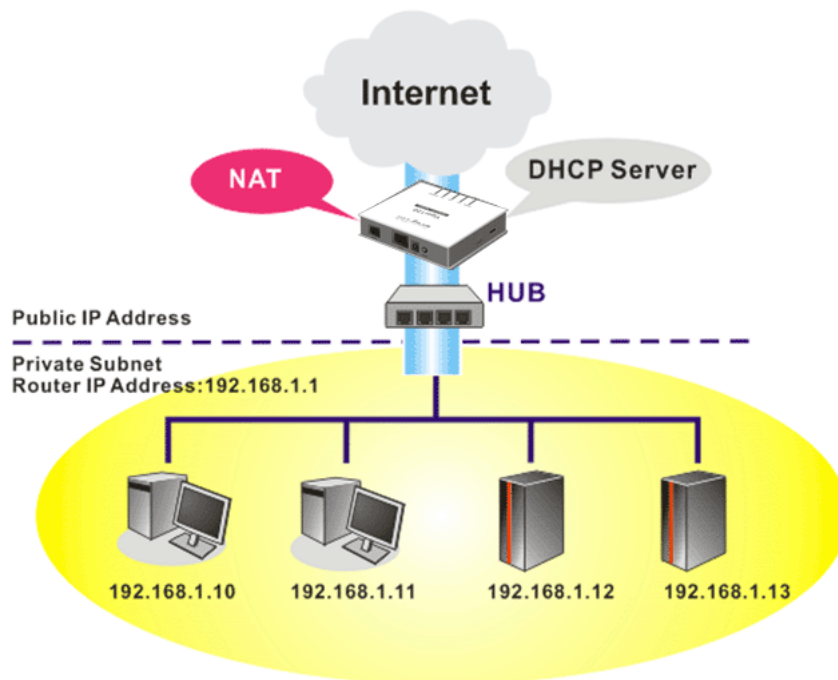
3.2 LAN

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

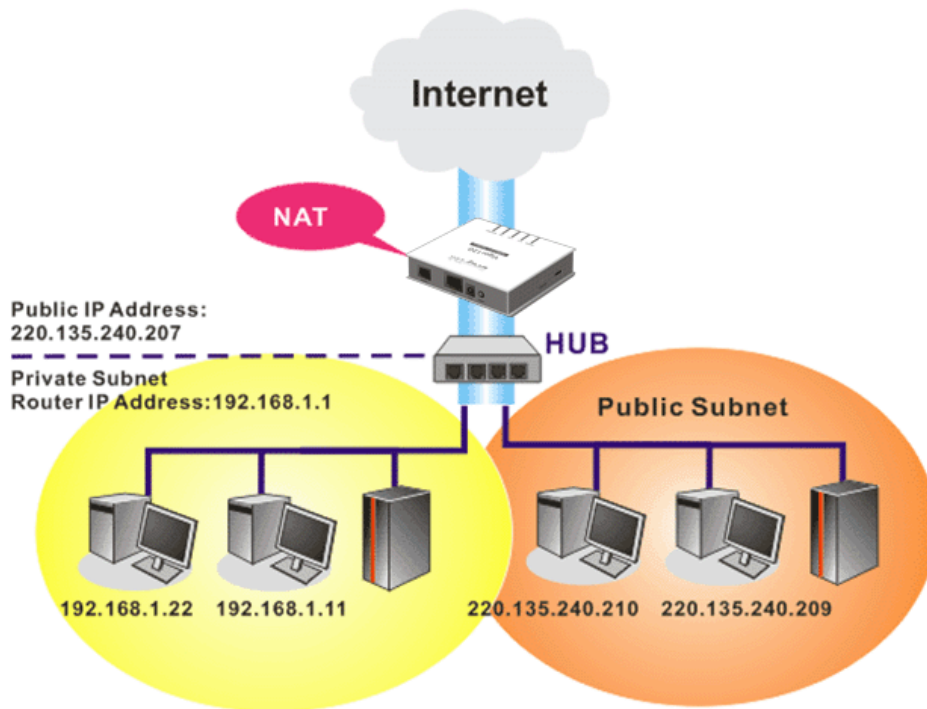
Internet Access
LAN
General Setup
Static Route
Bind IP to MAC
NAT

3.2.1 Basics of LAN

The most generic function of Vigor modem is NAT. It creates a private subnet of your own. As mentioned previously, the modem will talk to other public hosts on the Internet by using public IP address and talking to local hosts by using its private IP address. What NAT does is to translate the packets from public IP address to private IP address to forward the right packets to the right host and vice versa. Besides, Vigor modem has a built-in DHCP server that assigns private IP address to each local host. See the following diagram for a briefly understanding.



In some special case, you may have a public IP subnet from your ISP such as 220.135.240.0/24. This means that you can set up a public subnet or call second subnet that each host is equipped with a public IP address. As a part of the public subnet, the Vigor modem will serve for IP routing to help hosts in the public subnet to communicate with other public hosts or servers outside. Therefore, the modem should be set as the gateway for public hosts.

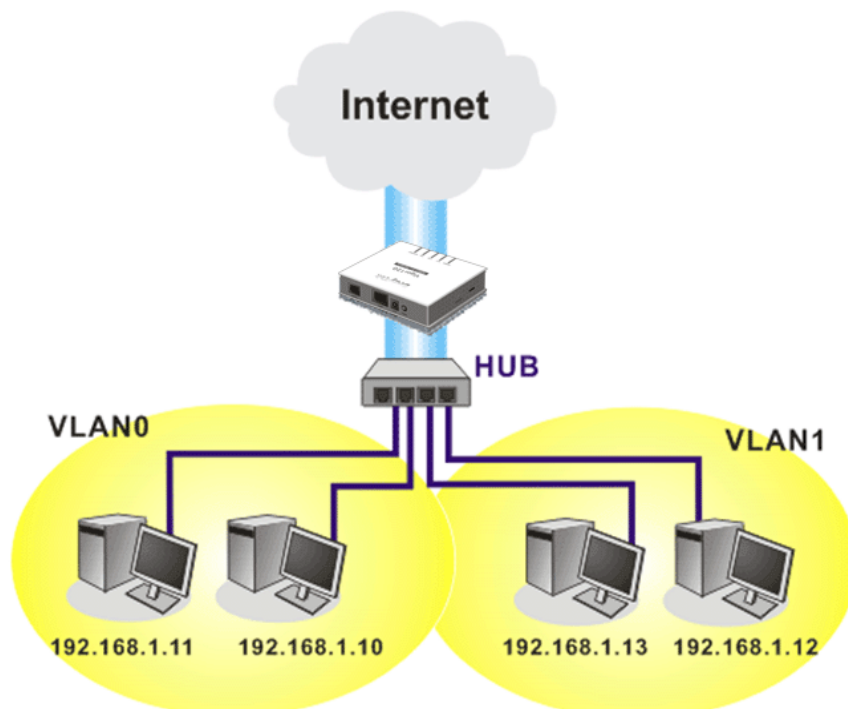


What is Routing Information Protocol (RIP)

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

What is Static Route

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



3.2.2 General Setup

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

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

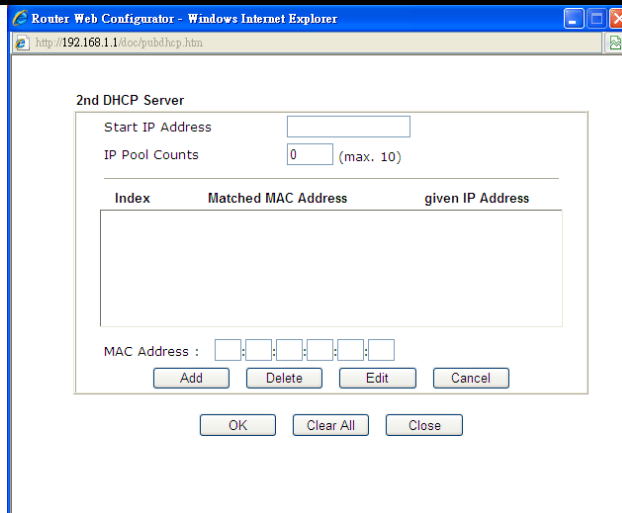
There are two configuration pages for LAN1, Ethernet TCP/IP and DHCP Setup (based on IPv4) and IPv6 Setup. Click the tab for each type and refer to the following explanations for detailed information.

LAN >> General Setup

Ethernet TCP / IP and DHCP Setup	LAN 1 IPv6 Setup
<p>LAN IP Network Configuration</p> <p>For NAT Usage</p> <p>1st IP Address <input type="text" value="192.168.1.1"/></p> <p>1st Subnet Mask <input type="text" value="255.255.255.0"/></p> <p>For IP Routing Usage <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p>2nd IP Address <input type="text" value="192.168.2.1"/></p> <p>2nd Subnet Mask <input type="text" value="255.255.255.0"/></p> <p><input type="button" value="2nd Subnet DHCP Server"/></p> <p>RIP Protocol Control <input type="text" value="Disable"/></p>	<p>DHCP Server Configuration</p> <p><input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server</p> <p>Relay Agent: <input type="radio"/> 1st Subnet <input type="radio"/> 2nd Subnet</p> <p>DHCP Server IP Address <input type="text"/></p> <p>Start IP Address <input type="text" value="192.168.1.10"/></p> <p>IP Pool Counts <input type="text" value="150"/></p> <p>Gateway IP Address <input type="text" value="192.168.1.1"/></p> <p>Lease Time <input type="text" value="259200"/> (s)</p> <p><input type="button" value="Advanced"/> You can configure DHCP options here.</p> <p>DNS Server IP Address</p> <p>Primary IP Address <input type="text"/></p> <p>Secondary IP Address <input type="text"/></p> <p><input type="checkbox"/> Force router to use address for DNS</p>
<input type="button" value="OK"/>	

Available settings are explained as follows:

Item	Description
LAN IP Network Configuration	<p>For NAT Usage,</p> <p>1st IP Address - Type in private IP address for connecting to a local private network (Default: 192.168.1.1).</p> <p>1st Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)</p> <p>For IP Routing Usage - Click Enable to invoke this function. The default setting is Disable.</p> <p>2nd Address - Type in secondary IP address for connecting to a subnet. (Default: 192.168.2.1/ 24)</p> <p>2nd Subnet Mask - An address code that determines the size of the network. (Default: 255.255.255.0/ 24)</p> <p>2nd Subnet DHCP Server - You can configure the modem to serve as a DHCP server for the 2nd subnet.</p>



- **Start IP Address:** Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 2nd IP address of your modem is 220.135.240.1, the starting IP address must be 220.135.240.2 or greater, but smaller than 220.135.240.254.
- **IP Pool Counts:** Enter the number of IP addresses in the pool. The maximum is 10. For example, if you type 3 and the 2nd IP address of your modem is 220.135.240.1, the range of IP address by the DHCP server will be from 220.135.240.2 to 220.135.240.11.
- **MAC Address:** Enter the MAC Address of the host one by one and click **Add** to create a list of hosts to be assigned, deleted or edited IP address from above pool. Set a list of MAC Address for 2nd DHCP server will help modem to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet.

RIP Protocol Control,

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

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

DHCP Server Configuration

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

If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help

you to redirect the DHCP request to the specified location.

Enable Server - Let the modem assign IP address to every host in the LAN.

Disable Server – Let you manually assign IP address to every host in the LAN.

Relay Agent – (1st subnet/2nd subnet) Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.

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

Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your modem is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.

IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.

Gateway IP Address - Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the modem, which means the modem is the default gateway.

Lease Time – Enter the time to determine how long the IP address assigned by DHCP server can be used.

– If required, click it to set option number for DHCP.

Advanced

DHCP packets can be processed by adding option number and data information when such function is enabled.

LAN >> General Setup

DHCP Options Status

Enable Disable

Options List

Index	Option Number	Ascii/Hex	Data
-------	---------------	-----------	------

Option Number:

Data Type: Ascii Hex (Example of Hex Data Type Input Format:0xff 0x00 0xc0 0xa8)

Data:

Note: Maximum number of custom DHCP option is five.

Enable/Disable – Enable/Disable the function of DHCP Option. This modem allows you to add up to five Option Numbers. Each DHCP option is composed by an option number with data. For example,

Option number: 100

Data: abcd

When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets.

Option Number – Type a number for such function.

	<p>Different number means different meaning. Please contact with your ISP for obtaining the correct number value.</p> <p>Data Type – Choose the type (ASCII or Hex) for the data to be calculated.</p> <p>Data – Type the content of the data to be processed by the function of DHCP option.</p>																
<p>DNS Server IP Address</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>The default DNS Server IP address can be found via Online Status:</p> <p>Online Status</p> <hr/> <p>Physical Connection System Uptime: 22:22:45</p> <table border="1" data-bbox="703 1133 1394 1205"> <thead> <tr> <th colspan="2">IPv4</th> <th colspan="2">IPv6</th> </tr> </thead> <tbody> <tr> <td>LAN Status</td> <td>Primary DNS: 8.8.8.8</td> <td></td> <td>Secondary DNS: 8.8.4.4</td> </tr> <tr> <td>IP Address</td> <td>TX Packets</td> <td>RX Packets</td> <td></td> </tr> <tr> <td>192.168.1.1</td> <td>0</td> <td>41533</td> <td></td> </tr> </tbody> </table> <p>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.</p> <p>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.</p> <p>Force router to use address for DNS- Force Vigor modem to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).</p>	IPv4		IPv6		LAN Status	Primary DNS: 8.8.8.8		Secondary DNS: 8.8.4.4	IP Address	TX Packets	RX Packets		192.168.1.1	0	41533	
IPv4		IPv6															
LAN Status	Primary DNS: 8.8.8.8		Secondary DNS: 8.8.4.4														
IP Address	TX Packets	RX Packets															
192.168.1.1	0	41533															

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

Details Page for LAN1 – IPv6 Setup

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

LAN 1 Ethernet TCP / IP and DHCP Setup
LAN 1 IPv6 Setup

RADVD Configuration

Enable Disable

Advertisement Lifetime Seconds (Range : 600 - 9000)

DHCPv6 Server Configuration

Enable Server Disable Server

Start IPv6 Address

End IPv6 Address

DNS Server IPv6 Address

Primary DNS Server

Secondary DNS Server

Static IPv6 Address configuration

IPv6 Address / Prefix Length

Current IPv6 Address Table

Index	IPv6 Address/Prefix Length	Scope
1	FE80::21D:AAFF:FEA8:B768/64	Link

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

Available settings are explained as follows:

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

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

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

3.2.3 Static Route

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

Static Route for IPv4

LAN >> Static Route Setup

IPv4			IPv6			Set to Factory Default	View Routing Table
Index	Destination Address	Status	Index	Destination Address	Status		
<u>1.</u>	???	?	<u>6.</u>	???	?		
<u>2.</u>	???	?	<u>7.</u>	???	?		
<u>3.</u>	???	?	<u>8.</u>	???	?		
<u>4.</u>	???	?	<u>9.</u>	???	?		
<u>5.</u>	???	?	<u>10.</u>	???	?		

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

Available settings are explained as follows:

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

Viewing Routing Table

Displays the routing table for your reference.

```
Diagnostics >> View Routing Table

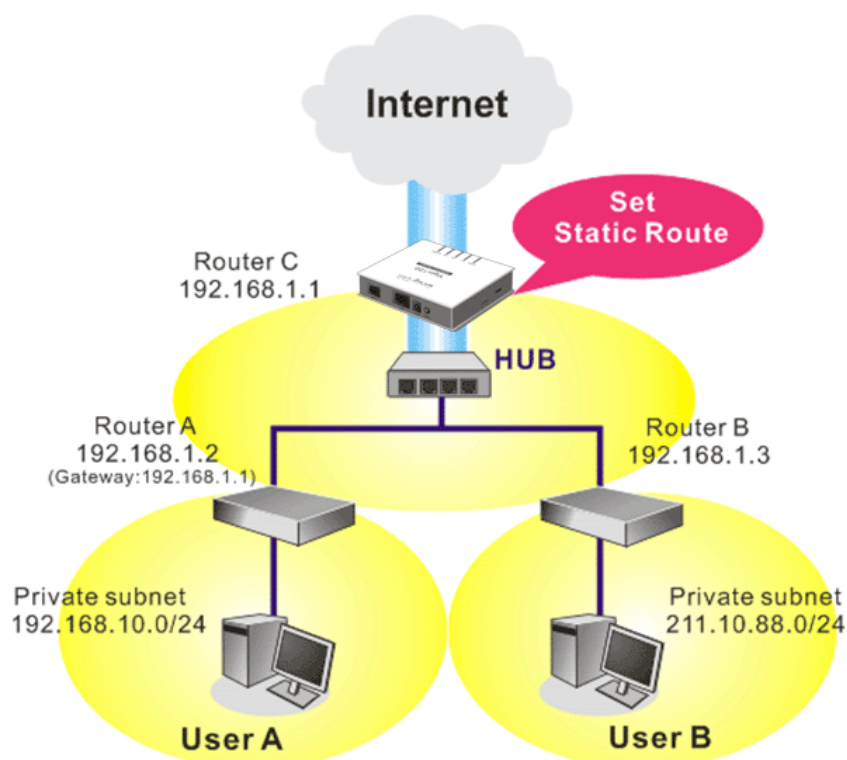
Current Running Routing Table      IPv6 Routing Table      Refresh |
Key: C - connected, S - static, R - RIP, * - default, ~ - private
C~ 192.168.1.0/255.255.255.0 directly connected LAN1
```

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

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

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

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



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

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

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

LAN >> Static Route Setup

Index No. 1

Enable

Destination IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Gateway IP Address: 192.168.1.2

Network Interface: LAN

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

OK Cancel Delete

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.

LAN >> Static Route Setup

Index No. 2

Enable

Destination IP Address: 211.100.88.0

Subnet Mask: 255.255.255.0

Gateway IP Address: 192.168.1.3

Network Interface: LAN

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

OK Cancel Delete

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

Current Running Routing Table	IPv6 Routing Table	Refresh
Key: C - connected, S - static, R - RIP, * - default, ~ - private		
S~	192.168.10.0/ 255.255.255.0	via 192.168.1.2 LAN1
C~	192.168.1.0/ 255.255.255.0	directly connected LAN1
S~	211.100.88.0/ 255.255.255.0	via 192.168.1.3 LAN1

Static Route for IPv6

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

LAN >> Static Route Setup

IPv4	IPv6	Set to Factory Default	View IPv6 Routing Table		
Index	Destination Address	Status	Index	Destination Address	Status
<u>1.</u>	::/0	x	<u>11.</u>	::/0	x
<u>2.</u>	::/0	x	<u>12.</u>	::/0	x
<u>3.</u>	::/0	x	<u>13.</u>	::/0	x
<u>4.</u>	::/0	x	<u>14.</u>	::/0	x
<u>5.</u>	::/0	x	<u>15.</u>	::/0	x
<u>6.</u>	::/0	x	<u>16.</u>	::/0	x
<u>7.</u>	::/0	x	<u>17.</u>	::/0	x
<u>8.</u>	::/0	x	<u>18.</u>	::/0	x
<u>9.</u>	::/0	x	<u>19.</u>	::/0	x
<u>10.</u>	::/0	x	<u>20.</u>	::/0	x

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

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

Available settings are explained as follows:

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

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

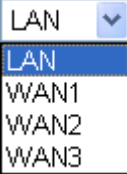
LAN >> Static Route Setup

Index No. 1

<input type="checkbox"/> Enable	
Destination IPv6 Address / Prefix Len	:: / 0
Gateway IPv6 Address	
Network Interface	LAN

OK Cancel Delete

Available settings are explained as follows:

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

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

3.2.4 Bind IP to MAC

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

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

Bind IP to MAC

Enable Disable Strict Bind

ARP Table		IP Bind List		
	Select All Sort Refresh		Select All Sort	
IP Address	Mac Address	Index	IP Address	Mac Address
192.168.1.10	E0-CB-4E-DA-48-79			

Add or Update

IP Address

Mac Address : : : : :

Comment

Show Comment

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

Available settings are explained as follows:

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

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

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

3.3 NAT

Usually, the modem serves as an NAT (Network Address Translation) modem. NAT is a mechanism that one or more private IP addresses can be mapped into a single public one.

Public IP address is usually assigned by your ISP, for which you may get charged. Private IP addresses are recognized only among internal hosts.

When the outgoing packets destined to some public server on the Internet reach the NAT modem, the modem will change its source address into the public IP address of the modem, select the available public port, and then forward it. At the same time, the modem shall list an entry in a table to memorize this address/port-mapping relationship. When the public server response, the incoming traffic, of course, is destined to the modem's public IP address and the modem will do the inversion based on its table. Therefore, the internal host can communicate with external host smoothly.

The benefit of the NAT includes:

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

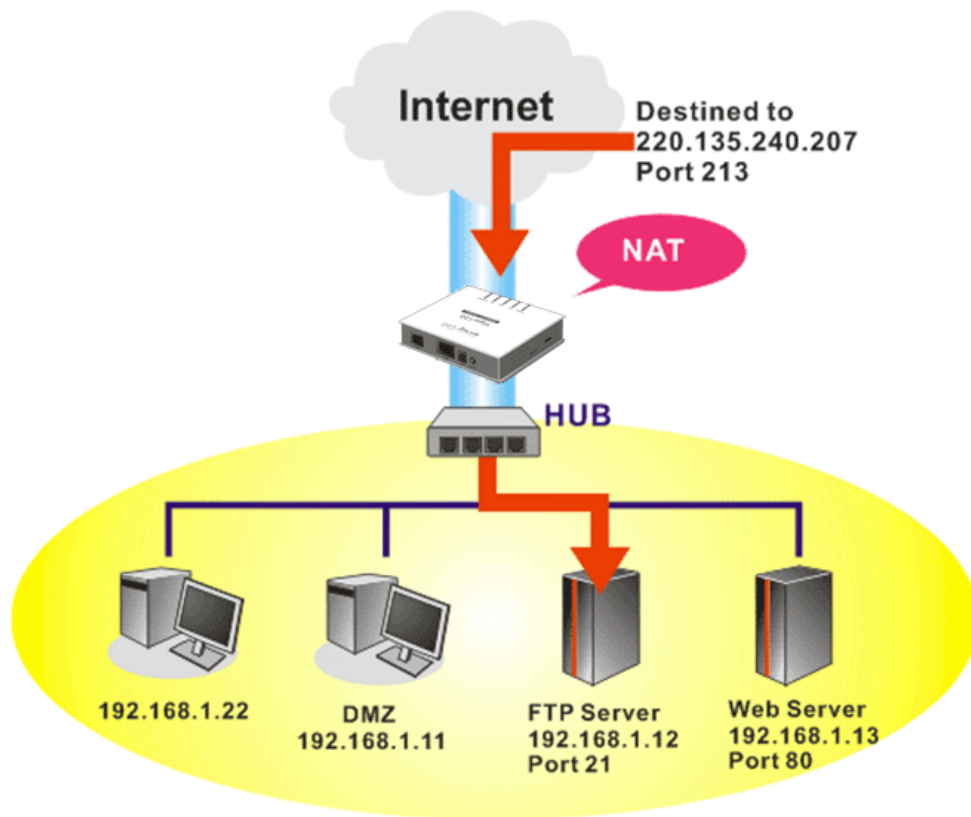
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the modem. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

Below shows the menu items for NAT.



3.3.1 Port Redirection

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



The port redirection can only apply to incoming traffic.

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

NAT >> Port Redirection

Port Redirection | [Set to Factory Default](#) |

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

<< [1-10](#) | [11-20](#) >> [Next](#) >>

Each item is explained as follows:

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

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

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

NAT >> Port Redirection

Index No. 1

Enable

Mode: Single

Service Name:

Protocol: ---

WAN IP: 1.All

Public Port:

Private IP:

Private Port:

Note: In "Range" Mode the End IP will be calculated automatically once the Public Port and Start IP have been entered.

Available settings are explained as follows:

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

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

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

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

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

System Maintenance >> Management

IPv4 Management Setup

Router Name:

Management Access Control

Allow management from the Internet

- FTP Server
- HTTP Server
- HTTPS Server
- Telnet Server
- SSH Server

Disable PING from the Internet

Access List

List	IP	Subnet Mask
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>

IPv6 Management Setup

Management Port Setup

User Define Ports Default Ports

Telnet Port: (Default: 23)

HTTP Port: (Default: 80)

HTTPS Port: (Default: 443)

FTP Port: (Default: 21)

SSH Port: (Default: 22)

SNMP Setup

Enable SNMP Agent

Get Community:

Set Community:

Manager Host IP:

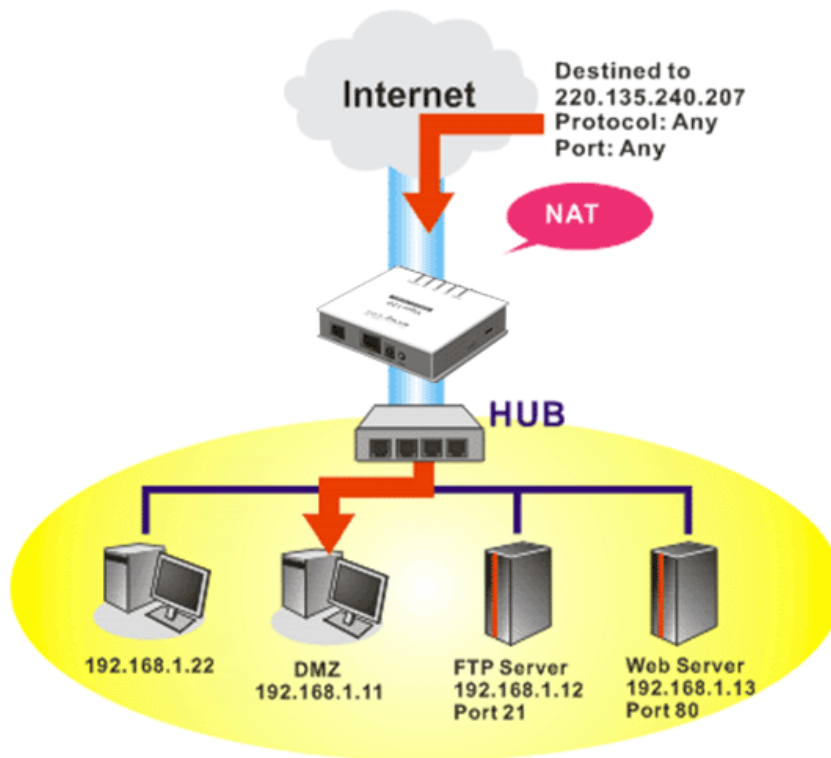
Trap Community:

Notification Host IP:

Trap Timeout: seconds

3.3.2 DMZ Host

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



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

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

NAT >> DMZ Host Setup

DMZ Host Setup

WAN1

WAN 1

None

Private IP

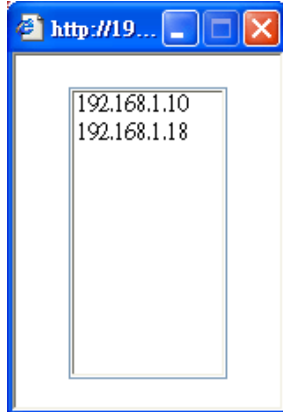
MAC Address of the True IP DMZ Host

Note: When a True-IP DMZ host is turned on, it will force the router's WAN connection to be always on.

Available settings are explained as follows:

Item	Description
<p>WAN 1</p> <p>None <input type="button" value="v"/></p> <p>None</p> <p>Private IP</p> <p>Active True IP</p>	<p>Choose Private IP or Active True IP first.</p> <p>Active True IP selection is available for WAN1 only.</p>
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.
Choose PC	Click this button and then a window will automatically pop

up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.



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

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

NAT >> DMZ Host Setup

DMZ Host Setup

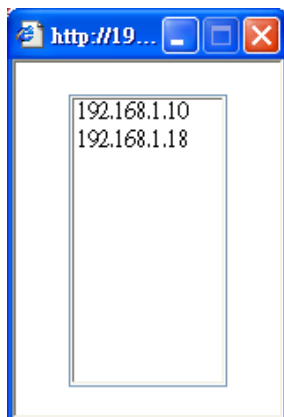
WAN1				
WAN 1				
Index	Enable	Aux. WAN IP	Private IP	
1.	<input type="checkbox"/>	---	0.0.0.0	Choose PC
2.	<input type="checkbox"/>	192.168.1.56	0.0.0.0	Choose PC

Available settings are explained as follows:

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

Choose PC

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



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

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

3.3.3 Open Ports

Open Ports allows you to open a range of ports for the traffic of special applications.

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

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

NAT >> Open Ports

Open Ports Setup | [Set to Factory Default](#) |

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

<< [1-10](#) | [11-20](#) >> [Next](#) >>

Available settings are explained as follows:

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

Comment	Specify the name for the defined network service.
WAN Interface	Display the WAN interface used by such index.
Aux. WAN IP	Display the IP address defined in WAN Alias for PPPoE/PPPoA or MPoA mode.
Local IP Address	Display the private IP address of the local host offering the service.
Status	Display the state for the corresponding entry. X or V is to represent the Inactive or Active state.

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

NAT >> Open Ports >> Edit Open Ports

Index No. 1

Enable Open Ports

Comment

WAN Interface

WAN IP

Local Computer

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	TCP	80	80	2.	----	0	0
3.	UDP	100	120	4.	----	0	0
5.	TCP/UDP	80	120	6.	----	0	0
7.	----	0	0	8.	----	0	0
9.	----	0	0	10.	----	0	0

Available settings are explained as follows:

Item	Description
Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
WAN Interface	Specify the WAN interface that will be used for this entry.
WAN IP	Specify the WAN IP address that will be used for this entry. This setting is available when WAN IP Alias is configured.
Local Computer	Enter the private IP address of the local host or click Choose PC to select one. Choose PC - Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.
Protocol	Specify the transport layer protocol. It could be TCP , UDP , or ---- (none) for selection.

Start Port	Specify the starting port number of the service offered by the local host.
End Port	Specify the ending port number of the service offered by the local host.

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

3.4 Firewall

3.4.1 Basics for Firewall

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

Firewall Facilities

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

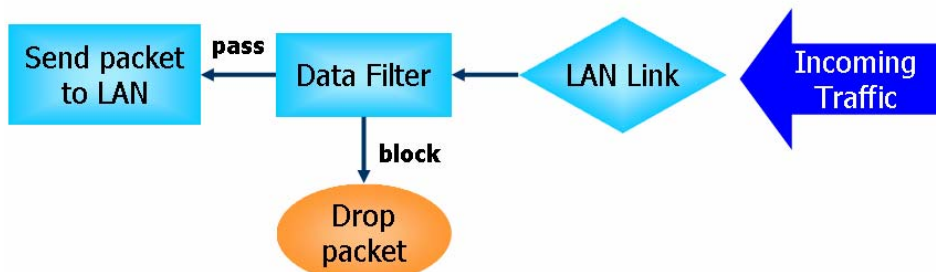
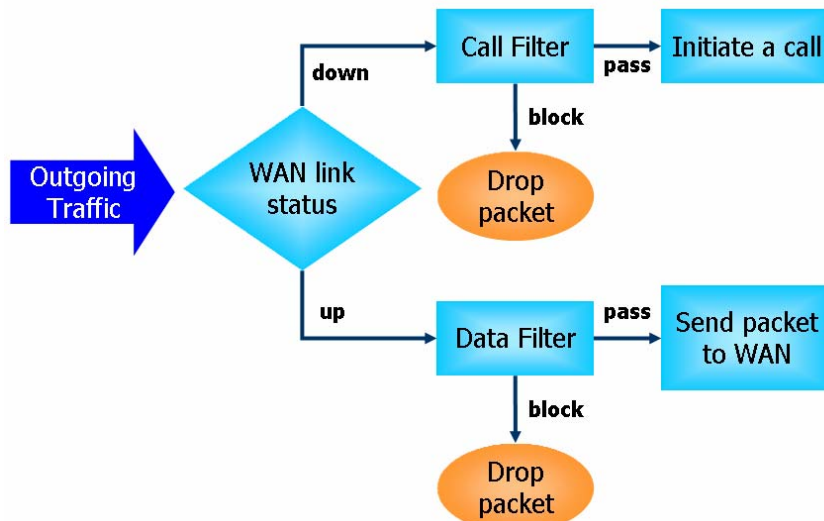
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

IP Filters

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

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

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



Stateful Packet Inspection (SPI)

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

URL Content Filter

To provide an appropriate cyberspace to users, Vigor modem equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor modem can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system.

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

Denial of Service (DoS) Defense

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

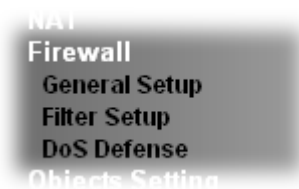
The **DoS Defense** function enables the Vigor modem to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog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

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

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

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

Below shows the menu items for Firewall.



3.4.2 General Setup

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

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

General Setup

General Setup
Default Rule

Call Filter Enable Disable

Data Filter Enable Disable

Start Filter Set Set#1 ▼

Start Filter Set Set#2 ▼

Accept large incoming fragmented UDP or ICMP packets (for some games, ex. CS)

Enable Strict Security Firewall

OK
Cancel

Available settings are explained as follows:

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

Default Rule Page

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

General Setup

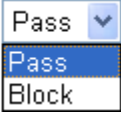
General Setup
Default Rule

Actions for default rule:

Application	Action/Profile	Syslog
Filter	Pass <input type="button" value="v"/>	<input type="checkbox"/>
Sessions Control	18 / <input type="text" value="12000"/>	<input type="checkbox"/>
URL Content Filter	None <input type="button" value="v"/>	<input type="checkbox"/>

Advance Setting

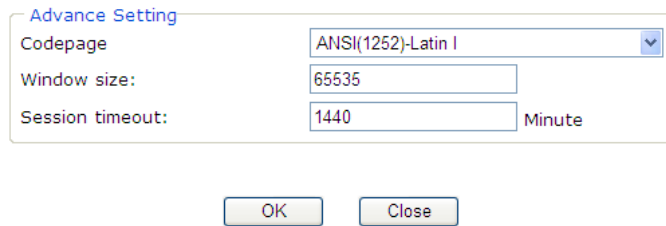
Available settings are explained as follows:

Item	Description
Filter	Select Pass or Block for the packets that do not match with the filter rules. <div style="text-align: right; margin-top: 10px;">  </div>
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.
URL Content Filter	Select one of the URL Content Filter profile settings (created in CSM>> URL Content Filter) for applying with this modem. Please set at least one profile for choosing in CSM>> URL Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.

Advance Setting

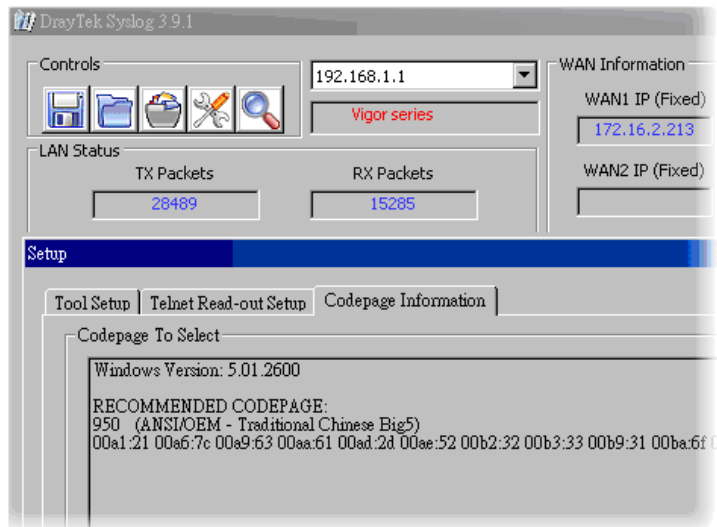
Click **Edit** to open the following window. However, it is **strongly recommended** to use the default settings here.

Firewall >> General Setup



Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.

If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.



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

Session timeout – Setting timeout for sessions can make the best utilization of network resources.

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

3.4.3 Filter Setup

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

Firewall >> Filter Setup

Filter Setup		Set to Factory Default	
Set	Comments	Set	Comments
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	

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.

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1

Comments :

Filter Rule	Active	Comments	Move Up	Move Down
<input type="button" value="1"/>	<input checked="" type="checkbox"/>	Block NetBios		Down
<input type="button" value="2"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="3"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="4"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="5"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="6"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="7"/>	<input type="checkbox"/>		UP	

Next Filter Set

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.

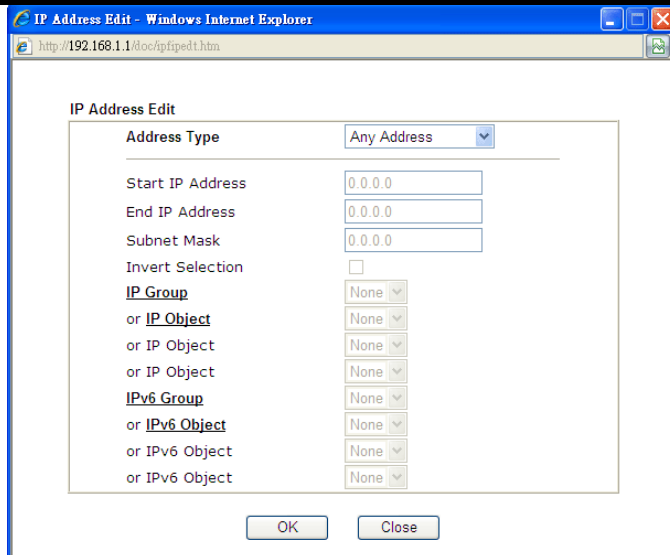
To edit **Filter Rule**, click the **Filter Rule** index button to enter the **Filter Rule** setup page.

Filter Set 1 Rule 1

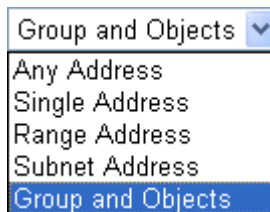
<input checked="" type="checkbox"/> Check to enable the Filter Rule		
Comments:	Block NetBios	
Index(1-15) in Schedule Setup:	, , ,	
Clear sessions when schedule ON:	<input type="checkbox"/> Enable	
<hr/>		
Direction:	LAN/RT/VPN -> WAN	
Source IP:	Any	<input type="button" value="Edit"/>
Destination IP:	Any	<input type="button" value="Edit"/>
Service Type:	TCP/UDP, Port: from 137~139 to any	<input type="button" value="Edit"/>
Fragments:	Don't Care	
<hr/>		
Application	Action/Profile	Syslog
Filter:	Block Immediately	<input type="checkbox"/>
Branch to Other Filter Set:	None	
Sessions Control	0 / 12000	<input type="checkbox"/>
MAC Bind IP	Non-Strict	<input type="checkbox"/>
URL Content Filter:	None	<input type="checkbox"/>
<hr/>		
Advance Setting	<input type="button" value="Edit"/>	

Available settings are explained as follows:

Item	Description
Check to enable the Filter Rule	Check this box to enable the filter rule.
Comments	Enter filter set comments/description. Maximum length is 14- character long.
Index(1-15)	Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this field is blank and the function will always work.
Clear sessions when schedule ON	Check this box to clear the sessions when the above schedule profiles are applied.
Direction	<p>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.</p> <div style="border: 1px solid black; padding: 5px; width: fit-content;"> <p>LAN/RT/VPN -> WAN</p> <p style="background-color: #0056b3; color: white; padding: 2px;">LAN/RT/VPN -> WAN</p> <p>WAN -> LAN/RT/VPN</p> <p>LAN/RT/VPN -> LAN/RT/VPN</p> </div> <p>Note: RT means routing domain for 2nd subnet or other LAN.</p>
Source/Destination IP	Click Edit to access into the following dialog to choose the source/destination IP or IP ranges.



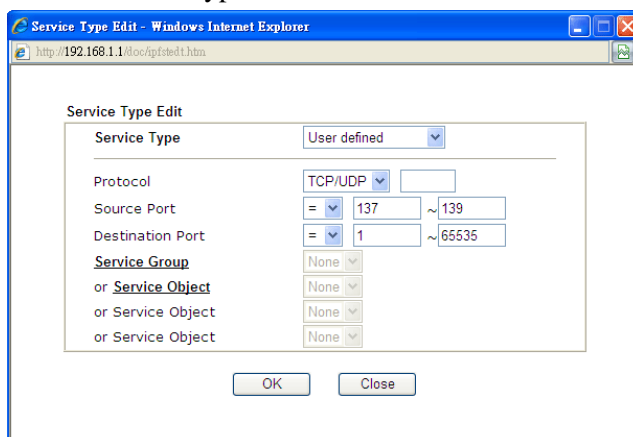
To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.



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.

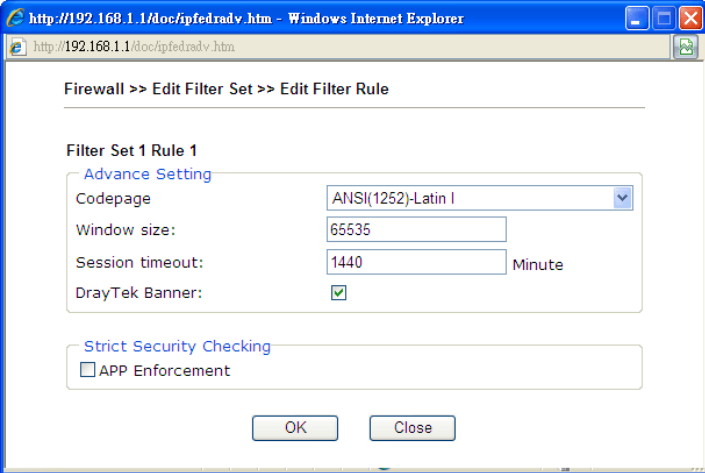
Service Type

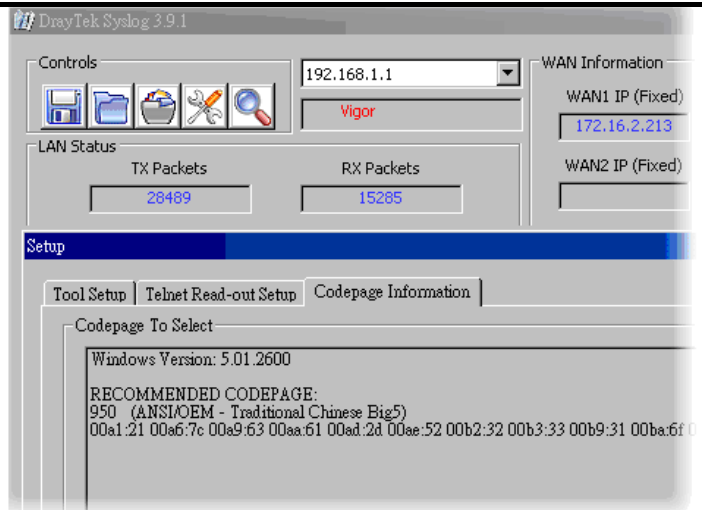
Click **Edit** to access into the following dialog to choose a suitable service type.



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.

	<div data-bbox="699 197 970 309" style="border: 1px solid black; padding: 2px;"> User defined ▼ User defined Group and Objects </div> <p>Protocol - Specify the protocol(s) which this filter rule will apply to.</p> <p>Source/Destination Port –</p> <p>(=) – 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.</p> <p>(!=) – 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.</p> <p>(>) – the port number greater than this value is available.</p> <p>(<) – the port number less than this value is available for this profile.</p> <p>Service Group/Object - Use the drop down list to choose the one that you want.</p>
Fragments	Specify the action for fragmented packets. And it is used for Data Filter only. <p>Don't care -No action will be taken towards fragmented packets.</p> <p>Unfragmented -Apply the rule to unfragmented packets.</p> <p>Fragmented - Apply the rule to fragmented packets.</p> <p>Too Short - Apply the rule only to packets that are too short to contain a complete header.</p>
Filter	Specifies the action to be taken when packets match the rule. <p>Block Immediately - Packets matching the rule will be dropped immediately.</p> <p>Pass Immediately - Packets matching the rule will be passed immediately.</p> <p>Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.</p> <p>Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.</p>
Branch to other Filter Set	If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the modem will apply the specified filter rule for ever and will not return to previous filter rule any more.
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.
MAC Bind IP	Strict – Make the MAC address and IP address settings configured in IP Object for Source IP and Destination IP

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



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

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

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



Example

As stated before, all the traffic will be separated and arbitrated using one 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.

Firewall >> General Setup

General Setup

General Setup Default Rule

Call Filter Enable Start Filter Set: Set#1

Disable

Data Filter Enable Start Filter Set: Set#2

Disable

Accept large incoming fragmented UDP or ICMP packets (for some g:

Enable Strict Security Firewall

OK Cancel

Firewall >> Filter Setup

Filter Setup | Set to Factory Default |

Set	Comments	Set	Comments
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1

Comments: Default Call Filter

Filter Rule	Active	Comments
1	<input checked="" type="checkbox"/>	Block NetBios
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	
7	<input type="checkbox"/>	

OK Clear Cancel

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 1

Check to enable the Filter Rule

Comments: Block NetBios

Index(1-15) in Schedule Setup: , , ,

Clear sessions when schedule ON: Enable

Direction: LAN/RT/VPN -> WAN

Source IP: Any Edit

Destination IP: Any Edit

Service Type: TCP/UDP, Port: from 137~139 to any Edit

Fragments: Dont Care

Application

Filter: Block Immediately ActionProfile Syslog

Branch to Other Filter Set: None

Sessions Control: 0 / 12000

MAC Bind IP: Non-Strict

URL Content Filter: None

Advance Setting Edit

3.4.4 DoS Defense

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

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

Firewall >> DoS defense Setup

DoS defense Setup

Enable DoS Defense Select All

<input type="checkbox"/> Enable SYN flood defense	Threshold	<input type="text" value="50"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable UDP flood defense	Threshold	<input type="text" value="150"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable ICMP flood defense	Threshold	<input type="text" value="50"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable Port Scan detection	Threshold	<input type="text" value="150"/>	packets / sec

Block IP options
 Block Land
 Block Smurf
 Block trace route
 Block SYN fragment
 Block Fraggle Attack

Block TCP flag scan
 Block Tear Drop
 Block Ping of Death
 Block ICMP fragment
 Block Unassigned Numbers

Enable DoS defense function to prevent the attacks from hacker or crackers.

OK
Clear All
Cancel

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	<p>Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor modem will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor modem.</p> <p>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.</p>
Enable UDP flood defense	Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor modem

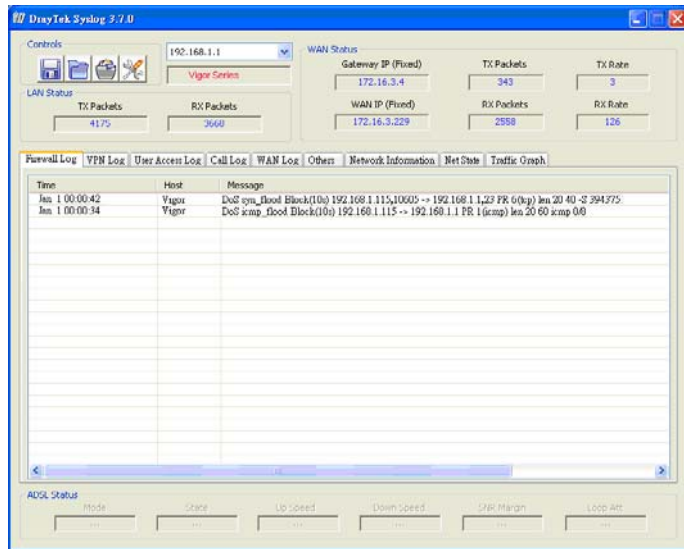
	<p>will start to randomly discard the subsequent UDP packets for a period defined in Timeout.</p> <p>The default setting for threshold and timeout are 150 packets per second and 10 seconds, respectively. That means, when 150 packets per second received, they will be regarded as “attack event” and the session will be paused for 10 seconds.</p>
Enable ICMP flood defense	<p>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.</p> <p>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.</p>
Enable PortScan detection	<p>Port Scan attacks the Vigor modem by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor modem will send out a warning.</p> <p>By default, the Vigor modem sets the threshold as 150 packets per second. That means, when 150 packets per second received, they will be regarded as “attack event”.</p>
Block IP options	<p>Check the box to activate the Block IP options function. The Vigor modem will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages...etc. An eavesdropper outside might learn the details of your private networks.</p>
Block Land	<p>Check the box to enforce the Vigor modem to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.</p>
Block Smurf	<p>Check the box to activate the Block Smurf function. The Vigor modem will ignore any broadcasting ICMP echo request.</p>
Block trace router	<p>Check the box to enforce the Vigor modem not to forward any trace route packets.</p>
Block SYN fragment	<p>Check the box to activate the Block SYN fragment function. The Vigor modem will drop any packets having SYN flag and more fragment bit set.</p>
Block Fraggle Attack	<p>Check the box to activate the Block fraggle Attack function.</p>

	<p>Any broadcast UDP packets received from the Internet is blocked.</p> <p>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.</p>
Block TCP flag scan	<p>Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include <i>no flag scan</i>, <i>FIN without ACK scan</i>, <i>SYN FINscan</i>, <i>Xmas scan</i> and <i>full Xmas scan</i>.</p>
Block Tear Drop	<p>Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor modem is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.</p>
Block Ping of Death	<p>Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor modems will block any packets realizing this attacking activity.</p>
Block ICMP Fragment	<p>Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.</p>
Block Unassigned Numbers	<p>Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the modem should have ability to detect and reject this kind of packets.</p>
Warning Messages	<p>We provide Syslog function for user to retrieve message from Vigor modem. The user, as a Syslog Server, shall receive the report sending from Vigor modem which is a Syslog Client.</p> <p>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.</p>

SysLog / Mail Alert Setup

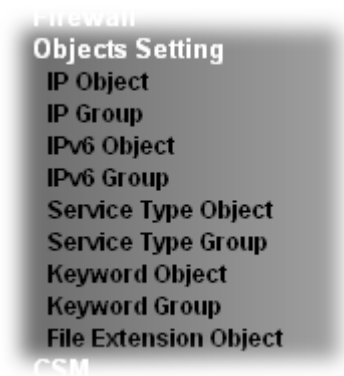
<p>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Syslog Save to:</p> <p><input checked="" type="checkbox"/> Syslog Server</p> <p><input type="checkbox"/> USB Disk</p> <p>Router Name: <input type="text"/></p> <p>Server IP Address: <input type="text"/></p> <p>Destination Port: <input type="text" value="514"/></p> <p>Mail Syslog: <input type="checkbox"/> Enable</p> <p>Enable syslog message:</p> <p><input checked="" type="checkbox"/> Firewall Log</p> <p><input checked="" type="checkbox"/> User Access Log</p> <p><input checked="" type="checkbox"/> WAN Log</p> <p><input checked="" type="checkbox"/> Router/DSL information</p> <p>AlertLog Setup</p> <p><input type="checkbox"/> Enable</p> <p>AlertLog Port: <input type="text" value="514"/></p>	<p>Mail Alert Setup</p> <p><input checked="" type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/></p> <p>SMTP Server: <input type="text"/></p> <p>SMTP Port: <input type="text" value="25"/></p> <p>Mail To: <input type="text"/></p> <p>Return-Path: <input type="text"/></p> <p><input type="checkbox"/> Authentication</p> <p>User Name: <input type="text"/></p> <p>Password: <input type="text"/></p> <p>Enable E-Mail Alert:</p> <p><input checked="" type="checkbox"/> DoS Attack</p> <p><input checked="" type="checkbox"/> IM-P2P</p> <p><input checked="" type="checkbox"/> VPN LOG</p>
---	--

Note: 1. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to".
 2. Mail Syslog feature sends a Syslog file when its size reaches 1M Bytes.



3.5 Objects Settings

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



3.5.1 IP Object

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

Objects Setting >> IP Object

IP Object Profiles: | [Set to Factory Default](#) |

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

<< [1-32](#) | [33-64](#) | [65-96](#) | [97-128](#) | [129-160](#) | [161-192](#) >> [Next](#) >>

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.

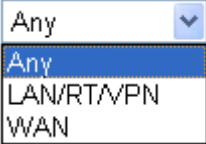
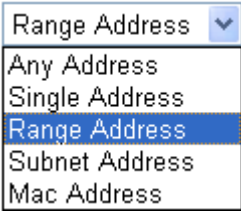
2. The configuration page will be shown as follows:

Objects Setting >> IP Object

Profile Index : 1

Name:	RD Department
Interface:	Any
Address Type:	Range Address
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	192.168.1.59
End IP Address:	192.168.1.65
Subnet Mask:	0.0.0.0
Invert Selection:	<input type="checkbox"/>

Available settings are explained as follows:

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

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

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

Objects Setting >> IP Object

IP Object Profiles:

Index	Name	Index
<u>1.</u>	RD Department	<u>17.</u>
<u>2.</u>	Financial Dept	<u>18.</u>
<u>3.</u>	HR Department	<u>19.</u>
<u>4.</u>		<u>20.</u>
<u>5.</u>		<u>21.</u>
<u>6.</u>		<u>22.</u>

3.5.2 IP Group

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

Objects Setting >> IP Group

IP Group Table:

[Set to Factory Default](#)

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

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:

Objects Setting >> IP Group

Profile Index : 1

Name:

Interface:

Available IP Objects

1-RD Department

2-Financial Dept

3-HR Department

Selected IP Objects

Available settings are explained as follows:

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

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

3.5.3 IPv6 Object

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

Objects Setting >> IPv6 Object

IPv6 Object Profiles: [Set to Factory Default](#)

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

<< [1-32](#) | [33-64](#) >> [Next](#) >>

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:

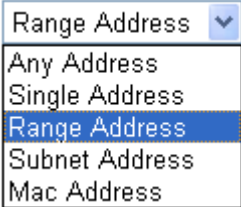
1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> IPv6 Object

Profile Index : 1

Name:	<input type="text"/>
Address Type:	Subnet Address <input type="button" value="v"/>
Mac Address:	<input type="text" value="00:00:00:00:00:00"/>
Start IP Address:	<input type="text"/>
End IP Address:	<input type="text"/>
Prefix Length:	<input type="text"/>
Invert Selection:	<input type="checkbox"/>

Available settings are explained as follows:

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

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

3.5.4 IPv6 Group

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

Objects Setting >> IPv6 Group

IPv6 Group Table: | [Set to Factory Default](#) |

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

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:

Objects Setting >> IPv6 Group

Profile Index : 1

Name:

Available IPv6 Objects

>>

<<

Selected IPv6 Objects

Available settings are explained as follows:

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

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

3.5.5 Service Type Object

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

Objects Setting >> Service Type Object

Service Type Object Profiles: | [Set to Factory Default](#) |

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

<< [1-32](#) | [33-64](#) | [65-96](#) >> [Next](#) >>

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:

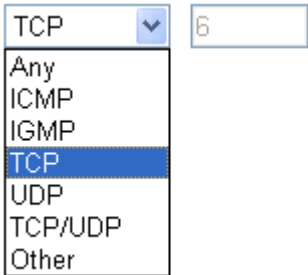
1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> Service Type Object Setup

Profile Index : 1

Name	<input type="text" value="www"/>
Protocol	TCP <input type="text" value="6"/>
Source Port	= <input type="text" value="1"/> ~ <input type="text" value="65535"/>
Destination Port	= <input type="text" value="1"/> ~ <input type="text" value="65535"/>

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. 
Source/Destination Port	<p>Source Port and the Destination Port column are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number.</p> <p>(=) – 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.</p> <p>(!=) – 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.</p> <p>(>) – the port number greater than this value is available.</p> <p>(<) – the port number less than this value is available for this profile.</p>

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

Objects Setting >> Service Type Object

Service Type Object Profiles:

Index	Name	Index
<u>1.</u>	www	<u>17.</u>
<u>2.</u>	SIP	<u>18.</u>
<u>3.</u>		<u>19.</u>
<u>4.</u>		<u>20.</u>

3.5.6 Service Type Group

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

Objects Setting >> Service Type Group

Service Type Group Table:

[Set to Factory Default](#)

Group	Name	Group	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

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:

Objects Setting >> Service Type Group Setup

Profile Index : 1

Name:

Available Service Type Objects		Selected Service Type Objects
1-www	<input type="button" value=">>"/> <input type="button" value="<<"/>	
2-SIP		

Available settings are explained as follows:

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

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

3.5.7 Keyword Object

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

Objects Setting >> Keyword Object

Keyword Object Profiles: [Set to Factory Default](#)

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

<< [1-32](#) | [33-64](#) | [65-96](#) | [97-128](#) | [129-160](#) | [161-192](#) | [193-200](#) >> [Next](#) >>

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:

Objects Setting >> Keyword Object Setup

Profile Index : 1

Name	<input type="text"/>
Contents	<input type="text"/>

Limit of Contents: Max 3 Words and 63 Characters.
Each word should be separated by a single space.

You can replace a character with %HEX.
Example:
Contents: backdoo%72 virus keep%20out

Result:
1. backdoor
2. virus
3. keep out

Available settings are explained as follows:

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

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

3.5.8 Keyword Group

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

Objects Setting >> Keyword Group

Keyword Group Table: | [Set to Factory Default](#) |

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

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:

Objects Setting >> Keyword Group Setup

Profile Index : 1

Name:

Available Keyword Objects

1-Key-1
2-Key-2

Selected Keyword Objects(Max 16 Objects)

(Empty)

Available settings are explained as follows:

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

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

3.5.9 File Extension Object

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

Objects Setting >> File Extension Object

File Extension Object Profiles: | [Set to Factory Default](#) |

Profile	Name	Profile	Name
<u>1.</u>		<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	

Available settings are explained as follows:

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

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

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

Objects Setting >> File Extension Object Setup

Profile Index: 1 Profile Name:

Categories	File Extensions
Image <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .bmp <input type="checkbox"/> .dib <input type="checkbox"/> .gif <input type="checkbox"/> .jpeg <input type="checkbox"/> .jpg <input type="checkbox"/> .jpg2 <input type="checkbox"/> .jp2 <input type="checkbox"/> .pct <input type="checkbox"/> .pcx <input type="checkbox"/> .pic <input type="checkbox"/> .pict <input type="checkbox"/> .png <input type="checkbox"/> .tif <input type="checkbox"/> .tiff
Video <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .asf <input type="checkbox"/> .avi <input type="checkbox"/> .mov <input type="checkbox"/> .mpe <input type="checkbox"/> .mpeg <input type="checkbox"/> .mpg <input type="checkbox"/> .mp4 <input type="checkbox"/> .qt <input type="checkbox"/> .rm <input type="checkbox"/> .wmv <input type="checkbox"/> .3gp <input type="checkbox"/> .3gpp <input type="checkbox"/> .3gpp2 <input type="checkbox"/> .3g2
Audio <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .aac <input type="checkbox"/> .aiff <input type="checkbox"/> .au <input type="checkbox"/> .mp3 <input type="checkbox"/> .m4a <input type="checkbox"/> .m4p <input type="checkbox"/> .ogg <input type="checkbox"/> .ra <input type="checkbox"/> .ram <input type="checkbox"/> .vox <input type="checkbox"/> .wav <input type="checkbox"/> .wma
Java <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .class <input type="checkbox"/> .jad <input type="checkbox"/> .jar <input type="checkbox"/> .jav <input type="checkbox"/> .java <input type="checkbox"/> .jcm <input type="checkbox"/> .js <input type="checkbox"/> .jse <input type="checkbox"/> .jsp <input type="checkbox"/> .jtk
ActiveX <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .alx <input type="checkbox"/> .apb <input type="checkbox"/> .axs <input type="checkbox"/> .ocx <input type="checkbox"/> .olb <input type="checkbox"/> .ole <input type="checkbox"/> .tlb <input type="checkbox"/> .viv <input type="checkbox"/> .vrm
Compression <input type="checkbox"/>	

Available settings are explained as follows:

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

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

3.6 CSM Profile

Content Security Management (CSM)

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

URL Content Filter

To provide an appropriate cyberspace to users, Vigor modem equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can

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

On the other hand, Vigor modem can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

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



3.6.1 URL Content Filter Profile

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

CSM >> URL Content Filter Profile

URL Content Filter Profile Table: | [Set to Factory Default](#) |

Profile	Name	Profile	Name
1.		5.	
2.		6.	
3.		7.	
4.		8.	

Administration Message (Max 255 characters) [Default Message](#)

```
<body><center><br><p>The requested Web page has been blocked by URL Content Filter.<p>Please contact your system administrator for further information.</center></body>
```

Each item is explained as follows:

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

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

Profile Index: 1

Profile Name:

Priority: Log:

1.URL Access Control

Enable URL Access Control Prevent web access from IP address

Action: Group/Object Selections:

2.Web Feature

Enable Restrict Web Feature

Action: Cookie Proxy Upload File Extension Profile:

Available settings are explained as follows:

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

	<div data-bbox="703 203 1147 376"> <input type="text" value="Both : Pass"/> <ul style="list-style-type: none"> Both : Pass Both : Block Either : URL Access Control First Either : Web Feature First </div>
Log	<p>None – There is no log file will be recorded for this profile.</p> <p>Pass – Only the log about Pass will be recorded in Syslog.</p> <p>Block – Only the log about Block will be recorded in Syslog.</p> <p>All – All the actions (Pass and Block) will be recorded in Syslog.</p> <div data-bbox="703 645 826 817"> <input type="text" value="None"/> <ul style="list-style-type: none"> None Pass Block All </div>
URL Access Control	<p>Enable URL Access Control - Check the box to activate URL Access Control. Note that the priority for URL Access Control is higher than Restrict Web Feature. If the web content match the setting set in URL Access Control, the modem will execute the action specified in this field and ignore the action specified under Restrict Web Feature.</p> <p>Prevent web access from IP address - Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.</p> <p>Action – This setting is available only when Either : URL Access Control First or Either : Web Feature First is selected. Pass - Allow accessing into the corresponding webpage with the keywords listed on the box below.</p> <p>Block - Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the keyword set here, it will be processed with reverse action.</p> <p>Action:</p> <div data-bbox="699 1615 818 1727"> <input type="text" value="Block"/> <ul style="list-style-type: none"> Pass Block </div> <p>Group/Object Selections – The Vigor modem provides several frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor modem will decline the connection request to the website whose URL string matched to any user-defined keyword. It</p>

should be noticed that the more simplified the blocking keyword list is, the more efficiently the Vigor modem performs.

Object/Group Edit

<u>Keyword Object</u>	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or <u>Keyword Group</u>	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None

OK Close

Web Feature

Enable Restrict Web Feature - Check this box to make the keyword being blocked or passed.

Action - This setting is available only when **Either: URL Access Control First** or **Either: Web Feature First** is selected. **Pass** allows accessing into the corresponding webpage with the keywords listed on the box below.

Pass - Allow accessing into the corresponding webpage with the keywords listed on the box below.

Block - Restrict accessing into the corresponding webpage with the keywords listed on the box below.

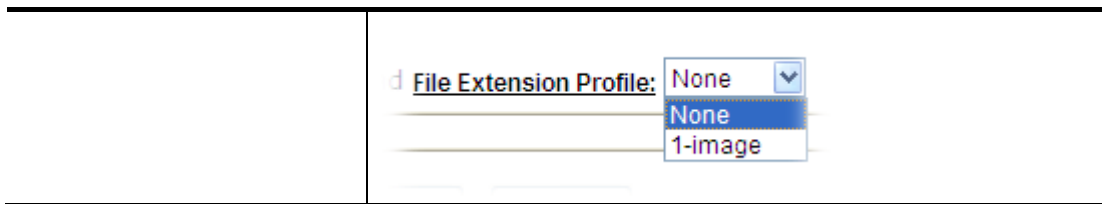
If the web pages do not match with the specified feature set here, it will be processed with reverse action.

Cookie - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy.

Proxy - Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages.

Upload - Check the box to block the file upload by way of web page.

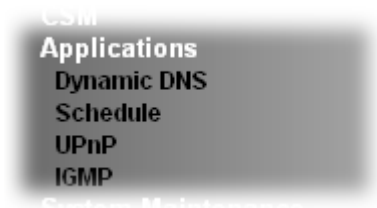
File Extension Profile - Choose one of the profiles that you configured in **Object Setting>> File Extension Objects** previously for passing or blocking the file downloading.



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

3.7 Applications

Below shows the menu items for Applications.



3.7.1 Dynamic DNS

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

Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The modem provides up to three accounts from three different DDNS service providers. Basically, Vigor modems are compatible with the DDNS services supplied by most popular DDNS service providers such as www.dyndns.org, www.no-ip.com, www.dtdns.com, www.changeip.com, www.dynamic-nameserver.com. You should visit their websites to register your own domain name for the modem.

Enable the Function and Add a Dynamic DNS Account

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

Applications >> Dynamic DNS Setup

| [Set to Factory Default](#) |

Enable Dynamic DNS Setup [View Log](#) [Force Update](#)

Auto-Update interval Min(s) (1~14400)

Accounts:

Index	Domain Name	Active
1.		x
2.		x
3.		x

Available settings are explained as follows:

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

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

Applications >> Dynamic DNS Setup >> Dynamic DNS Account Setup

Index : 1

Enable Dynamic DNS Account

Service Provider: ▼

Service Type: ▼

Domain Name: . ▼

Login Name: (max. 64 characters)

Password: (max. 23 characters)

Wildcards

Backup MX

Mail Extender:

Determine Real WAN IP: ▼

Available settings are explained as follows:

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

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

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

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

Disable the Function and Clear all Dynamic DNS Accounts

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

Delete a Dynamic DNS Account

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

3.7.2 Schedule

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

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

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

Applications >> Schedule

Schedule: | [Set to Factory Default](#) |

Index	Status	Index	Status
1.	x	9.	x
2.	x	10.	x
3.	x	11.	x
4.	x	12.	x
5.	x	13.	x
6.	x	14.	x
7.	x	15.	x
8.	x		

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

Available settings are explained as follows:

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

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

To add a schedule:

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

Applications >> Schedule

Index No. 1

Enable Schedule Setup

Start Date (yyyy-mm-dd) 2000 . 1 . 1

Start Time (hh:mm) 0 : 0

Duration Time (hh:mm) 0 : 0

Action Force On

Idle Timeout 0 minute(s).(max. 255, 0 for default)

How Often

Once

Weekdays

Sun Mon Tue Wed Thu Fri Sat

Available settings are explained as follows:

Item	Description
Enable Schedule Setup	Check to enable the schedule.

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

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

Example

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

Office

Hour:

(Force On)



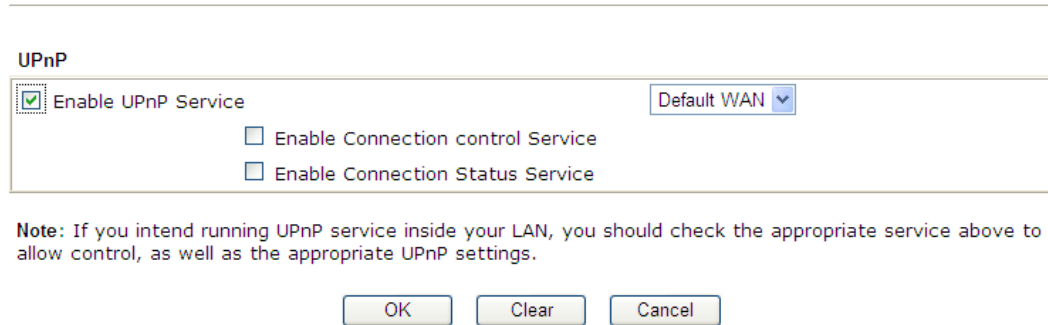
Mon - Sun 9:00 am to 6:00 pm

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

3.7.3 UPnP

The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT modems, the major feature of UPnP on the modem is "NAT Traversal". This enables applications inside the firewall to automatically open the ports that they need to pass through a modem. It is more reliable than requiring a modem to work out by itself which ports need to be opened. Further, the user does not have to manually set up port mappings or a DMZ. **UPnP is available on Windows XP** and the modem provide the associated support for MSN Messenger to allow full use of the voice, video and messaging features.

Applications >> UPnP



UPnP

Enable UPnP Service Default WAN ▾

Enable Connection control Service

Enable Connection Status Service

Note: If you intend running UPnP service inside your LAN, you should check the appropriate service above to allow control, as well as the appropriate UPnP settings.

OK Clear Cancel

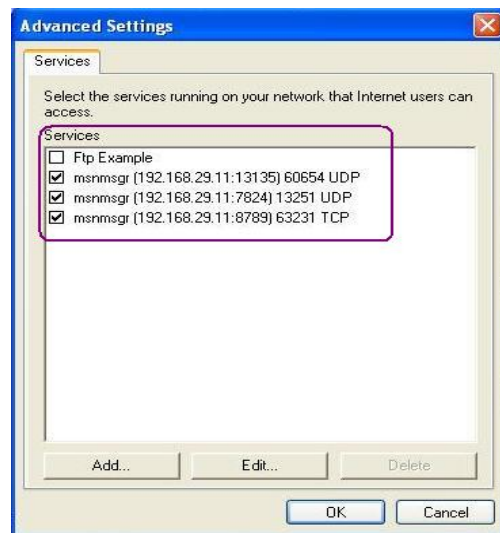
Available settings are explained as follows:

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

After setting **Enable UPNP Service** setting, an icon of **IP Broadband Connection on Modem** on Windows XP/Network Connections will appear. The connection status and control status will be able to be activated. The NAT Traversal of UPnP enables the multimedia features of your applications to operate. This has to manually set up port mappings or use other similar methods. The screenshots below show examples of this facility.



The UPnP facility on the modem enables UPnP aware applications such as MSN Messenger to discover what are behind a NAT modem. The application will also learn the external IP address and configure port mappings on the modem. Subsequently, such a facility forwards packets from the external ports of the modem to the internal ports used by the application.



The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software
 Enabling firewall applications on your PC may cause the UPnP function not working properly. This is because these applications will block the accessing ability of some network ports.

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

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

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

3.7.4 IGMP

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

Applications >> IGMP

IGMP

Enable IGMP Proxy WAN1 ▾

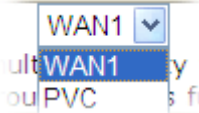
IGMP Proxy is to act as a multicast proxy for hosts on the LAN side. Enable IGMP Proxy, if you will access any multicast group. But this function take no effect when Bridge Mode is enabled.

OK Cancel

| Refresh |

Working Multicast Groups		
Index	Group ID	P1

Available settings are explained as follows:

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

3.8 System Maintenance

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

Below shows the menu items for System Maintenance.



3.8.1 System Status

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

System Status

Model Name : Vigor130
 Firmware Version : 3.7.1
 Build Date/Time : Mar 15 2013 17:02:13

LAN				
MAC Address	1st IP Address	1st Subnet Mask	DHCP Server	DNS
LAN 00-1D-AA-82-EB-F0	192.168.1.1	255.255.255.0	Yes	8.8.8.8

WAN				
Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1 Disconnected	00-1D-AA-82-EB-F1	PPPoA	---	---

IPv6			
Address	Scope	Internet Access Mode	
LAN FE80::21D:AAFF:FE82:EBF0/64	Link	---	

Available settings are explained as follows:

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

	<ul style="list-style-type: none"> - Display the subnet mask address of the LAN interface. <p>DHCP Server</p> <ul style="list-style-type: none"> - Display the current status of DHCP server of the LAN interface <p>DNS</p> <ul style="list-style-type: none"> - Display the assigned IP address of the primary DNS.
WAN	<p>Link Status</p> <ul style="list-style-type: none"> - Display current connection status. <p>MAC Address</p> <ul style="list-style-type: none"> - Display the MAC address of the WAN Interface. <p>Connection</p> <ul style="list-style-type: none"> - Display the connection type. <p>IP Address</p> <ul style="list-style-type: none"> - Display the IP address of the WAN interface. <p>Default Gateway</p> <ul style="list-style-type: none"> - Display the assigned IP address of the default gateway.
IPv6	<p>Address - Display the IPv6 address for LAN.</p> <p>Scope - Display the scope of IPv6 address. For example, IPv6 Link Local could only be used for direct IPv6 link. It can't be used for IPv6 internet.</p> <p>Internet Access Mode – Display the connection mode chosen for accessing into Internet.</p>

3.8.2 TR-069

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

System Maintenance >> TR-069 Setting

ACS and CPE Settings

ACS Server On: Internet ▼

ACS Server

URL:

Username:

Password:

CPE Client

Enable Disable

URL:

Port:

Username:

Password:

Periodic Inform Settings

Disable Enable

Interval Time: second(s)

STUN Settings

Disable Enable

Server Address:

Server Port:

Minimum Keep Alive Period: second(s)

Maximum Keep Alive Period: second(s)

Available settings are explained as follows:

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

	Or click Disable to close the mechanism of notification.
STUN Settings	<p>The default is Disable. If you click Enable, please type the relational settings listed below:</p> <p>Server IP – Type the IP address of the STUN server.</p> <p>Server Port – Type the port number of the STUN server.</p> <p>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”.</p> <p>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.</p>

3.8.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	<input type="text"/>
New Password	<input type="text"/>
Confirm Password	<input type="text"/>

Note: Password can contain only a-z A-Z 0-9 , ; : . " < > * + = \ | ? @ # ^ ! ()

Available settings are explained as follows:

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

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

3.8.4 Configuration Backup

Backup the Configuration

Follow the steps below to backup your configuration.

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

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration

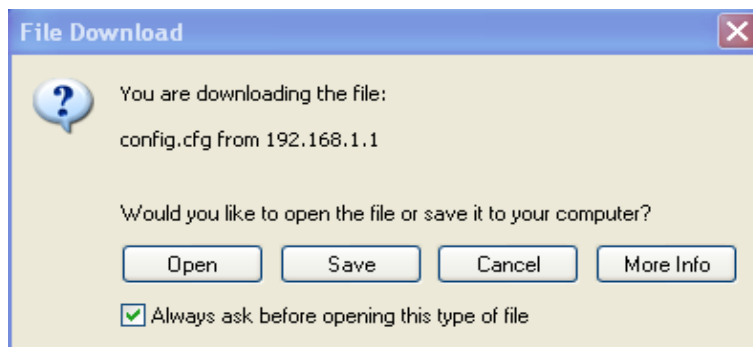
Select a configuration file.

Click Restore to upload the file.

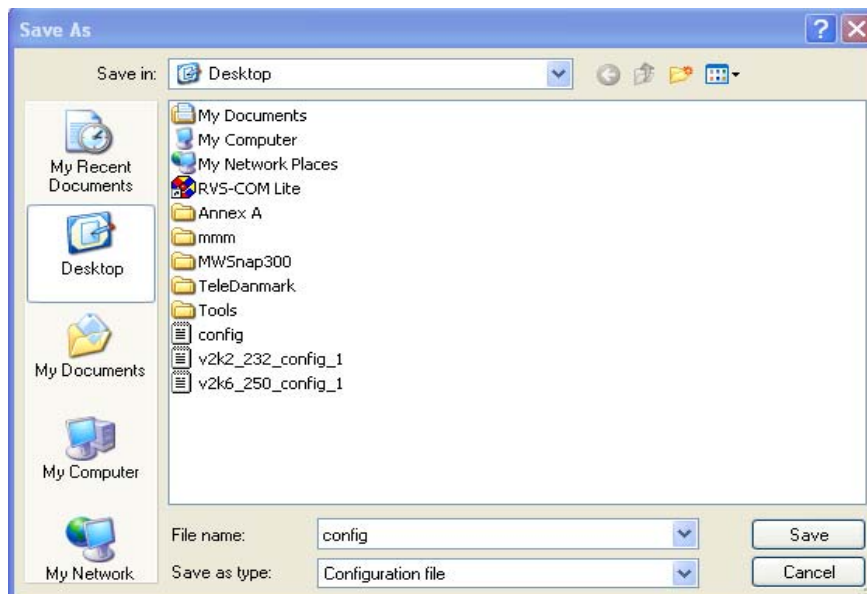
Backup

Click Backup to download current running configurations as a file.

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



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



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

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

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

Restore Configuration

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

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration
Select a configuration file. <input type="text"/> <input type="button" value="Browse.."/>
Click Restore to upload the file. <input type="button" value="Restore"/>
Backup
Click Backup to download current running configurations as a file. <input type="button" value="Backup"/> <input type="button" value="Cancel"/>

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

3.8.5 Syslog/Mail Alert

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

System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

<p>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Syslog Save to:</p> <p><input checked="" type="checkbox"/> Syslog Server</p> <p>Router Name <input style="width: 100%;" type="text"/></p> <p>Server IP Address <input style="width: 100%;" type="text"/></p> <p>Destination Port <input style="width: 100%;" type="text" value="514"/></p> <p>Enable syslog message:</p> <p><input checked="" type="checkbox"/> Firewall Log</p> <p><input checked="" type="checkbox"/> User Access Log</p> <p><input checked="" type="checkbox"/> WAN Log</p> <p><input checked="" type="checkbox"/> Router/DSL information</p>	<p>Mail Alert Setup</p> <p><input checked="" type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/></p> <p>SMTP Server <input style="width: 100%;" type="text"/></p> <p>SMTP Port <input style="width: 100%;" type="text" value="25"/></p> <p>Mail To <input style="width: 100%;" type="text"/></p> <p>Return-Path <input style="width: 100%;" type="text"/></p> <p><input type="checkbox"/> Authentication</p> <p>User Name <input style="width: 100%;" type="text"/></p> <p>Password <input style="width: 100%;" type="text"/></p> <p>Enable E-Mail Alert:</p> <p><input checked="" type="checkbox"/> DoS Attack</p>
--	--

Available settings are explained as follows:

Item	Description
SysLog Access Setup	<p>Enable - Check Enable to activate function of syslog.</p> <p>Syslog Save to – Check Syslog Server to save the log to Syslog server.</p>
Router Name	<p>Display the name for such modem configured in System Maintenance>>Management.</p> <p>If there is no name here, simply lick the link to access into System Maintenance>>Management to set the modem name.</p> <p>Server IP Address -The IP address of the Syslog server.</p> <p>Destination Port - Assign a port for the Syslog protocol.</p> <p>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.</p>
Mail Alert Setup	<p>Check “Enable” to activate function of mail alert.</p> <p>Send a test e-mail - Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not.</p> <p>SMTP Server - The IP address of the SMTP server.</p> <p>Mail To - Assign a mail address for sending mails out.</p> <p>Return-Path - Assign a path for receiving the mail from outside.</p>

Authentication - Check this box to activate this function while using e-mail application.

User Name - Type the user name for authentication.

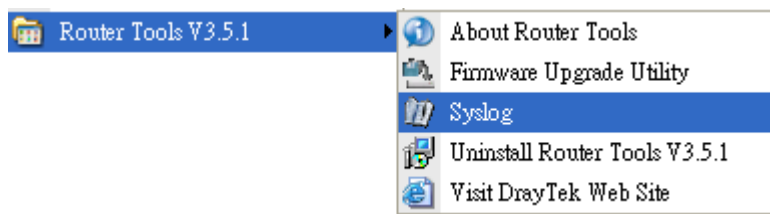
Password - Type the password for authentication.

Enable E-mail Alert - Check the box to send alert message to the e-mail box while the modem detects the item you specify here.

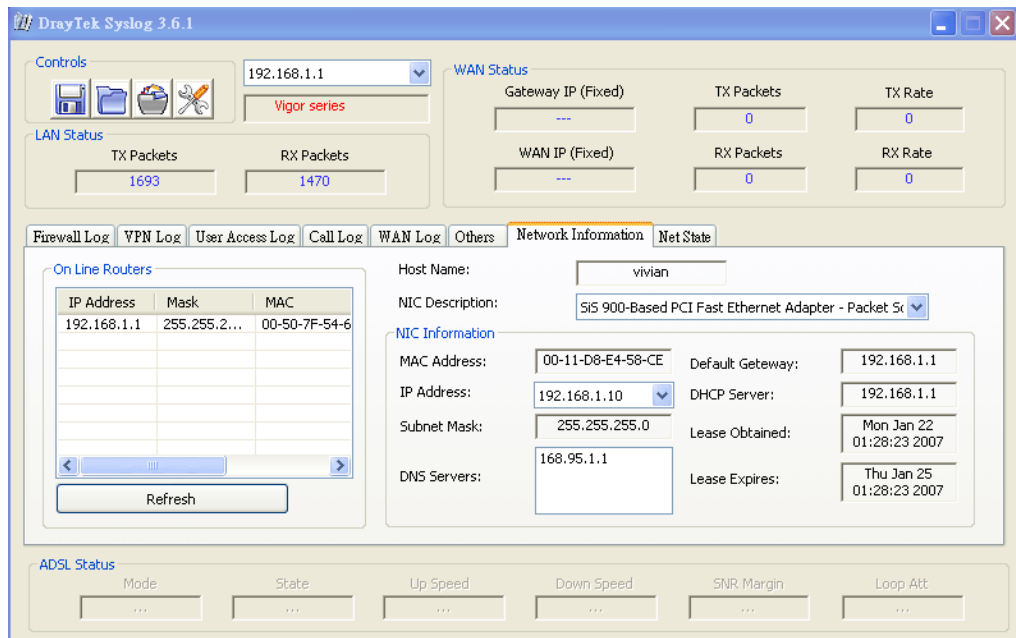
Click **OK** to save these settings.

For viewing the Syslog, please do the following:

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



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



3.8.6 Time and Date

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

System Maintenance >> Time and Date

Time Information

Current System Time: 2000 Jan 1 Sat 20 : 28 : 54 Inquire Time

Time Setup

Use Browser Time
 Use Internet Time

Time Server:

Priority:

Time Zone:

Enable Daylight Saving:

Automatically Update Interval:

Available settings are explained as follows:

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

Click **OK** to save these settings.

3.8.7 Management

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

The management pages for IPv4 and IPv6 protocols are different.

For IPv4

System Maintenance >> Management

IPv4 Management Setup	IPv6 Management Setup												
Router Name <input type="text"/> <hr/> Management Access Control <input type="checkbox"/> Allow management from the Internet <input type="checkbox"/> FTP Server <input checked="" type="checkbox"/> HTTP Server <input checked="" type="checkbox"/> HTTPS Server <input checked="" type="checkbox"/> Telnet Server <input type="checkbox"/> SSH Server <input checked="" type="checkbox"/> Disable PING from the Internet <hr/> Access List <table border="1"> <thead> <tr> <th>List</th> <th>IP</th> <th>Subnet Mask</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>2</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>3</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>	List	IP	Subnet Mask	1	<input type="text"/>	<input type="text"/>	2	<input type="text"/>	<input type="text"/>	3	<input type="text"/>	<input type="text"/>	Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports Telnet Port <input type="text" value="23"/> (Default: 23) HTTP Port <input type="text" value="80"/> (Default: 80) HTTPS Port <input type="text" value="443"/> (Default: 443) FTP Port <input type="text" value="21"/> (Default: 21) SSH Port <input type="text" value="22"/> (Default: 22) <hr/> SNMP Setup <input type="checkbox"/> Enable SNMP Agent Get Community <input type="text" value="public"/> Set Community <input type="text" value="private"/> Manager Host IP <input type="text"/> Trap Community <input type="text" value="public"/> Notification Host IP <input type="text"/> Trap Timeout <input type="text" value="10"/> seconds
List	IP	Subnet Mask											
1	<input type="text"/>	<input type="text"/>											
2	<input type="text"/>	<input type="text"/>											
3	<input type="text"/>	<input type="text"/>											

OK

Available settings are explained as follows:

Item	Description
Router Name	Type in the modem name provided by ISP.
Management Access Control	<p>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.</p> <p>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.</p>
Access List	<p>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.</p> <p>List IP - Indicate an IP address allowed to login to the modem.</p> <p>Subnet Mask - Represent a subnet mask allowed to login to the modem.</p>
Management Port Setup	User Defined Ports - Check to specify user-defined port numbers for the Telnet, HTTP and FTP servers.

	Default Ports - Check to use standard port numbers for the Telnet and HTTP servers.
SNMP	<p>Enable SNMP Agent - Check it to enable this function..</p> <p>Get Community - Set the name for getting community by typing a proper character. The default setting is public.</p> <p>Set Community - Set community by typing a proper name. The default setting is private.</p> <p>Manager Host IP - Set one host as the manager to execute SNMP function. Please type in IPv4 address to specify certain host.</p> <p>Trap Community - Set trap community by typing a proper name. The default setting is public.</p> <p>Notification Host IP - Set the IPv4 address of the host that will receive the trap community.</p> <p>Trap Timeout - The default setting is 10 seconds.</p>

For IPv6

System Maintenance >> Management

IPv4 Management Setup	IPv6 Management Setup
<p>Management Access Control</p> <p>Allow management from the Internet</p> <p><input type="checkbox"/> Telnet Server (Port : 23)</p> <p><input type="checkbox"/> HTTP Server (Port : 80)</p> <p><input type="checkbox"/> Enable PING from the Internet</p> <hr/> <p>Access List</p> <p>List IPv6 Address / Prefix Length</p> <p>1. <input type="text"/> / <input type="text" value="128"/></p> <p>2. <input type="text"/> / <input type="text" value="128"/></p> <p>3. <input type="text"/> / <input type="text" value="128"/></p> <p>Note : Telnet / Http server port is the same as IPv4.</p> <p style="text-align: center;"><input type="button" value="OK"/></p>	

Available settings are explained as follows:

Item	Description
Management Access Control	<p>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.</p> <p>Enable PING from the Internet - Check the checkbox to enable all PING packets from the Internet. For security issue, this function is disabled by default.</p>
Access List	<p>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.</p> <p>IPv6 Address /Prefix Length- Indicate the IP address(es)</p>

allowed to login to the modem.

3.8.8 Reboot System

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

System Maintenance >> Reboot System

Reboot System

Do you want to reboot your router ?

- Using current configuration
- Using factory default configuration

Reboot Now

Auto Reboot Time Schedule

Index(1-15) in Schedule Setup: , , ,

Note: Action and Idle Timeout settings will be ignored.

OK

Cancel

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

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

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

3.8.9 Firmware Upgrade

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

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

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

System Maintenance >> Firmware Upgrade

Web Firmware Upgrade

Select a firmware file.

Click Upgrade to upload the file.

TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.7.1


Firmware Upgrade Procedures:

1. Click "OK" to start the TFTP server.
2. Open the Firmware Upgrade Utility or other 3-party TFTP client software.
3. Check that the firmware filename is correct.
4. Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.
5. After the upgrade is complete, the TFTP server will automatically stop running.

Do you want to upgrade firmware ?

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

System Maintenance >> Firmware Upgrade

 TFTP server is running. Please execute a Firmware Upgrade Utility software to upgrade router's firmware. This server will be closed by itself when the firmware upgrading finished.

3.9 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor modem. Below shows the menu items for Diagnostics.



3.9.1 Dial-out Triggering

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

Diagnostics >> Dial-out Triggering

| [Refresh](#) |

Dial-out Triggered Packet Header

HEX Format:

```
00 00 00 00 00 00-00 00 00 00 00 00-00 00
```



```
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
```

Decoded Format:

```
0.0.0.0 -> 0.0.0.0
Pr 0 len 0 (0)
```

Available settings are explained as follows:

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

3.9.2 Routing Table

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

Diagnostics >> View Routing Table

Current Running Routing Table	IPv6 Routing Table	Refresh
Key: C - connected, S - static, R - RIP, * - default, ~ - private		
C~ 192.168.1.0/ 255.255.255.0 directly connected LAN		

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

Diagnostics >> View Routing Table

Current Running Routing Table	IPv6 Routing Table	Refresh		
Destination	Interface	Flags	Metric	Next Hop
FE80::/64	LAN	U	256	
FF00::/8	LAN	U	256	

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

3.9.3 ARP Cache Table

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

[Diagnostics >> View ARP Cache Table](#)

IP Address	MAC Address	Netbios Name
192.168.1.10	E0-CB-4E-DA-48-79	

Available settings are explained as follows:

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

3.9.4 IPv6 Neighbour Table

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

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

[Diagnostics >> View IPv6 Neighbour Table](#)

IPv6 Address	Mac Address	Interface	Status
FF02::1	33-33-00-00-00-01	LAN	CONF

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

3.9.5 DHCP Table

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

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

Diagnostics >> View DHCP Assigned IP Addresses

DHCP IP Assignment Table		DHCPv6 IP Assignment Table			Refresh
DHCP server: Running					
Index	IP Address	MAC Address	Leased Time	HOST ID	
1	192.168.1.10	E0-CB-4E-DA-48-79	71:51:19	carrie-0c7cb251	

Diagnostics >> View DHCP Assigned IP Addresses

DHCP IP Assignment Table		DHCPv6 IP Assignment Table		Refresh
DHCPv6 server binding client:				
Index	IPv6 Address	MAC Address	Leased Time	

Each item is explained as follows:

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

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

3.9.6 NAT Sessions Table

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

Diagnostics >> NAT Sessions Table

NAT Active Sessions Table | [Refresh](#) |

Private IP :Port	#Pseudo Port	Peer IP :Port	Interface

Available settings are explained as follows:

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

3.9.7 Ping Diagnosis

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

Diagnostics >> Ping Diagnosis

Ping Diagnosis

IPV4 IPV6
 Ping to: Host / IP IP Address:

 Result | [Clear](#) |

Diagnostics >> Ping Diagnosis

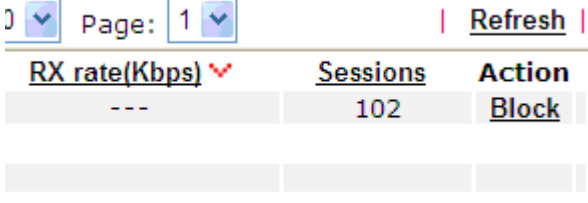
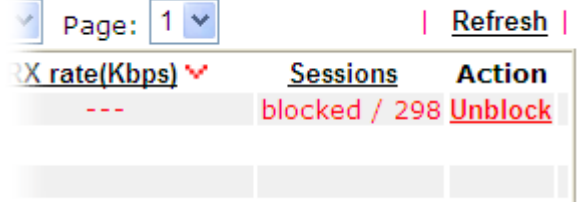
Ping Diagnosis

IPV4 IPV6
 Ping IPv6 Address:

 Result | [Clear](#) |

Available settings are explained as follows:

Item	Description
IPV4 /IPV6	Choose the interface for such function.
Ping through	Use the drop down list to choose the WAN interface that you want to ping through or choose Unspecified to be determined by the modem automatically.
Ping to	Use the drop down list to choose the destination that you want to ping.
IP Address	Type the IP address of the Host/IP that you want to ping.
Ping IPv6 Address	Type the IPv6 address that you want to ping.
Run	Click this button to start the ping work. The result will be displayed on the screen.

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

3.9.9 Trace Route

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

Diagnostics >> Trace Route

Trace Route

IPV4 IPV6

Protocol: ▾

Host / IP Address:

Result | [Clear](#) |

or

Diagnostics >> Trace Route

Trace Route

IPV4 IPV6

Trace Host / IP Address:

Result | [Clear](#) |

Available settings are explained as follows:

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

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

3.9.10 TSPC Status

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

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

Diagnostics >> IPv6 TSPC Status

WAN	Refresh
TSPC Disabled	

Available settings are explained as follows:

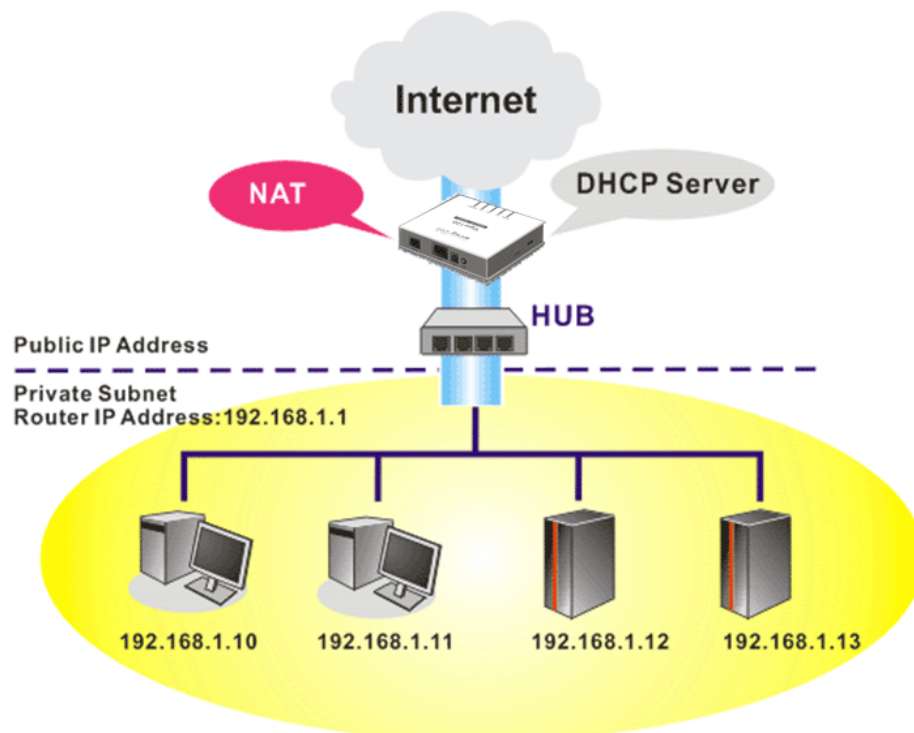
Item	Description
Refresh	Click this link to refresh this page manually.

4

Application and Examples

4.1 LAN – Created by Using NAT

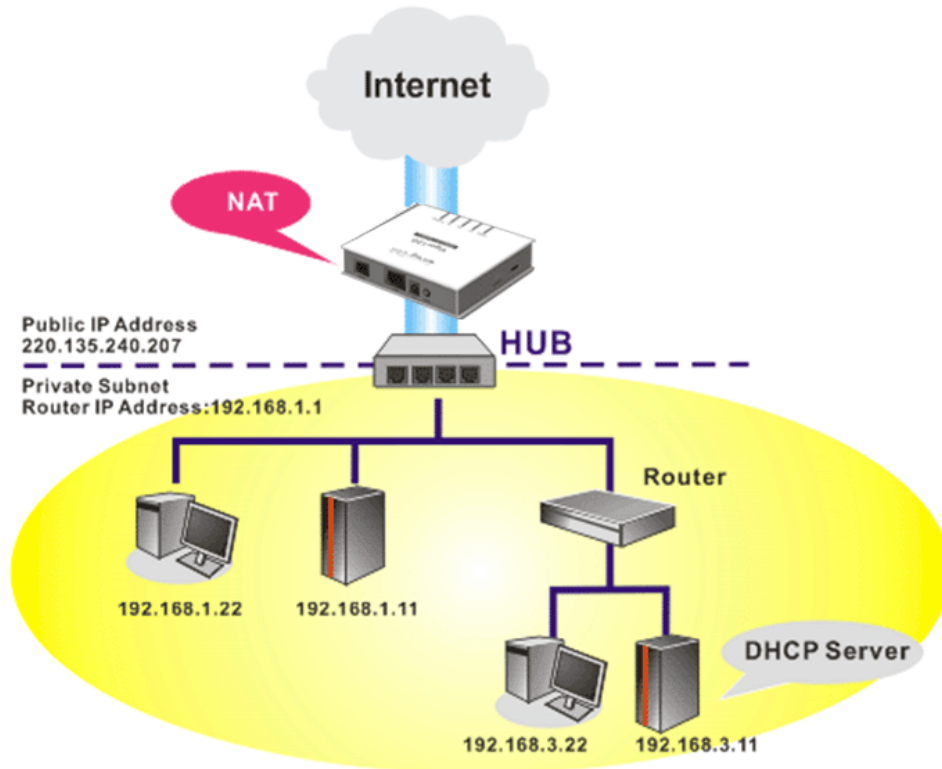
An example of default setting and the corresponding deployment are shown below. The default Vigor modem private IP address/Subnet Mask is 192.168.1.1/255.255.255.0. The built-in DHCP server is enabled so it assigns every local NATed host an IP address of 192.168.1.x starting from 192.168.1.10.



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

Ethernet TCP / IP and DHCP Setup	LAN 1 IPv6 Setup
LAN IP Network Configuration For NAT Usage 1st IP Address: 192.168.1.5 1st Subnet Mask: 255.255.255.0 For IP Routing Usage: <input type="radio"/> Enable <input checked="" type="radio"/> Disable 2nd IP Address: 192.168.2.1 2nd Subnet Mask: 255.255.255.0 2nd Subnet DHCP Server: <input type="button" value="2nd Subnet DHCP Server"/>	DHCP Server Configuration <input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server Relay Agent: <input type="radio"/> 1st Subnet <input type="radio"/> 2nd Subnet DHCP Server IP Address: <input type="text"/> Start IP Address: 192.168.1.10 IP Pool Counts: 150 Gateway IP Address: 192.168.1.5 Lease Time: 259200 (s) <input type="button" value="Advanced"/> You can configure DHCP options here.
RIP Protocol Control: <input type="button" value="Disable"/>	DNS Server IP Address Primary IP Address: <input type="text"/> Secondary IP Address: <input type="text"/> <input type="checkbox"/> Force router to use address for DNS

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



Ethernet TCP / IP and DHCP Setup	LAN 1 IPv6 Setup
LAN IP Network Configuration For NAT Usage 1st IP Address: <input type="text" value="192.168.1.5"/> 1st Subnet Mask: <input type="text" value="255.255.255.0"/> For IP Routing Usage: <input type="radio"/> Enable <input checked="" type="radio"/> Disable 2nd IP Address: <input type="text" value="192.168.2.1"/> 2nd Subnet Mask: <input type="text" value="255.255.255.0"/> <input type="button" value="2nd Subnet DHCP Server"/> RIP Protocol Control: <input type="text" value="Disable"/> <input type="button" value="v"/>	DHCP Server Configuration <input type="radio"/> Enable Server <input checked="" type="radio"/> Disable Server Relay Agent: <input type="radio"/> 1st Subnet <input type="radio"/> 2nd Subnet DHCP Server IP Address: <input type="text"/> Start IP Address: <input type="text" value="192.168.1.10"/> IP Pool Counts: <input type="text" value="150"/> Gateway IP Address: <input type="text" value="192.168.1.5"/> Lease Time: <input type="text" value="259200"/> (s) <input type="button" value="Advanced"/> You can configure DHCP options here. DNS Server IP Address Primary IP Address: <input type="text"/> Secondary IP Address: <input type="text"/> <input type="checkbox"/> Force router to use address for DNS

5

Trouble Shooting

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

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the modem from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

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



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

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

For Windows

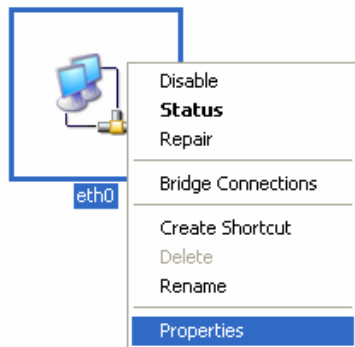


The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.draytek.com.

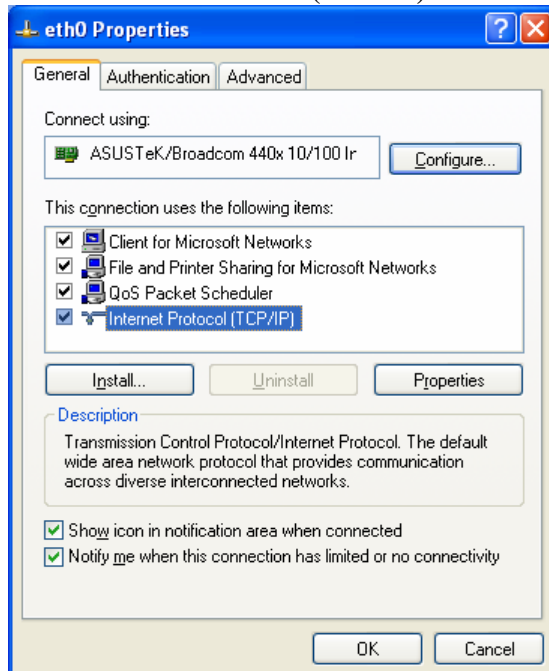
1. Go to **Control Panel** and then double-click on **Network Connections**.



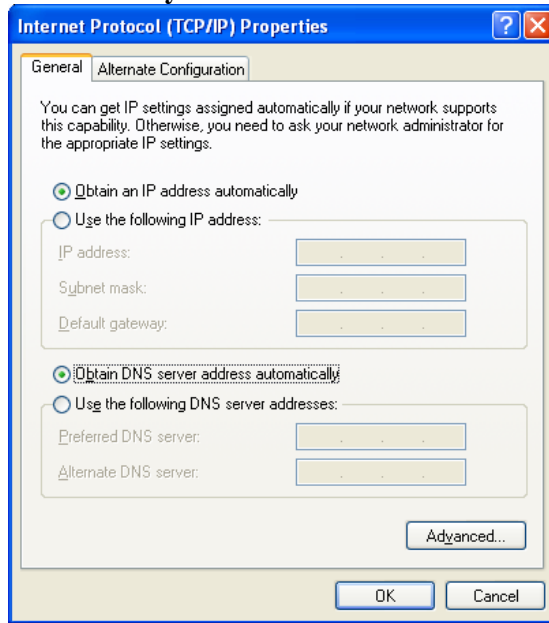
2. Right-click on **Local Area Connection** and click on **Properties**.



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

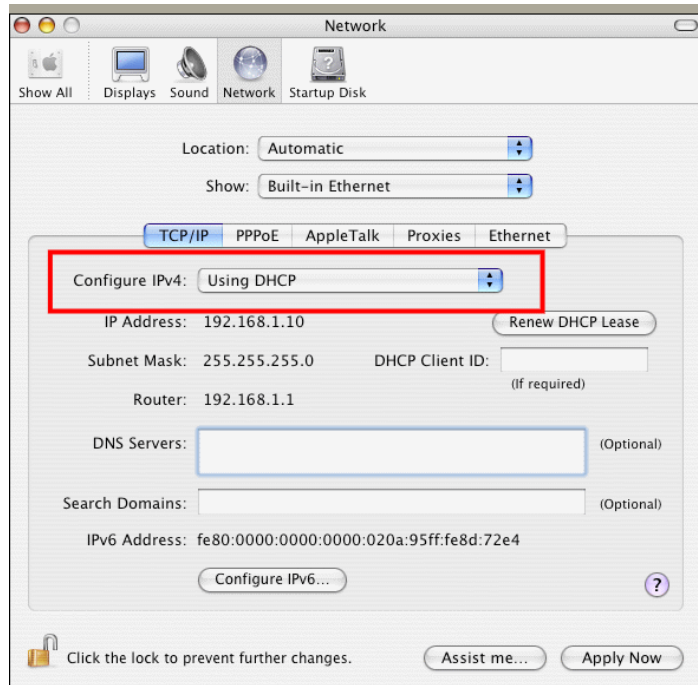


4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



For MacOs

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



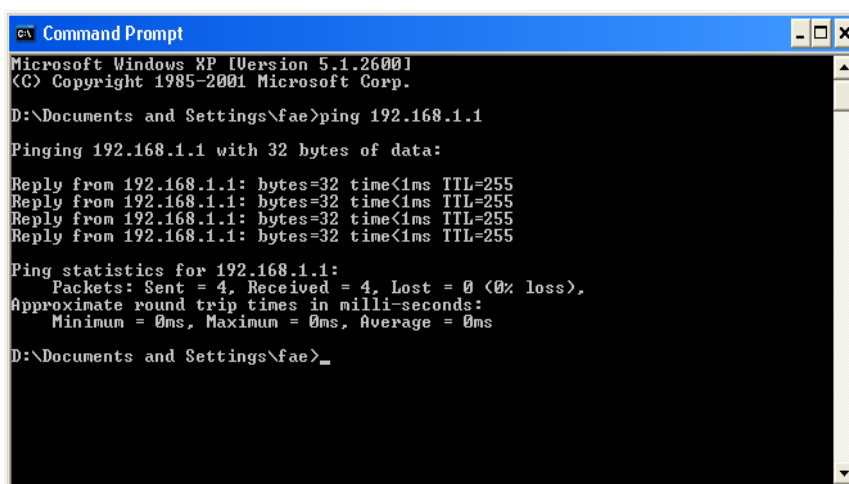
5.3 Pinging the Modem from Your Computer

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

Please follow the steps below to ping the modem correctly.

For Windows

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



```

C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_

```

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

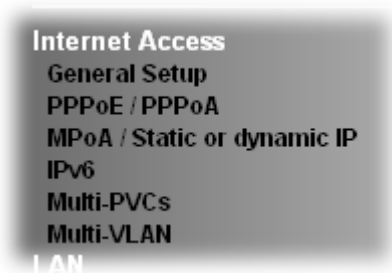
For MacOs (Terminal)

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

```
Terminal — bash — 80x24
Last login: Sat Jan 3 02:24:18 on ttty1
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$
```

5.4 Checking If the ISP Settings are OK or Not

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



5.5 Backing to Factory Default Setting If Necessary

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



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

Software Reset

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

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

Reboot System

Do you want to reboot your router ?

Using current configuration
 Using factory default configuration

Reboot Now

Auto Reboot Time Schedule

Index(1-15) in Schedule Setup: , , ,

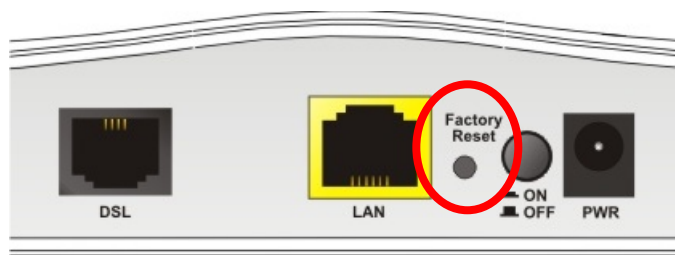
Note: Action and Idle Timeout settings will be ignored.

OK

Cancel

Hardware Reset

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



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

5.6 Contacting Your Dealer

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