



**Vigor120 Series  
ADSL2/2+ Modem  
User's Guide**

**Version: 1.0**

**Date: 2008/09/22**

## Copyright Information

### Copyright Declarations

Copyright 2008 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 by 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 County, HsinChu Industrial Park, Hsin-Chu, Taiwan 303

Product: Vigor120

DrayTek Corp. declares that Vigor120 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.



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

## Table of Contents

# 1

<b>Preface .....</b>	<b>1</b>
1.1 Web Configuration Buttons Explanation .....	1
1.2 LED Indicators and Connectors .....	2
1.3 Hardware Installation .....	4

# 2

<b>Basic Configuration .....</b>	<b>5</b>
2.1 Accessing Web Page .....	5
2.2 Changing Password .....	6
2.3 Quick Start Wizard .....	7
2.3.1 Adjusting Protocol/Encapsulation .....	7
2.3.2 PPPoE/PPPoA .....	9
2.3.3 1483 Bridged IP .....	10
2.3.4 1483 Routed IP .....	11
2.4 Online Status .....	12
2.5 Saving Configuration .....	14

# 3

<b>Advanced Configuration.....</b>	<b>15</b>
3.1 Internet Access.....	15
3.1.1 Basics of Internet Protocol (IP) Network.....	15
3.1.2 PPPoE/PPPoA.....	16
3.1.4 Multi-PVCs.....	21
3.2 LAN .....	24
3.2.1 Basics of LAN .....	24
3.2.2 General Setup.....	26
3.2.3 Static Route .....	27
3.3 NAT .....	30
3.3.1 Port Redirection .....	30
3.3.2 DMZ Host.....	33
3.3.3 Open Ports.....	35
3.4 Firewall.....	37
3.4.1 Basics for Firewall.....	37
3.4.2 General Setup.....	39
3.4.3 Filter Setup .....	40
3.4.4 DoS Defense .....	45
3.4.5 URL Content Filter .....	47
3.5 Objects Settings .....	50
3.5.1 IP Object .....	50
3.5.2 IP Group .....	51

3.5.3 Service Type Object .....	53
3.5.4 Service Type Group .....	54
3.6 Applications .....	55
3.6.1 Dynamic DNS .....	55
3.6.2 Schedule .....	57
3.6.3 UPnP .....	59
3.6.4 IGMP .....	62
3.7 System Maintenance .....	62
3.7.1 System Status .....	62
3.7.2 TR-069 .....	63
3.7.3 Administrator Password .....	65
3.7.4 Configuration Backup .....	65
3.7.5 Syslog/Mail Alert .....	67
3.7.6 Time and Date .....	68
3.7.7 Management .....	69
3.7.8 Reboot System .....	70
3.7.9 Firmware Upgrade .....	71
3.8 Diagnostics .....	72
3.8.1 Dial-out Trigger .....	72
3.8.2 Routing Table .....	73
3.8.3 ARP Cache Table .....	73
3.8.4 DHCP Table .....	74
3.8.5 NAT Sessions Table .....	74
3.8.6 Ping Diagnosis .....	75
3.8.7 Trace Route .....	76

## 4

### **Application and Examples .....77**

4.1 LAN – Created by Using NAT .....	77
4.2 Upgrade Firmware for Your Modem .....	79

## 5

### **Trouble Shooting .....83**

5.1 Checking If the Hardware Status Is OK or Not .....	83
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not .....	84
5.3 Pinging the Modem from Your Computer .....	86
5.4 Checking If the ISP Settings are OK or Not .....	87
5.5 Backing to Factory Default Setting If Necessary .....	88
5.6 Contacting Your Dealer .....	89

# 1


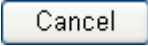
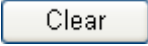
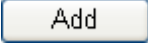
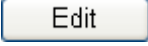
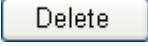
## Preface

Vigor120 Series is an ADSL modem. It integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

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.

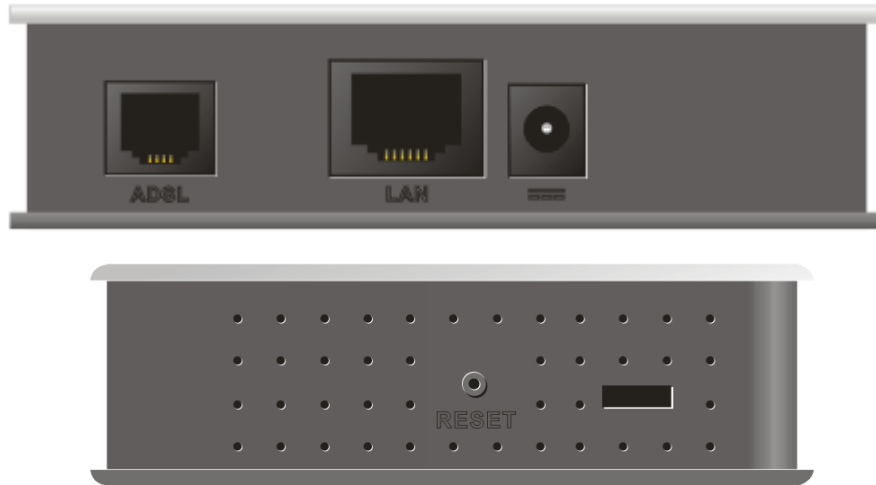
**Note:** For the other buttons shown on the web pages, please refer to Chapter 4 for detailed explanation.


## 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
Power	On	The modem is powered on.
	Off	The modem is powered off.
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).
DSL	On	DSL connection synchronized.
	Blinking	DSL connection is synchronizing.
INTERNET	On	Internet connection is established.
	Off	Internet connection is not established.
	Blinking	Data is transmitting (sending/receiving).



Interface	Description
ADSL	Connector for accessing the Internet through ADSL 2+.
LAN	Connector for local networked devices.
	Connector for a power adapter.
RESET	Restore the default settings. Usage: Turn on the router. Press the button and keep for more than 10 seconds. Then the router will restart with the factory default configuration.



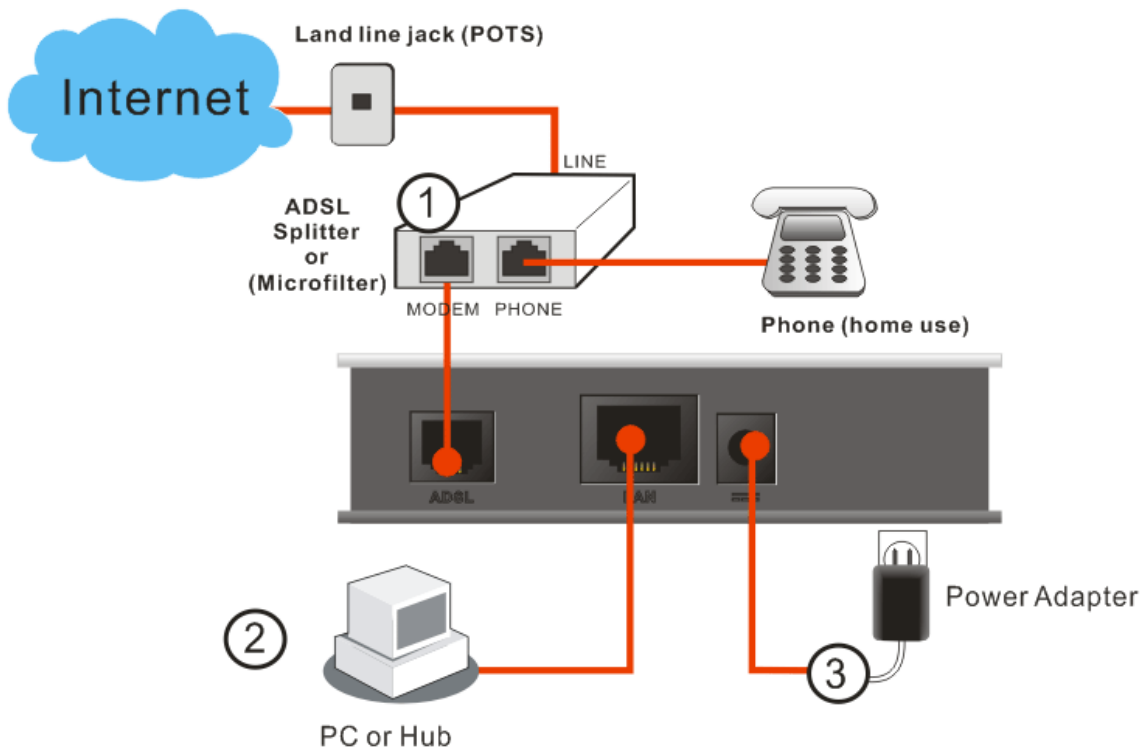
## 1.3 Hardware Installation

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 ADSL splitter with an ADSL line cable.
2. Connect the LAN port to your computer with a RJ-45 cable.
3. Connect one end of the power adapter to the Power port of this device. Connect the other end to the wall outlet of electricity.
4. Power on the modem.
5. Check the **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**. The following window will be open to ask for username and password.



3. Do not type any word on the window and click **Login** for the simple web pages for configuration.

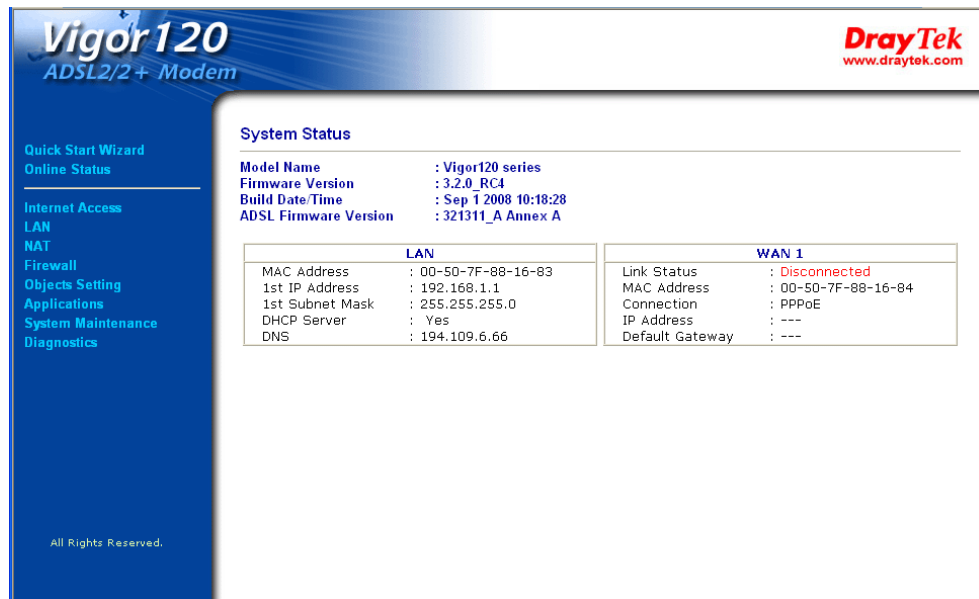


**Notice:** If you fail to access to the web configuration, please go to “Trouble Shooting” for detecting and solving your problem.

## 2.2 Changing Password

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

1. Open a web browser on your PC and type **http://192.168.1.1**. A pop-up window will open to ask for username and password.
2. Do not type any word (both username and password are Null for user operation) on the window and click **Login** on the window.
3. Now, the **Main Screen** will appear.



**Note:** The home page will change slightly in accordance with the type of the modem you have.

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

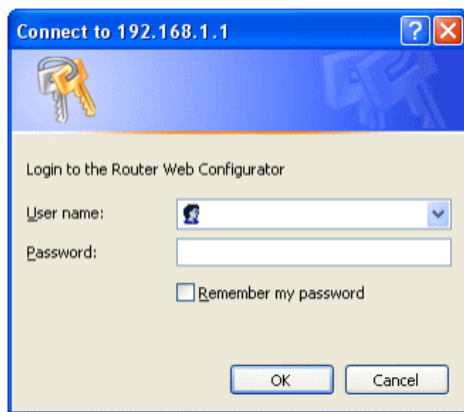
### System Maintenance >> Administrator Password Setup

#### Administrator Password

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

OK

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



## 2.3 Quick Start Wizard



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

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

New Password

Confirm Password

< Back   Next >   Finish   Cancel

In the **Quick Start Wizard**, you can configure the modem to access the Internet with different protocol/modes such as **PPPoE, PPPoA, Bridged IP, or Routed IP**. The modem supports the

### 2.3.1 Adjusting Protocol/Encapsulation

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

## Quick Start Wizard

### Connect to Internet

VPI: 0 [Auto detect]

VCI: 33

Protocol / Encapsulation: PPPoE LLC/SNAP

Fixed IP

IP Address

Subnet Mask

Default Gateway

Primary DNS

Second DNS

< Back   Next >   Finish   Cancel

Now, 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.

**VPI** Stands for **Virtual Path Identifier**. It is an 8-bit header inside each ATM cell that indicates where the cell should be routed. The ATM, is a method of sending data in small packets of fixed sizes. It is used for transferring data to client computers.

**VCI** Stands for **Virtual Channel Identifier**. It is a 16-bit field inside ATM cell's header that indicates the cell's next destination as it travels through the network. A virtual channel is a logical connection between two end devices on the network.

**Protocol/Encapsulation** Select an IP mode for this WAN interface. There are several available modes for Internet access such as **PPPoE**, **PPPoA**, **Bridged IP** and **Routed IP**.

Protocol / Encapsulation: 1483 Bridged IP LLC

Fixed IP

IP Address

Subnet Mask

Default Gateway

Primary DNS

**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 **Routed IP** and **Bridged IP**.

**Default Gateway** Assign an IP address to the gateway for the protocol of **Routed IP** and **Bridged IP**.

**Primary DNS** Assign an IP address to the primary DNS.

## Second DNS

Assign an IP address to the secondary DNS.

### 2.3.2 PPPoE/PPPoA

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

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. The following page will be shown:

[Quick Start Wizard](#)

#### Set PPPoE / PPPoA

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

**User Name** Assign a specific valid user name provided by the ISP.

**Password** Assign a valid password provided by the ISP.

**Confirm Password** Retype the password.

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

## Quick Start Wizard

Please confirm your settings:

VPI:	0
VCI:	33
Protocol / Encapsulation:	PPPoE / LLC
Fixed IP:	No
Primary DNS:	
Secondary DNS:	

< Back   Next >   Finish   Cancel

Click **Finish**. Then, the system status of this protocol will be shown.

### 2.3.3 1483 Bridged IP

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

#### Quick Start Wizard

Connect to Internet

VPI	<input type="text" value="0"/>	<input type="button" value="Auto detect"/>
VCI	<input type="text" value="35"/>	
Protocol / Encapsulation	<input type="text" value="1483 Bridged IP LLC"/> ▼	
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	<input type="text"/>	
Second DNS	<input type="text"/>	

< Back   Next >   Finish   Cancel

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

## Quick Start Wizard

### Please confirm your settings:

VPI:	0
VCI:	33
Protocol / Encapsulation:	1483 Bridge LLC
Fixed IP:	No
Primary DNS:	
Secondary DNS:	

Click **Finish**. Then, the system status of this protocol will be shown.

## 2.3.4 1483 Routed IP

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

### Quick Start Wizard

#### Connect to Internet

VPI	<input type="text" value="0"/>	<input type="button" value=" Auto detect"/>
VCI	<input type="text" value="33"/>	
Protocol / Encapsulation	<input type="text" value="1483 Routed IP LLC"/> ▼	
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	<input type="text"/>	
Second DNS	<input type="text"/>	

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



## Quick Start Wizard

Please confirm your settings:

VPI:	0
VCI:	33
Protocol / Encapsulation:	1483 Route LLC
Fixed IP:	No
Primary DNS:	
Secondary DNS:	

Click **Finish**. Then, the system status of this protocol will be shown.

## 2.4 Online Status

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.

### Online status for PPPoE

#### Online Status

System Status		System Uptime: 0:3:34				
Primary	Secondary					
<b>LAN Status</b>	Primary DNS: 168.95.192.1		Secondary DNS: 168.95.1.1			
IP Address	TX Packets	RX Packets				
192.168.1.1	573	534				
<b>WAN 1 Status</b>					<a href="#">&gt;&gt; Dial PPPoE</a>	
Enable	Line	Name	Mode	Up Time		
Yes	ADSL		PPPoE	0:01:29		
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
61.230.203.119	61.230.192.254	38	15	39	40	
Message [ PPP Shutdown ]						
<b>ADSL Information</b>	( ADSL Firmware Version: 321311_A)					
ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks		
	63	353	6	1		
<b>ADSL Status</b>	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.DMT	SHOWTIME	256000	2048000	23	31

## Online status for Static IP

### Online Status

System Status		System Uptime: 0:3:34				
Primary		Secondary				
LAN Status		Primary DNS: 194.109.6.66			Secondary DNS: 168.95.1.1	
IP Address		TX Packets		RX Packets		
192.168.1.1		573		534		
WAN 1 Status		>> <a href="#">Dial PPPoE</a>				
Enable	Line	Name	Mode	Up Time		
Yes	ADSL		Static IP	0:00:28		
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
192.168.33.12	192.168.33.1	2	4	1	9	
ADSL Information		( ADSL Firmware Version: 321311_A)				
ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks		
	6	9	0	18		
ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	ADSL2+ (G.992.5)	SHOWTIME	1026000	22215000	6	0

## Online status for DHCP

### Online Status

System Status		System Uptime: 0:3:34				
Primary		Secondary				
LAN Status		Primary DNS: 192.168.33.1			Secondary DNS: 168.95.1.1	
IP Address		TX Packets		RX Packets		
192.168.1.1		573		534		
WAN 1 Status		>> <a href="#">Dial PPPoE</a>				
Enable	Line	Name	Mode	Up Time		
Yes	ADSL		DHCP Client	0:00:28		
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
192.168.33.12	192.168.33.1	1	9	1	35	
ADSL Information		( ADSL Firmware Version: 321311_A)				
ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks		
	19	21	0	8		
ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	ADSL2+ (G.992.5)	SHOWTIME	1036000	22448000	6	0

Detailed explanation is shown below:

**Primary DNS** Displays the IP address of the primary DNS.

**Secondary DNS** Displays the IP address of the secondary DNS.

#### LAN Status

**IP Address** Displays the IP address of the LAN interface.

**TX Packets** Displays the total transmitted packets at the LAN interface.

**RX Packets** Displays the total number of received packets at the LAN interface.

#### WAN1 Status

**Line** Displays the physical connection (Ethernet) of this interface.

<b>Name</b>	Displays the name set in WAN1/WAN web page.
<b>Mode</b>	Displays the type of WAN connection (e.g., PPPoE).
<b>Up Time</b>	Displays the total uptime of the interface.
<b>IP</b>	Displays the IP address of the WAN interface.
<b>GW IP</b>	Displays the IP address of the default gateway.
<b>TX Packets</b>	Displays the total transmitted packets at the WAN interface.
<b>TX Rate</b>	Displays the speed of transmitted octets at the WAN interface.
<b>RX Packets</b>	Displays the total number of received packets at the WAN interface.
<b>RX Rate</b>	Displays the speed of received octets at the WAN interface.

**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 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.

# 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. Be aware that “Admin mode” will be displayed on the bottom left side.

The screenshot displays the web interface for a Vigor120 ADSL2/2+ Modem. The interface has a blue header with the product name and logo, and a left-hand navigation menu. The main content area shows the 'System Status' page, which includes a table of system information and two sub-tables for LAN and WAN 1 settings.

System Status	
Model Name	: Vigor120 series
Firmware Version	: 3.2.0_RC4
Build Date/Time	: Sep 1 2008 10:18:28
ADSL Firmware Version	: 321311_A Annex A

LAN	
MAC Address	: 00-50-7F-88-16-83
1st IP Address	: 192.168.1.1
1st Subnet Mask	: 255.255.255.0
DHCP Server	: Yes
DNS	: 194.109.6.66

WAN 1	
Link Status	: <b>Disconnected</b>
MAC Address	: 00-50-7F-88-16-84
Connection	: PPPoE
IP Address	: ---
Default Gateway	: ---

### 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 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.

PPPoE / PPPoA Client Mode

<b>PPPoE/PPPoA Client</b> <input checked="" type="radio"/> Enable <input type="radio"/> Disable		<b>ISP Access Setup</b>	
<b>DSL Modem Settings</b>		ISP Name: <input type="text"/>	
VPI	<input type="text" value="0"/>	Username: <input type="text" value="84005755@hinet.net"/>	
VCI	<input type="text" value="33"/>	Password: <input type="password" value="••••••••"/>	
Encapsulating Type	<input type="text" value="LLC/SNAP"/>	PPP Authentication: <input type="text" value="PAP or CHAP"/>	
Protocol	<input type="text" value="PPPoE"/>	<input checked="" type="checkbox"/> Always On	
Modulation	<input type="text" value="Multimode"/>	Idle Timeout: <input type="text" value="-1"/> second(s)	
<b>PPPoE Pass-through</b>		<b>IP Address From ISP</b> <input type="text" value="WAN IP Alias"/>	
<input type="checkbox"/> For Wired LAN		Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)	
<b>Note:</b> 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.		Fixed IP Address: <input type="text"/>	
		<input checked="" type="radio"/> Default MAC Address	
		<input type="radio"/> Specify a MAC Address	
		MAC Address: <input type="text" value="00"/> . <input type="text" value="50"/> . <input type="text" value="7F"/> : <input type="text" value="12"/> : <input type="text" value="34"/> : <input type="text" value="57"/>	
		Index(1-15) in <a href="#">Schedule</a> Setup:	
		=> <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>	

OK

**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**. **Select M-PVCs Channel** means no selection will be chosen.  
**VPI** - Type in the value provided by ISP.  
**VCI** - Type in the value provided by ISP.  
**Encapsulating Type** - Drop down the list to choose the type provided by ISP.  
**Protocol** - Drop down the list to choose the one provided by ISP. If you have already used **Quick Start Wizard** to set the protocol, then it is not necessary for you to change any settings in this group.

**PPPoE Pass-through**

The modem offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor modem. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction.  
**For Wired LAN** – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet. However, if this box is checked in PPPoA protocol, only PPPoE clients on the LAN will be served and only one session is allowed.

**ISP Access Setup**

Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If

you want to connect to Internet all the time, you can check **Always On**.

**Username** – Type in the username provided by ISP in this field.

**Password** – Type in the password provided by ISP in this field.

**PPP Authentication** – Select **PAP only** or **PAP or CHAP** for PPP.

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

### IP Address From ISP

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

**WAN IP Alias** - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	<input checked="" type="checkbox"/>	---	<input checked="" type="checkbox"/>
2.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
3.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
4.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
5.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
6.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
7.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
8.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>

OK Clear All Close

**Fixed IP** – Click **Yes** to use this function and type in a fixed IP address in the box of **Fixed IP Address**.

**Default MAC Address** – You can use **Default MAC Address** or specify another MAC address by typing on the boxes of MAC Address for the modem.

**Specify a MAC Address** – Type the MAC address for the modem manually.

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

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

## MPoA

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

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

[Internet Access >> MPoA \(RFC1483/2684\)](#)

**MPoA (RFC1483/2684) Mode**

MPoA (RFC1483/2684)  Enable  Disable

---

**DSL Modem Settings**

Multi-PVC channel:

Encapsulation:

VPI:

VCI:

Modulation:

---

**RIP Protocol**

Enable RIP

---

**Bridge Mode**

Enable Bridge Mode

**WAN IP Network Settings**

Obtain an IP address automatically

Router Name:  \*

Domain Name:  \*

\*: Required for some ISPs

Specify an IP address WAN IP Alias

IP Address:

Subnet Mask:

Gateway IP Address:

---

Default MAC Address

Specify a MAC Address

MAC Address:

---

**DNS Server IP Address**

Primary IP Address:

Secondary IP Address:

**MPoA (RFC1483/2684)** Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.

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

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

**Bridge Mode** If you choose **Bridged IP** as the protocol, you can check this box to invoke the function. The modem will work as a bridge modem.

**WAN IP Network** This group allows you to obtain an IP address automatically and



## Settings

allows you type in IP address manually.

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

**Modem Name** – Type in the modem name provided by ISP.

**Domain Name** – Type in the domain name that you have assigned.

**Specify an IP address** – Click this radio button to specify some data.

**WAN IP Alias** - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	<input checked="" type="checkbox"/>	---	<input checked="" type="checkbox"/>
2.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
3.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
4.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
5.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
6.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
7.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
8.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>

OK Clear All Close

**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.

### 3.1.4 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.

[WAN >> Multi-PVCs](#)

**Multi-PVCs**

General		ATM QoS				
Channel	Enable	VPI	VCI	QoS Type	Protocol	Encapsulation
1.	<input checked="" type="checkbox"/>	0	33	UBR	PPPoE	LLC/SNAP
2.	<input checked="" type="checkbox"/>	0	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

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

OK Clear Cancel

#### 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.

##### QoS Type

UBR  
 UBR  
 CBR  
 ABR  
 nrtVBR  
 rtVBR

#### Protocol

Select a proper protocol for this channel.

##### Protocol

PPPoE  
 PPPoA  
 PPPoE  
 MPoA

## Encapsulation

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

The image shows two dropdown menus for selecting encapsulation types. The first menu, labeled 'Encapsulation', has three options: 'VC MUX', 'VC MUX', and 'LLC/SNAP'. The second menu, also labeled 'Encapsulation', has six options: '1483 Route IP LLC', '1483 Bridged IP LLC', '1483 Route IP LLC', '1483 Bridged IP VC-Mux', '1483 Routed IP VC-Mux(IPoA)', and '1483 Bridged IP(IPoE)'. The '1483 Route IP LLC' option in the second menu is highlighted.

WAN link for Channel 3, 4 are provided for modem-borne application such as TR069 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 >> Multi-PVCs >> PVC Channel 3

The screenshot shows a configuration window titled 'WAN for Router-borne Application: Management'. It has radio buttons for 'Enable' and 'Disable', with 'Disable' selected. Below this is the 'DSL Modem Settings' section with fields for VPI (1), VCI (43), QoS Type (UBR), Protocol (PPPoA), and Encapsulation (VC MUX). The 'PPPoE/PPPoA Client' section includes 'ISP Access Setup' with fields for ISP Name, Username, Password, and PPP Authentication (PAP or CHAP), and an 'IP Address From ISP' section with radio buttons for 'Yes' and 'No (Dynamic IP)'. The 'MPoA (RFC1483/2684)' section has radio buttons for 'Obtain an IP address automatically' and 'Specify an IP address', with fields for Router Name, Domain Name, IP Address, Subnet Mask, Gateway IP Address, Primary IP Address, and Secondary IP Address. 'OK' and 'Cancel' buttons are at the bottom.

## ATM QoS

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

Multi-PVCs

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

Note: 1.Set 0 means default value.  
 2.PCR(max) = ADSL Up Speed / 53 / 8.

OK Clear Cancel

**QoS Type**

Select a proper QoS type for the channel according to the information that your ISP provides.

**QoS Type**

UBR

- UBR
- CBR
- ABR
- nrtVBR
- rtVBR

**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.

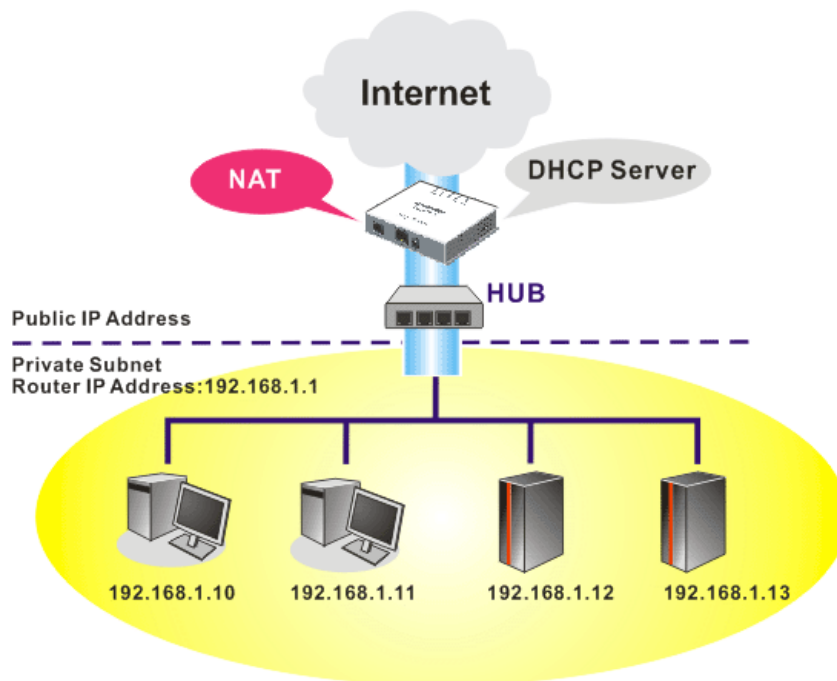
## 3.2 LAN

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

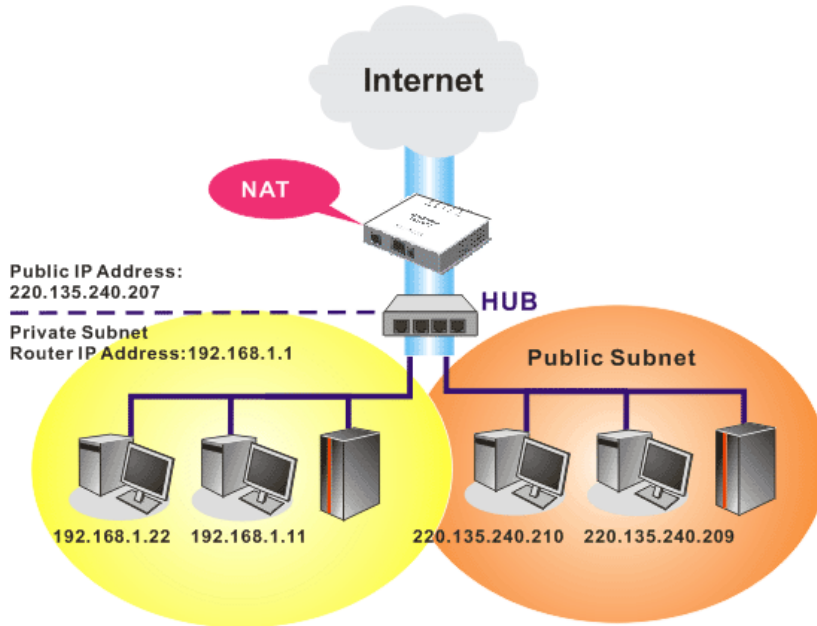


### 3.2.1 Basics of LAN

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



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

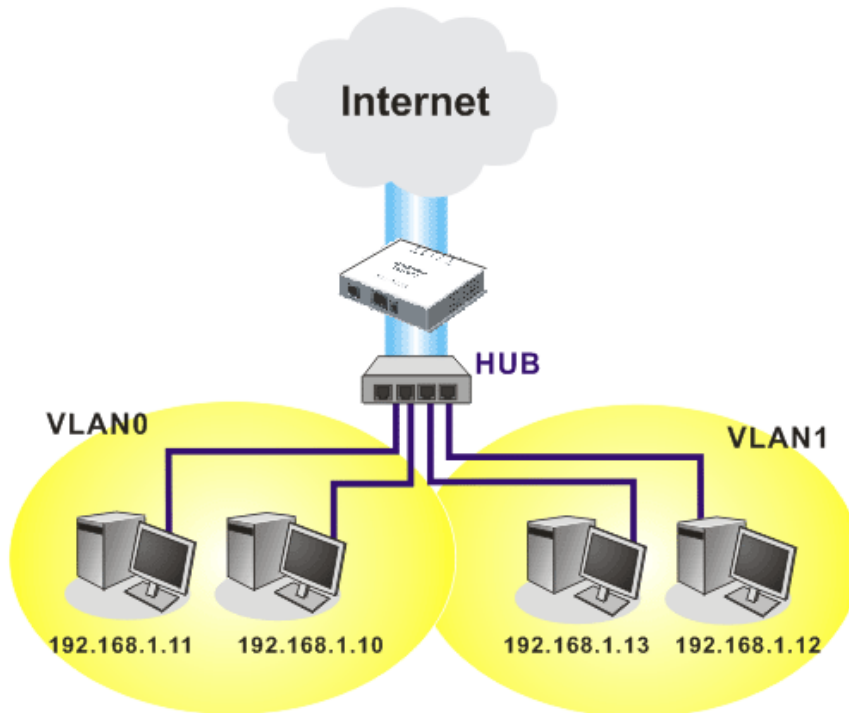


### What is Routing Information Protocol (RIP)

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

### What is Static Route

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



## 4.2.2 General Setup

This page provides you the general settings for LAN.

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

[LAN >> General Setup](#)

### Ethernet TCP / IP and DHCP Setup

LAN IP Network Configuration		DHCP Server Configuration	
For NAT Usage		<input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server	
IP Address	<input type="text" value="192.168.1.1"/>	Start IP Address	<input type="text" value="192.168.1.10"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>	IP Pool Counts	<input type="text" value="50"/>
		Gateway IP Address	<input type="text" value="192.168.1.1"/>
		<b>DNS Server IP Address</b>	
		Primary IP Address	<input type="text"/>
		Secondary IP Address	<input type="text"/>

OK

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

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

**DHCP Server Configuration** DHCP stands for Dynamic Host Configuration Protocol. The modem by factory default acts a DHCP server for your network so it automatically 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 Modem's, you can let Relay Agent help you to redirect the DHCP request to the specified location.

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

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

**Start IP Address** - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your 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.

**DNS Server Configuration** DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS

server converts the user-friendly name into its equivalent IP address.

**Primary IP Address** - You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default DNS Server IP address: 194.109.6.66 to this field.

**Secondary IP Address** - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.

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

[Online Status](#)

System Status		System Uptime: 0:3:34	
Primary	Secondary		
LAN Status	Primary DNS: 194.109.6.66	Secondary DNS: 168.95.1.1	
IP Address	TX Packets	RX Packets	
192.168.1.1	573	534	

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

If the IP address of a domain name is already in the DNS cache, the modem will resolve the domain name immediately. Otherwise, the modem forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.

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

### 3.2.3 Static Route

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

[LAN >> Static Route Setup](#)

Static Route Configuration			<a href="#">Set to Factory Default</a>	<a href="#">View Routing Table</a>	
Index	Destination Address	Status	Index	Destination Address	Status
<a href="#">1.</a>	???	?	<a href="#">6.</a>	???	?
<a href="#">2.</a>	???	?	<a href="#">7.</a>	???	?
<a href="#">3.</a>	???	?	<a href="#">8.</a>	???	?
<a href="#">4.</a>	???	?	<a href="#">9.</a>	???	?
<a href="#">5.</a>	???	?	<a href="#">10.</a>	???	?

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

- 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 profiles.



## Viewing Routing Table

Displays the routing table for your reference.

```
Diagnosics >> View Routing Table

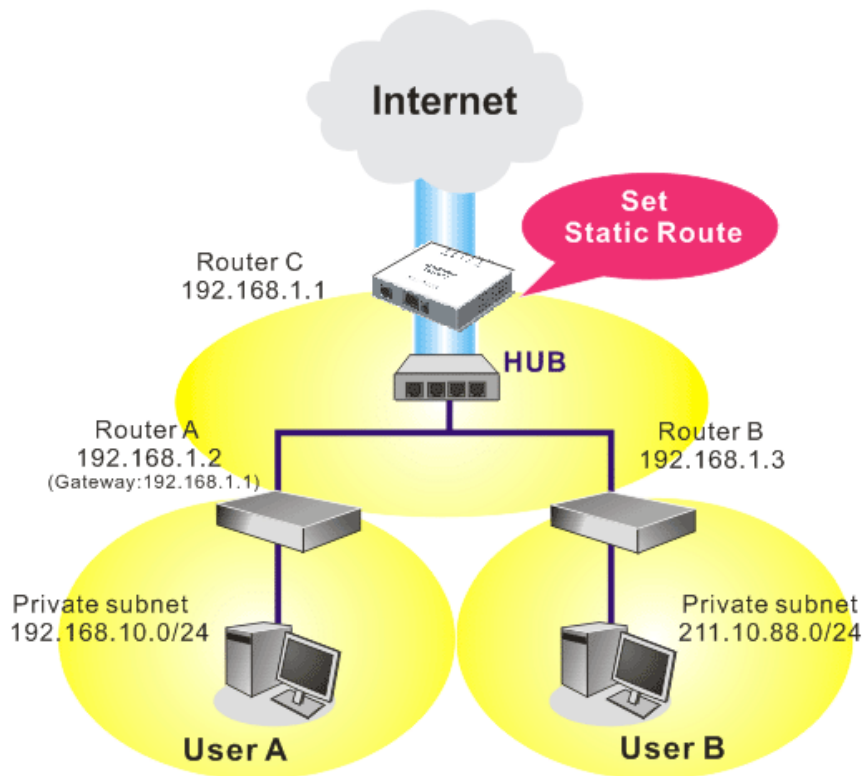
Current Running Routing Table | Refresh |
Key: C - connected, S - static, R - RIP, * - default, ~ - private
C~ 192.168.1.0/ 255.255.255.0 is directly connected, LAN
```

## Add Static Routes to Private and Public Networks

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**

<input checked="" type="checkbox"/> Enable	
Destination IP Address	192.168.10.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.2
Network Interface	LAN

OK Cancel

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. 1**

<input checked="" type="checkbox"/> Enable	
Destination IP Address	211.100.88.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.3
Network Interface	LAN

OK Cancel

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

Current Running 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,	LAN
C~	192.168.1.0/	255.255.255.0	is directly connected,	LAN
S~	211.100.88.0/	255.255.255.0	via 192.168.1.3,	LAN

### 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.

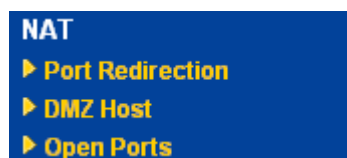
When the outgoing packets destined to some public server on the Internet reach the NAT modem, the modem will change its source address into the public IP address of the modem, select the available public port, and then forward it. At the same time, the modem shall list an entry in a table to memorize 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.

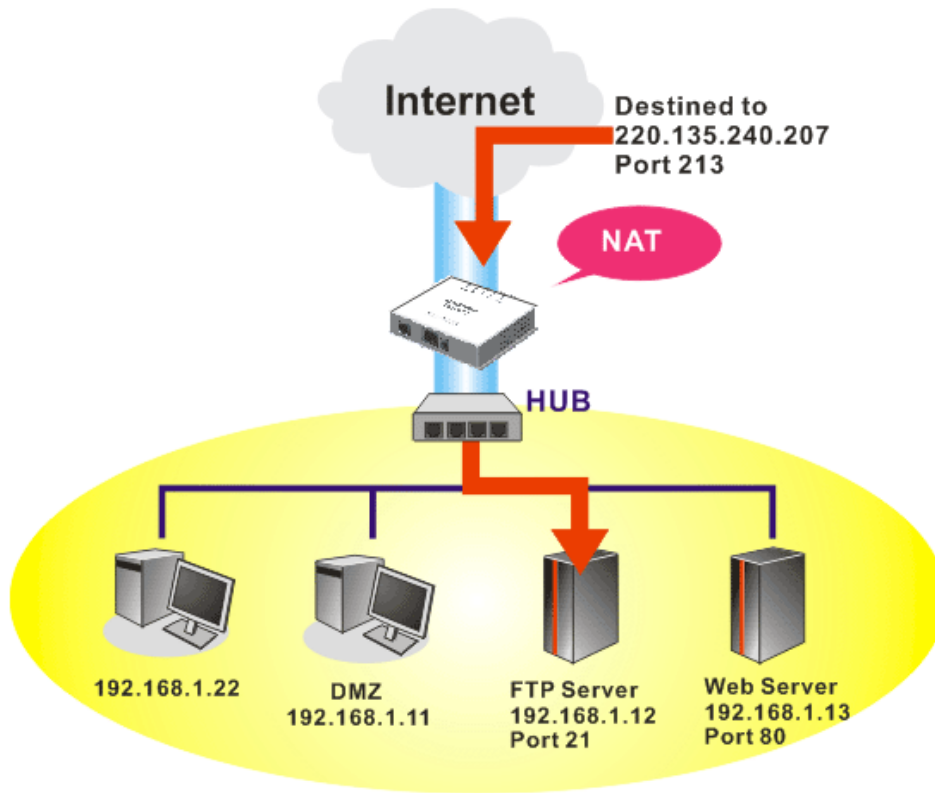
Below shows the menu items for NAT.



#### 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	Public Port	Private IP	Status
<a href="#">1.</a>				x
<a href="#">2.</a>				x
<a href="#">3.</a>				x
<a href="#">4.</a>				x
<a href="#">5.</a>				x
<a href="#">6.</a>				x
<a href="#">7.</a>				x
<a href="#">8.</a>				x
<a href="#">9.</a>				x
<a href="#">10.</a>				x

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

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

## NAT >> Port Redirection

### Index No. 1

<input checked="" type="checkbox"/> Enable	
Mode	Single
Service Name	Single
Protocol	---
WAN IP	1.All
Public Port	0
Private IP	
Private Port	0

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

OK Clear Cancel

#### **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.

#### **Active**

Check this box to activate the port-mapping entry you have defined.

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 configurator 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.

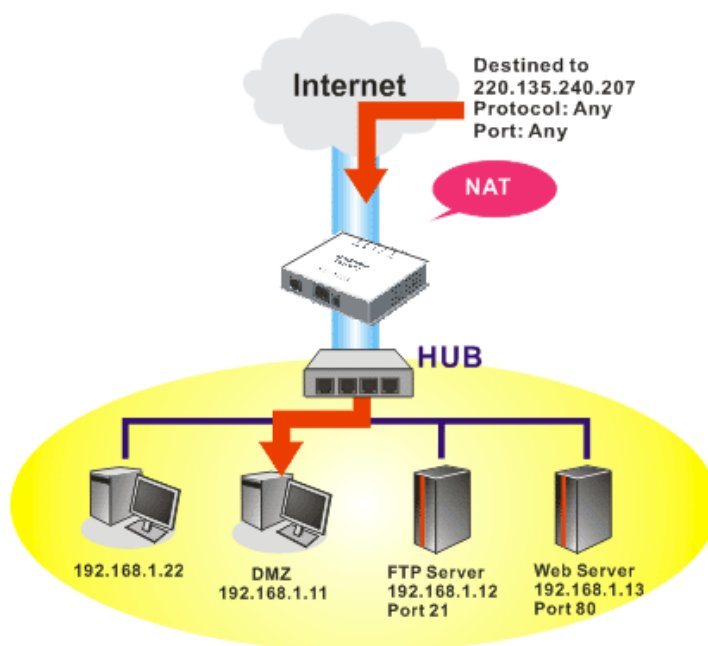
**System Maintenance >> Management**

**Management Setup**

<p><b>Management Access Control</b></p> <p><input checked="" type="checkbox"/> Allow management from the Internet</p> <p><input type="checkbox"/> FTP Server</p> <p><input checked="" type="checkbox"/> HTTP Server</p> <p><input checked="" type="checkbox"/> Telnet Server</p> <p><input checked="" type="checkbox"/> Disable PING from the Internet</p> <hr/> <p><b>Access List</b></p> <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"/>	<p><b>Management Port Setup</b></p> <p><input checked="" type="radio"/> User Define Ports    <input type="radio"/> Default Ports</p> <p>Telnet Port    <input type="text" value="23"/> (Default: 23)</p> <p>HTTP Port    <input type="text" value="80"/> (Default: 80)</p> <p>FTP Port    <input type="text" value="21"/> (Default: 21)</p>
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"/>											

### 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**

WAN  
None

Private IP  Choose PC

MAC Address of the True IP DMZ Host 00 . 00 . 00 : 00 . 00 . 00

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

OK

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**

Index	Enable	Aux. WAN IP	Private IP	Choose PC
1.	<input type="checkbox"/>	192.168.1.55	<input type="text"/>	Choose PC

OK Clear

**Enable**

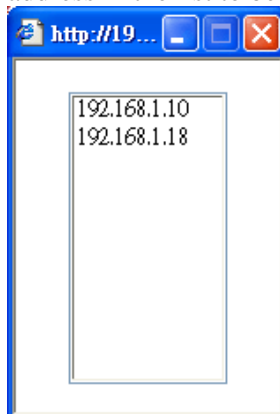
Check to enable the DMZ Host function.

**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.

[NAT >> DMZ Host Setup](#)

DMZ Host Setup

WAN			
Index	Enable	Aux. WAN IP	Private IP
1.	<input checked="" type="checkbox"/>	192.168.1.55	<input type="text" value="192.168.1.10"/>

### 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	Local IP Address	Status
<a href="#">1.</a>			X
<a href="#">2.</a>			X
<a href="#">3.</a>			X
<a href="#">4.</a>			X
<a href="#">5.</a>			X
<a href="#">6.</a>			X
<a href="#">7.</a>			X
<a href="#">8.</a>			X
<a href="#">9.</a>			X
<a href="#">10.</a>			X

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

**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.

**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

Local Computer

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	----- ▾	<input type="text" value="0"/>	<input type="text" value="0"/>	6.	----- ▾	<input type="text" value="0"/>	<input type="text" value="0"/>
2.	----- ▾	<input type="text" value="0"/>	<input type="text" value="0"/>	7.	----- ▾	<input type="text" value="0"/>	<input type="text" value="0"/>
3.	----- ▾	<input type="text" value="0"/>	<input type="text" value="0"/>	8.	----- ▾	<input type="text" value="0"/>	<input type="text" value="0"/>
4.	----- ▾	<input type="text" value="0"/>	<input type="text" value="0"/>	9.	----- ▾	<input type="text" value="0"/>	<input type="text" value="0"/>
5.	----- ▾	<input type="text" value="0"/>	<input type="text" value="0"/>	10.	----- ▾	<input type="text" value="0"/>	<input type="text" value="0"/>

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

## 3.4 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:

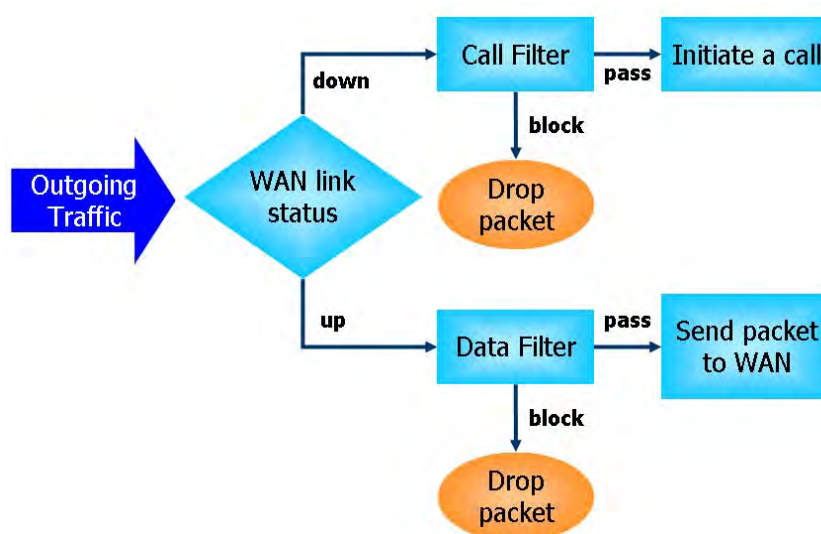
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

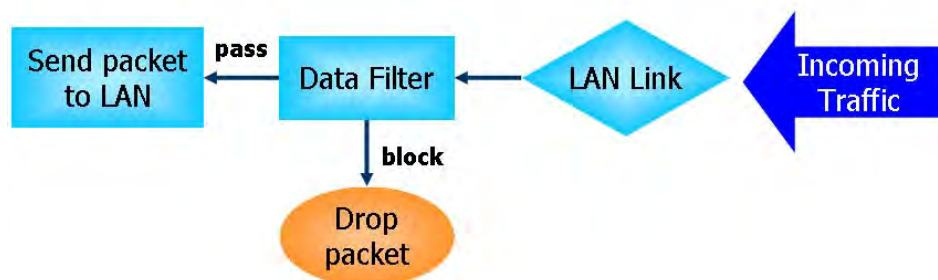
#### IP Filters

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.

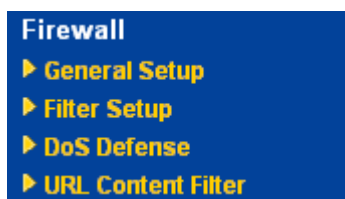
The **DoS Defense** function enables the Vigor modem to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog 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  | 9. SYN fragment          |
| 2. UDP flood attack  | 10. Fraggle attack       |
| 3. ICMP flood attack | 11. TCP flag scan        |
| 4. Port Scan attack  | 12. Tear drop attack     |
| 5. IP options        | 13. Ping of Death attack |
| 6. Land attack       | 14. ICMP fragment        |
| 7. Smurf attack      | 15. Unknown protocol     |
| 8. Trace route       |                          |

Below shows the menu items for Firewall.



### 4.4.2 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.

[Firewall >> General Setup](#)

**General Setup**

<b>Call Filter</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Start Filter Set	Set#1
<b>Data Filter</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Start Filter Set	Set#2

---

**Actions for default rule:**

Application	Action/Profile	Log
Filter	Pass	<input type="checkbox"/>

---

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

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

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

## Filter

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

Pass ▼  
Pass  
Block

## Log

For troubleshooting needs you can specify the filter log by checking the box. The log will be displayed on Draytek Syslog window.

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**”.

### 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
<a href="#">1.</a>	Default Call Filter	<a href="#">7.</a>	
<a href="#">2.</a>	Default Data Filter	<a href="#">8.</a>	
<a href="#">3.</a>		<a href="#">9.</a>	
<a href="#">4.</a>		<a href="#">10.</a>	
<a href="#">5.</a>		<a href="#">11.</a>	
<a href="#">6.</a>		<a href="#">12.</a>	

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		<a href="#">Down</a>
<input type="button" value="2"/>	<input type="checkbox"/>		<a href="#">UP</a>	<a href="#">Down</a>
<input type="button" value="3"/>	<input type="checkbox"/>		<a href="#">UP</a>	<a href="#">Down</a>
<input type="button" value="4"/>	<input type="checkbox"/>		<a href="#">UP</a>	<a href="#">Down</a>
<input type="button" value="5"/>	<input type="checkbox"/>		<a href="#">UP</a>	<a href="#">Down</a>
<input type="button" value="6"/>	<input type="checkbox"/>		<a href="#">UP</a>	<a href="#">Down</a>
<input type="button" value="7"/>	<input type="checkbox"/>		<a href="#">UP</a>	

Next Filter Set  ▼

<b>Filter Rule</b>	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.
<b>Active</b>	Enable or disable the filter rule.
<b>Comment</b>	Enter filter set comments/description. Maximum length is 23-character long.
<b>Move Up/Down</b>	Use <b>Up</b> or <b>Down</b> link to move the order of the filter rules.
<b>Next Filter Set</b>	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.

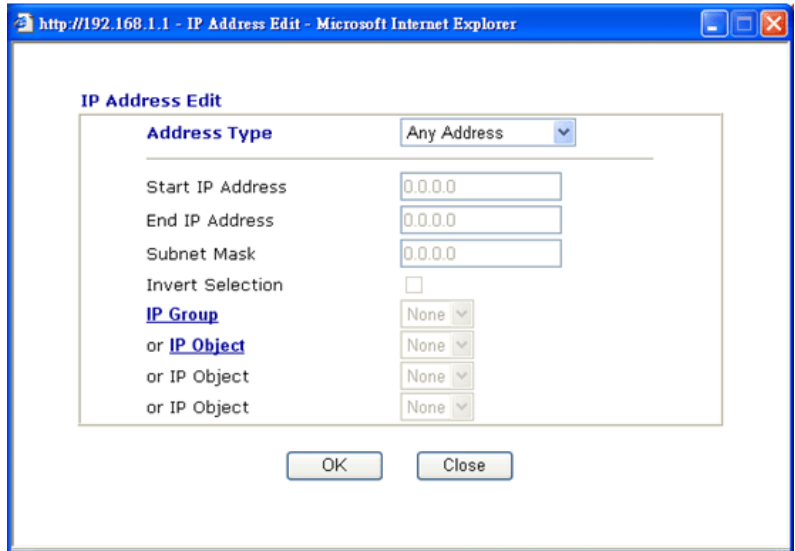
To edit **Filter Rule**, click the **Filter Rule** index button to enter the **Filter Rule** setup page.

[Firewall >> Edit Filter Set >> Edit Filter Rule](#)

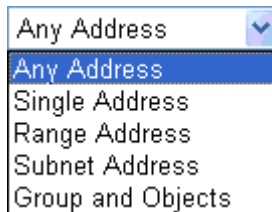
#### Filter Set 1 Rule 1

<input checked="" type="checkbox"/>	Check to enable the Filter Rule	
Comments:	<input type="text" value="Block NetBios"/>	
Index(1-15) in <a href="#">Schedule</a> Setup:	<input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>	
Direction:	<input type="text" value="LAN -&gt; WAN"/>	
Source IP:	<input type="text" value="Any"/>	<input type="button" value="Edit"/>
Destination IP:	<input type="text" value="Any"/>	<input type="button" value="Edit"/>
Service Type:	<input type="text" value="TCP/UDP, Port: from 137~139 to any"/>	<input type="button" value="Edit"/>
Fragments:	<input type="text" value="Don't Care"/>	
<b>Application</b>	<b>Action/Profile</b>	<b>Syslog</b>
Filter:	<input type="text" value="Block Immediately"/>	<input type="checkbox"/>
Branch to Other Filter Set:	<input type="text" value="None"/>	

<b>Check to enable the Filter Rule</b>	Check this box to enable the filter rule.
<b>Comments</b>	Enter filter set comments/description. Maximum length is 14-character long.
<b>Index(1-15)</b>	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 <b>Applications &gt;&gt; Schedule</b> setup. The default setting of this filed is blank and the function will always work.
<b>Direction</b>	Set the direction of packet flow (LAN->WAN/WAN->LAN). It is for <b>Data Filter</b> only. For the <b>Call Filter</b> , this setting is not available since <b>Call Filter</b> is only applied to outgoing traffic.
<b>Source/Destination IP</b>	Click <b>Edit</b> to access into the following dialog to choose the source/destination IP or IP ranges.



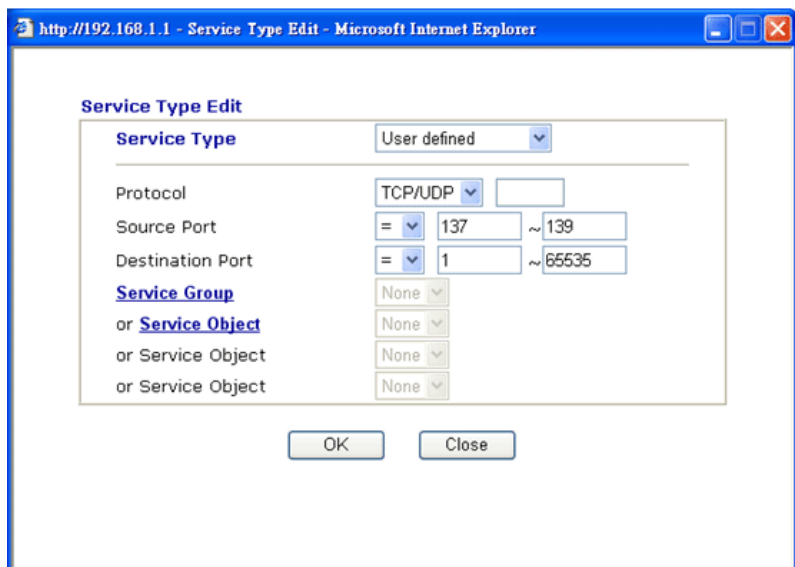
To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.



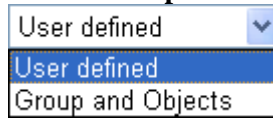
From the **IP Group** drop down list, choose the one that you want to apply. Or use the **IP Object** drop down list to choose the object that you want.

### 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.



A screenshot of a dropdown menu. The menu is open, showing two options: 'User defined' (which is highlighted in blue) and 'Group and Objects'.

**Protocol** - Specify the protocol(s) which this filter rule will apply to.  
**Source/Destination Port** -

(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type.

(! =) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.

(>) – the port number greater than this value is available.

(<) – the port number less than this value is available for this profile.

**Service Group/Object** - Use the drop down list to choose the one that you want.

#### **Fragments**

Specify the action for fragmented packets. And it is used for **Data Filter** only.

**Don't care** -No action will be taken towards fragmented packets.

**Unfragmented** -Apply the rule to unfragmented packets.

**Fragmented** - Apply the rule to fragmented packets.

**Too Short** - Apply the rule only to packets that are too short to contain a complete header.

#### **Filter**

Specifies the action to be taken when packets match the rule.

**Block Immediately** - Packets matching the rule will be dropped immediately.

**Pass Immediately** - Packets matching the rule will be passed immediately.

**Block If No Further Match** - A packet matching the rule, and that does not match further rules, will be dropped.

**Pass If No Further Match** - A packet matching the rule, and that does not match further rules, will be passed through.

#### **Branch to other Filter Set**

If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the modem will apply the specified filter rule for ever and will not return to previous filter rule any more.

#### **SysLog**

For troubleshooting needs you can specify the filter log here. Check the corresponding box to enable the log function. Then, the filter log will be shown on Draytek Syslog window.



## 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**

Call Filter:  Enable  Disable Start Filter Set: Set#1

Data Filter:  Enable  Disable Start Filter Set: Set#2

Actions for default rule:

Application: Filter Action/Profile: Pass Log:

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

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	Move Up	Move Down
1	<input checked="" type="checkbox"/>	Block NetBios		Down
2	<input type="checkbox"/>		UP	Down
3	<input type="checkbox"/>		UP	Down
4	<input type="checkbox"/>		UP	Down
5	<input type="checkbox"/>		UP	Down
6	<input type="checkbox"/>		UP	Down
7	<input type="checkbox"/>		UP	Down

Next Filter Set: N/A

OK Clear Cancel

Firewall >> Filter Setup >> Edit Filter Rule

**Filter Set 1 Rule 1**

Check to enable the Filter Rule

Comments: Block NetBios

Index(1-15) in Schedule Setup: [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

Direction: LAN -> WAN

Source IP: Any [Edit]

Destination IP: Any [Edit]

Service Type: TCP/UDP, Port: from 137-139 to any [Edit]

Fragments: Don't Care

Application: Filter: Block Immediately Syslog:

Branch to Other Filter Set: None

OK Clear Cancel

### 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

<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

<input type="checkbox"/> Block IP options	<input type="checkbox"/> Block TCP flag scan
<input type="checkbox"/> Block Land	<input type="checkbox"/> Block Tear Drop
<input type="checkbox"/> Block Smurf	<input type="checkbox"/> Block Ping of Death
<input type="checkbox"/> Block trace route	<input type="checkbox"/> Block ICMP fragment
<input type="checkbox"/> Block SYN fragment	<input type="checkbox"/> Block UnknownProtocol
<input type="checkbox"/> Block Fraggle Attack	

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

OK Clear All Cancel

#### Enable Dos Defense

Check the box to activate the DoS Defense Functionality.

#### Enable SYN flood defense

Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor modem will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor modem. By default, the threshold and timeout values are set to 50 packets per second and 10 seconds, respectively.

#### Enable UDP flood defense

Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor modem will start to randomly discard the subsequent UDP packets for a period defined in Timeout. The default setting for threshold and timeout are 150 packets per second and 10 seconds, respectively.

#### Enable ICMP flood defense

Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the modem will discard the ICMP echo requests coming from the Internet. The default setting for threshold and timeout are 50 packets per second and 10 seconds, respectively.

#### Enable PortScan

Port Scan attacks the Vigor modem by sending lots of packets to

<b>detection</b>	many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor modem will send out a warning. By default, the Vigor modem sets the threshold as 150 packets per second.
<b>Block IP options</b>	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.
<b>Block Land</b>	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.
<b>Block Smurf</b>	Check the box to activate the Block Smurf function. The Vigor modem will ignore any broadcasting ICMP echo request.
<b>Block trace modem</b>	Check the box to enforce the Vigor modem not to forward any trace route packets.
<b>Block SYN fragment</b>	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.
<b>Block Fraggle Attack</b>	Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked. Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.
<b>Block TCP flag scan</b>	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> .
<b>Block Tear Drop</b>	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.
<b>Block Ping of Death</b>	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.
<b>Block ICMP Fragment</b>	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.

## Block Unknown Protocol

Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the modem should have ability to detect and reject this kind of packets.

## Warning Messages

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

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

System Maintenance >> SysLog / Mail Alert Setup

**SysLog / Mail Alert Setup**

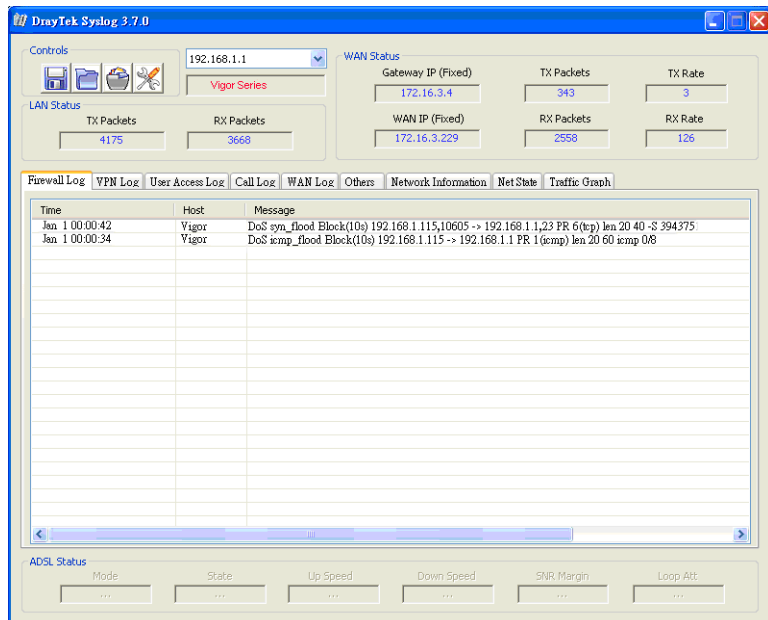
**SysLog Access Setup**

- Enable
- Server IP Address: 192.168.1.115
- Destination Port: 514
- Enable syslog message:
  - Firewall Log
  - User Access Log
  - Call Log
  - WAN Log
  - Router/DSL information

**Mail Alert Setup**

- Enable
- SMTP Server: [ ]
- Mail To: [ ]
- Return-Path: [ ]
- Authentication
  - User Name: [ ]
  - Password: [ ]
- Enable E-Mail Alert:
  - DoS Attack

OK Clear Cancel



### 3.4.5 URL Content Filter

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

For example, if you add key words such as “sex”, Vigor router will limit web access to web sites or web pages such as “www.sex.com”, ”www.backdoor.net/images/sex/p\_386.html”. Or you may simply specify the full or partial URL such as “www.sex.com” or “sex.com”.

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

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

[Firewall >> URL Content Filter](#)

**Content Filter Setup**

**Enable URL Access Control**

Black List (block those matching keyword)  
 White List (pass those matching keyword)

No	ACT	Keyword	No	ACT	Keyword
1	<input type="checkbox"/>	<input type="text"/>	5	<input type="checkbox"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	6	<input type="checkbox"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	7	<input type="checkbox"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	8	<input type="checkbox"/>	<input type="text"/>

Note that multiple keywords are allowed to specify in the blank. For example: **hotmail yahoo msn**

**Prevent web access from IP address**

---

**Enable Restrict Web Feature**

Java    ActiveX    Compressed files    Executable files    Multimedia files  
 Cookie    Proxy

---

**Enable Excepting Subnets**

No	Act	IP Address		Subnet Mask
1	<input type="checkbox"/>	<input type="text"/>	~	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	~	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	~	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	~	<input type="text"/>

---

**Time Schedule**

Index(1-15) in [Schedule](#) Setup: , , ,

Note: Action and Idle Timeout settings will be ignored.

**Enable URL Access Control** Check the box to activate URL Access Control.

**Black List (block those matching keyword)** Click this button to restrict accessing into the corresponding webpage with the keywords listed on the box below.

**White List (pass those matching keyword)** Click this button to allow accessing into the corresponding webpage with the keywords listed on the box below.

**Keyword** The Vigor router provides 8 frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor router will decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the

more simplified the blocking keyword list, the more efficiently the Vigor router perform.

**Prevent web access from IP address**

Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control.

You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.

**Enable Restrict Web Feature**

Check the box to activate the function.

**Java** - Check the checkbox to activate the Block Java object function. The Vigor router will discard the Java objects from the Internet.

**ActiveX** - Check the box to activate the Block ActiveX object function. Any ActiveX object from the Internet will be refused.

**Compressed file** - Check the box to activate the Block Compressed file function to prevent someone from downloading any compressed file. The following list shows the types of compressed files that can be blocked by the Vigor router. .

**zip, rar, .arj, .ace, .cab, .sit**

**Executable file** - Check the box to reject any downloading behavior of the executable file from the Internet.

**.exe, .com, .scr, .pif, .bas, .bat, .inf, .reg**

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

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

**.mov .mp3 .rm .ra .au .wmv  
.wav .asf .mpg .mpeg .avi .ram**

**Enable Excepting Subnets**

Four entries are available for users to specify some specific IP addresses or subnets so that they can be free from the *URL Access Control*. To enable an entry, click on the empty checkbox, named as **ACT**, in front of the appropriate entry.

**Time Schedule**

Specify what time should perform the URL content filtering facility.

## 3.5 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).

### Objects Setting

- ▶ IP Object
- ▶ IP Group
- ▶ Service Type Object
- ▶ Service Type Group

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

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

[Next >>](#)

**Set to Factory Default** Clear all profiles.

Click the number under Index column for settings in detail.

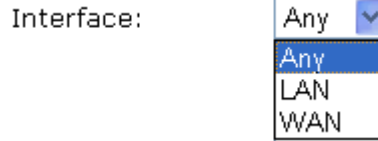
[Objects Setting >> IP Object](#)

Profile Index : 1

Name:	<input type="text" value="RD Department"/>
Interface:	<input type="text" value="Any"/>
Address Type:	<input type="text" value="Range Address"/>
Start IP Address:	<input type="text" value="192.168.1.64"/>
End IP Address:	<input type="text" value="192.168.1.75"/>
Subnet Mask:	<input type="text" value="0.0.0.0"/>
Invert Selection:	<input type="checkbox"/>

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

**Interface** Choose a proper interface (WAN, LAN or Any).



For example, the **Direction** setting in **Edit Filter Rule** will ask you specify IP or IP range for WAN or LAN or any IP address. If you choose LAN as the **Interface** here, and choose LAN as the direction setting in **Edit Filter Rule**, then all the IP addresses specified with LAN interface will be opened for you to choose in **Edit Filter Rule** page.

**Address Type** Determine the address type for the IP address.  
Select **Single Address** if this object contains one IP address only.  
Select **Range Address** if this object contains several IPs within a range.  
Select **Subnet Address** if this object contains one subnet for IP address.  
Select **Any Address** if this object contains any IP address.

**Start IP Address** Type the start IP address for Single Address type.

**End IP Address** Type the end IP address if the Range Address type is selected.

**Subnet Mask** Type the subnet mask if the Subnet Address type is selected.

**Invert Selection** If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.

Below is an example of IP objects settings.

### Objects Setting >> IP Object

#### IP Object Profiles:

Index	Name
<a href="#">1.</a>	RD Department
<a href="#">2.</a>	Financial Dept.
<a href="#">3.</a>	HR Department
<a href="#">4.</a>	
<a href="#">5.</a>	

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

**Set to Factory Default** Clear all profiles.

Click the number under Index column for settings in detail.

Objects Setting >> IP Group

Profile Index : 1

Name:	<input type="text" value="Admin"/>
Interface:	<input type="button" value="Any"/>
<b>Available IP Objects</b>	<b>Selected IP Objects</b>
<input type="text" value="1-RD Department"/> <input type="text" value="2-Financial Dept."/> <input type="text" value="3-HR Department"/>	<input type="text"/>
	<input type="button" value="&gt;&gt;"/> <input type="button" value="&lt;&lt;"/>

**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.

### 3.5.3 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
<a href="#">1.</a>		<a href="#">17.</a>	
<a href="#">2.</a>		<a href="#">18.</a>	
<a href="#">3.</a>		<a href="#">19.</a>	
<a href="#">4.</a>		<a href="#">20.</a>	
<a href="#">5.</a>		<a href="#">21.</a>	
<a href="#">6.</a>		<a href="#">22.</a>	
<a href="#">7.</a>		<a href="#">23.</a>	
<a href="#">8.</a>		<a href="#">24.</a>	
<a href="#">9.</a>		<a href="#">25.</a>	
<a href="#">10.</a>		<a href="#">26.</a>	
<a href="#">11.</a>		<a href="#">27.</a>	
<a href="#">12.</a>		<a href="#">28.</a>	
<a href="#">13.</a>		<a href="#">29.</a>	
<a href="#">14.</a>		<a href="#">30.</a>	
<a href="#">15.</a>		<a href="#">31.</a>	
<a href="#">16.</a>		<a href="#">32.</a>	

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

**Set to Factory Default** Clear all profiles.

Click the number under Index column for settings in detail.

[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="70"/> ~ <input type="text" value="80"/>

**Name** Type a name for this profile.

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

TCP	<input type="text" value="6"/>
<ul style="list-style-type: none"> <li>Any</li> <li>ICMP</li> <li>IGMP</li> <li style="background-color: #e0e0e0;">TCP</li> <li>UDP</li> <li>TCP/UDP</li> <li>Other</li> </ul>	

**Source/Destination Port** **Source Port** and the **Destination Port** column are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number.

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

Below is an example of service type objects settings.

[Objects Setting >> Service Type Object](#)

**Service Type Object Profiles:**

Index	Name	It
<a href="#">1.</a>	SIP	
<a href="#">2.</a>	RTP	
<a href="#">3.</a>		
<a href="#">4.</a>		

### 3.5.4 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
<a href="#">1.</a>		<a href="#">17.</a>	
<a href="#">2.</a>		<a href="#">18.</a>	
<a href="#">3.</a>		<a href="#">19.</a>	
<a href="#">4.</a>		<a href="#">20.</a>	
<a href="#">5.</a>		<a href="#">21.</a>	
<a href="#">6.</a>		<a href="#">22.</a>	
<a href="#">7.</a>		<a href="#">23.</a>	
<a href="#">8.</a>		<a href="#">24.</a>	
<a href="#">9.</a>		<a href="#">25.</a>	
<a href="#">10.</a>		<a href="#">26.</a>	
<a href="#">11.</a>		<a href="#">27.</a>	
<a href="#">12.</a>		<a href="#">28.</a>	
<a href="#">13.</a>		<a href="#">29.</a>	
<a href="#">14.</a>		<a href="#">30.</a>	
<a href="#">15.</a>		<a href="#">31.</a>	
<a href="#">16.</a>		<a href="#">32.</a>	

**Set to Factory Default**      Clear all profiles.

Click the number under Index column for settings in detail.

**Objects Setting >> Service Type Group Setup**

Profile Index : 1

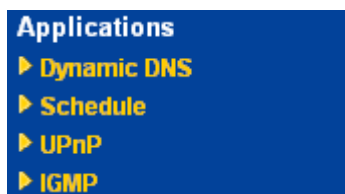
Name:

Available Service Type Objects		Selected Service Type Objects
1-SIP 2-RTP	>>  <<	

- |                                       |   |
|---------------------------------------|---|
| <b>Name</b>                           | Type a name for this profile.   |
| <b>Available Service Type Objects</b> | All the available service objects that you have added on <b>Objects Setting&gt;&gt;Service Type Object</b> will be shown in this box. |
| <b>Selected Service Type Objects</b>  | Click >> button to add the selected IP objects in this box.   |

## 3.6 Applications

Below shows the menu items for Applications.



### 3.6.1 Dynamic DNS

The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your 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](#)

**Dynamic DNS Setup** | [Set to Factory Default](#)

Enable Dynamic DNS Setup

**Accounts:**

Index	Domain Name	Active
<a href="#">1.</a>	.	x
<a href="#">2.</a>	.	x
<a href="#">3.</a>	.	x

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

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

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

**Domain Name** Display the domain name that you set on the setting page of DDNS setup.

**Active** Display if this account is active or inactive.

**View Log** Display DDNS log status.

**Force Update** Force the modem updates its information to DDNS server.

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:

**Enable Dynamic** Check this box to enable the current account. If you did

<b>DNS Account</b>	check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
<b>WAN Interface</b>	Select the WAN interface order to apply settings here.
<b>Service Provider</b>	Select the service provider for the DDNS account.
<b>Service Type</b>	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.
<b>Domain Name</b>	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
<b>Login Name</b>	Type in the login name that you set for applying domain.
<b>Password</b>	Type in the password that you set for applying domain.

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

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

#### Disable the Function and Clear all Dynamic DNS Accounts

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

### 3.6.2 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
<a href="#">1.</a>	x	<a href="#">9.</a>	x
<a href="#">2.</a>	x	<a href="#">10.</a>	x
<a href="#">3.</a>	x	<a href="#">11.</a>	x
<a href="#">4.</a>	x	<a href="#">12.</a>	x
<a href="#">5.</a>	x	<a href="#">13.</a>	x
<a href="#">6.</a>	x	<a href="#">14.</a>	x
<a href="#">7.</a>	x	<a href="#">15.</a>	x
<a href="#">8.</a>	x		

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

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

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

**Status** Display if this schedule setting is active or inactive.

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

To add a schedule, please click any index, say Index No. 1. The detailed settings of the call schedule with index 1 are shown below.

[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

OK Clear Cancel

**Enable Schedule Setup** Check to enable the schedule.

**Start Date (yyyy-mm-dd)** Specify the starting date of the schedule.

**Start Time (hh:mm)** Specify the starting time of the schedule.

**Duration Time (hh:mm)** Specify the duration (or period) for the schedule.

**Action** Specify which action Call Schedule should apply during the period of the schedule.  
**Force On** -Force the connection to be always on.  
**Force Down** -Force the connection to be always down.  
**Enable Dial-On-Demand** -Specify the connection to be dial-on-demand and the value of idle timeout should be specified in **Idle Timeout** field.  
**Disable Dial-On-Demand** -Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.

**Idle Timeout** Specify the duration (or period) for the schedule.  
**How often** -Specify how often the schedule will be applied  
**Once** -The schedule will be applied just once  
**Weekdays** -Specify which days in one week should perform the schedule.

**Example**

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

**Office  
Hour:**

**(Force On)**



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

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

### 3.6.3 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
- 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

#### Enable UPNP Service

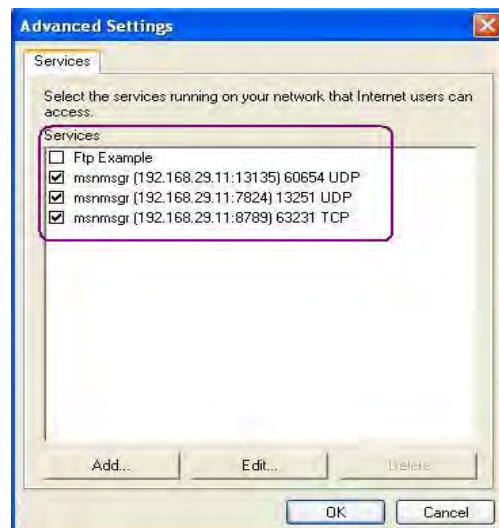
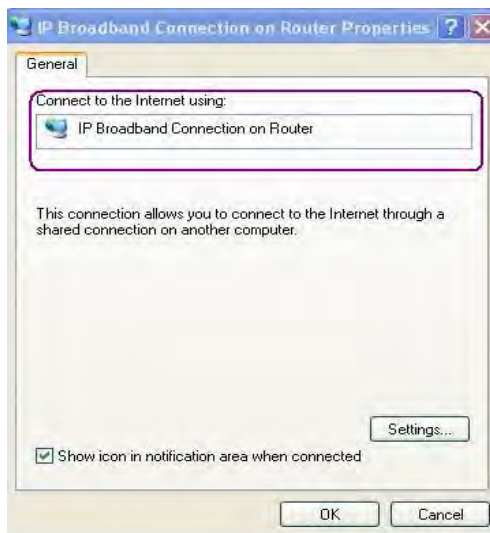
Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

After setting **Enable UPNP Service** setting, an icon of **IP Broadband Connection on 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.

### 3.6.4 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**

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 affect when Bridge Mode is enabled**.

OK

Cancel

[Refresh](#)

Working Multicast Groups

**Index**

**Group ID**

#### **Enable IGMP Proxy**

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

#### **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.

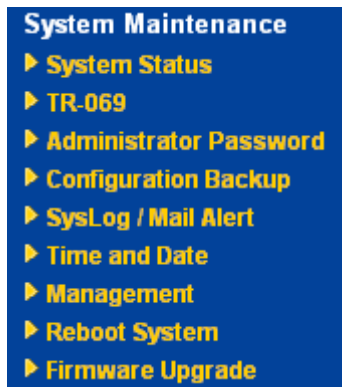
#### **Refresh**

Click this link to renew the working multicast group status.

## 3.7 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.



### 3.7.1 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** : Vigor120 series  
**Firmware Version** : 3.2.0\_RC2  
**Build Date/Time** : Aug 7 2008 11:58:09  
**ADSL Firmware Version** : 321311\_A Annex A

LAN		WAN 1	
MAC Address	: 00-50-7F-12-34-56	Link Status	: <b>Disconnected</b>
1st IP Address	: 192.168.1.1	MAC Address	: 00-50-7F-12-34-57
1st Subnet Mask	: 255.255.255.0	Connection	: PPPoE
DHCP Server	: Yes	IP Address	: ---
DNS	: 194.109.6.66	Default Gateway	: ---

**Model Name** Display the model name of the modem.  
**Firmware Version** Display the firmware version of the modem.  
**Build Date/Time** Display the date and time of the current firmware build.  
**ADSL Firmware Version** Display the ADSL firmware version.

### LAN-----

**MAC Address** Display the MAC address of the LAN Interface.  
**1<sup>st</sup> IP Address** Display the IP address of the LAN interface.  
**1<sup>st</sup> Subnet Mask** Display the subnet mask address of the LAN interface.  
**DHCP Server** Display the current status of DHCP server of the LAN interface.  
**DNS** Display the assigned IP address of the primary DNS.

### WAN-----

**Link Status** Display current connection status.  
**MAC Address** Display the MAC address of the WAN Interface.  
**Connection** Display the connection type.  
**IP Address** Display the IP address of the WAN interface.  
**Default Gateway** Display the assigned IP address of the default gateway.

## 3.7.2 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.

**ACS and CPE Settings**

**ACS Server On**

**ACS Server**

URL

Username

Password

**CPE Client**

Enable  Disable

URL

Port

Username

Password

**Periodic Inform Settings**

Disable  Enable

Interval Time  second(s)

Schedule Time

Date (yyyy-mm-dd)  -  -

Time (hh:mm:ss)  :  :

OK

**ACS Server On**

Choose the interface for the modem connecting to ACS server.

Internet

PVC

**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**

It is not necessary for you to type them. Such information is useful for Auto Configuration Server.

**Enable/Disable** – Sometimes, port conflict might be occurred. To solve such problem, you might want to change port number for CPE. Please click Enable and change the port number.

**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.

**Date (yyyy-mm-dd)** - Specify the starting date of the schedule.

**Time (hh:mm)** - Specify the starting time of the schedule.

### 3.7.3 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"/>

**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 configurator again.

### 3.7.4 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.

[LAN >> General Setup](#)

[System Maintenance >> Configuration Backup](#)

**Configuration Backup / Restoration**

**Restoration**

Select a configuration file.

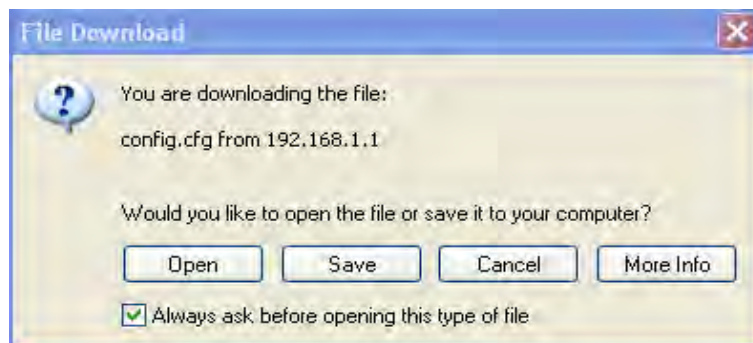
Click Restore to upload the file.

---

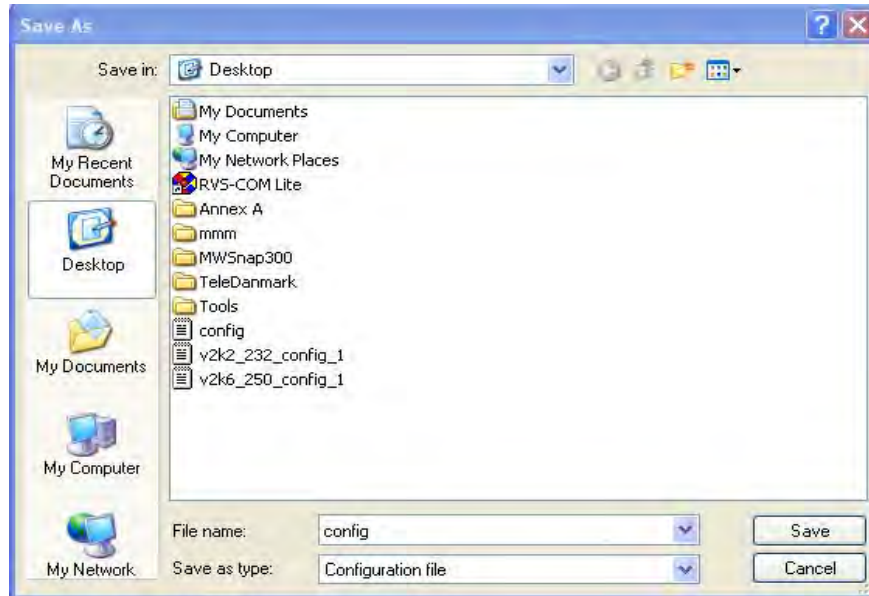
**Backup**

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.

[LAN >> General Setup](#)

[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 **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.

### 3.7.5 Syslog/Mail Alert

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

[System Maintenance >> SysLog / Mail Alert Setup](#)

**SysLog / Mail Alert Setup**

**SysLog Access Setup**

Enable

Server IP Address: 192.168.1.115

Destination Port: 514

Enable syslog message:

- Firewall Log
- User Access Log
- Call Log
- WAN Log
- Router/DSL information

**Mail Alert Setup**

Enable

SMTP Server:

Mail To:

Return-Path:

Authentication

User Name:

Password:

Enable E-Mail Alert:

- DoS Attack

**Enable (Syslog Access...)**

Check “**Enable**” to activate function of syslog.

**Syslog Server IP**

The IP address of the Syslog server.

**Destination Port**

Assign a port for the Syslog protocol.

**Enable syslog message**

Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Modem/DSL information to Syslog.

**Enable (Alert Setup...)**

Check “**Enable**” to activate function of mail alert.

**Send a test e-mail**

Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not.

**SMTP Server**

The IP address of the SMTP server.

**Mail To**

Assign a mail address for sending mails out.

**Return-Path**

Assign an e-mail address of another mailbox to accept all returned messages if fatal problems occur at the recipient mailbox.

The e-mail address typed here also acts as the Sender address while Vigor sends out the alert e-mails.

**Authentication**

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

**User Name**

Type the user name for authentication.

**Password**

Type the password for authentication.

**Enable E-mail Alert**

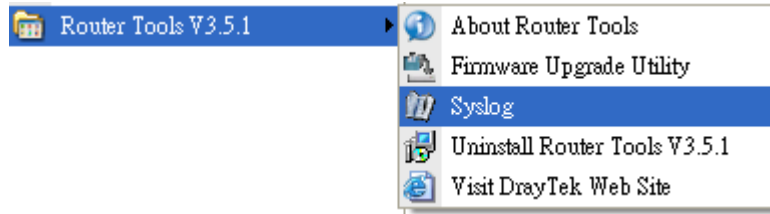
Check the box to send alert message to the e-mail box while the modem detecting the item(s) you specify here.

Click **OK** to save these settings.

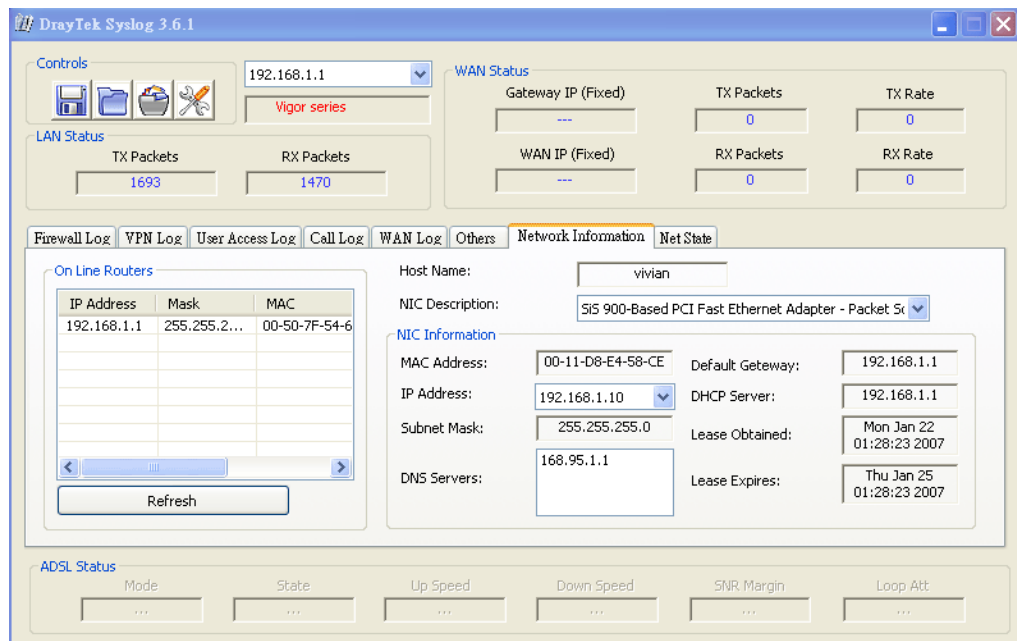


For viewing the Syslog, please do the following:

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



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



### 3.7.6 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 0 : 18 : 41 Inquire Time

##### Time Setup

Use Browser Time  
 Use Internet Time Client  
 Server IP Address: pool.ntp.org  
 Time Zone: (GMT) Greenwich Mean Time : Dublin  
 Enable Daylight Saving:   
 Automatically Update Interval: 30 min

OK Cancel

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

Click **OK** to save these settings.

### 3.7.7 Management

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

[System Maintenance >> Management](#)

**Management Setup**

<p><b>Management Access Control</b></p> <p><input checked="" type="checkbox"/> Allow management from the Internet</p> <p><input type="checkbox"/> FTP Server</p> <p><input checked="" type="checkbox"/> HTTP Server</p> <p><input checked="" type="checkbox"/> Telnet Server</p> <p><input checked="" type="checkbox"/> Disable PING from the Internet</p> <hr/> <p><b>Access List</b></p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 5%;">List</th> <th style="width: 40%;">IP</th> <th style="width: 55%;">Subnet Mask</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text"/></td> <td><input style="border-bottom: none; border-right: none; border-top: none; border-left: none; width: 100%;" type="text"/> <input type="button" value="v"/></td> </tr> <tr> <td>2</td> <td><input type="text"/></td> <td><input style="border-bottom: none; border-right: none; border-top: none; border-left: none; width: 100%;" type="text"/> <input type="button" value="v"/></td> </tr> <tr> <td>3</td> <td><input type="text"/></td> <td><input style="border-bottom: none; border-right: none; border-top: none; border-left: none; width: 100%;" type="text"/> <input type="button" value="v"/></td> </tr> </tbody> </table>	List	IP	Subnet Mask	1	<input type="text"/>	<input style="border-bottom: none; border-right: none; border-top: none; border-left: none; width: 100%;" type="text"/> <input type="button" value="v"/>	2	<input type="text"/>	<input style="border-bottom: none; border-right: none; border-top: none; border-left: none; width: 100%;" type="text"/> <input type="button" value="v"/>	3	<input type="text"/>	<input style="border-bottom: none; border-right: none; border-top: none; border-left: none; width: 100%;" type="text"/> <input type="button" value="v"/>	<p><b>Management Port Setup</b></p> <p><input checked="" type="radio"/> User Define Ports    <input type="radio"/> Default Ports</p> <p>Telnet Port    <input type="text" value="23"/> (Default: 23)</p> <p>HTTP Port    <input type="text" value="80"/> (Default: 80)</p> <p>FTP Port    <input type="text" value="21"/> (Default: 21)</p>
List	IP	Subnet Mask											
1	<input type="text"/>	<input style="border-bottom: none; border-right: none; border-top: none; border-left: none; width: 100%;" type="text"/> <input type="button" value="v"/>											
2	<input type="text"/>	<input style="border-bottom: none; border-right: none; border-top: none; border-left: none; width: 100%;" type="text"/> <input type="button" value="v"/>											
3	<input type="text"/>	<input style="border-bottom: none; border-right: none; border-top: none; border-left: none; width: 100%;" type="text"/> <input type="button" value="v"/>											

**Allow management from the Internet** Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the modem from Internet. Check the box(es) to specify.

**Disable PING from the Internet** Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.

**Access List** You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.  
**List IP** - Indicate an IP address allowed to login to the modem.

**Subnet Mask** - Represent a subnet mask allowed to login to the modem.

**Default Ports** Check to use standard port numbers for the Telnet, FTP and HTTP servers.

## User Defined Ports

Check to specify user-defined port numbers for the Telnet, HTTP and FTP servers.

### 3.7.8 Reboot System

The Web Configurator 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

If you want to reboot the modem using the current configuration, check **Using current configuration** and click **OK**. To reset the modem settings to default values, check **Using factory default configuration** and click **OK**. 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.

### 3.7.9 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](http://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: 3.2.0\_RC2

**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

---

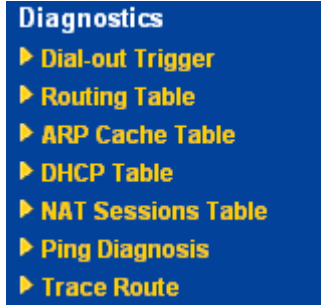
 TFTP server is running. Please execute a Firmware Upgrade Utility software to upgrade router's firmware. This server will be closed by itself when the firmware upgrading finished.

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

## 3.8 Diagnostics

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

Below shows the menu items for Diagnostics.



### 3.8.1 Dial-out Trigger

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

[Diagnostics >> Dial-out Trigger](#)

Dial-out Triggered Packet Header

| [Refresh](#) |

**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
```

**Decoded Format:**

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

**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.

### 3.8.2 Routing Table

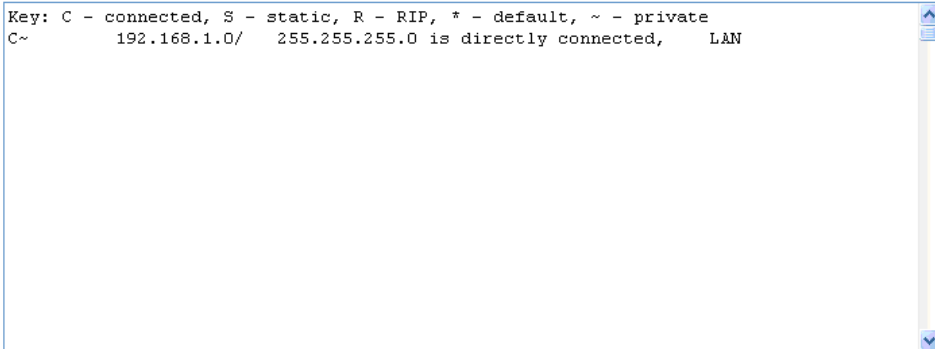
Click **Diagnostics** and click **Routing Table** to open the web page.

[Diagnostics >> View Routing Table](#)

---

**Current Running Routing Table** | [Refresh](#) |

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
C~      192.168.1.0/  255.255.255.0 is directly connected,   LAN
```



**Refresh**

Click it to reload the page.

### 3.8.3 ARP Cache Table

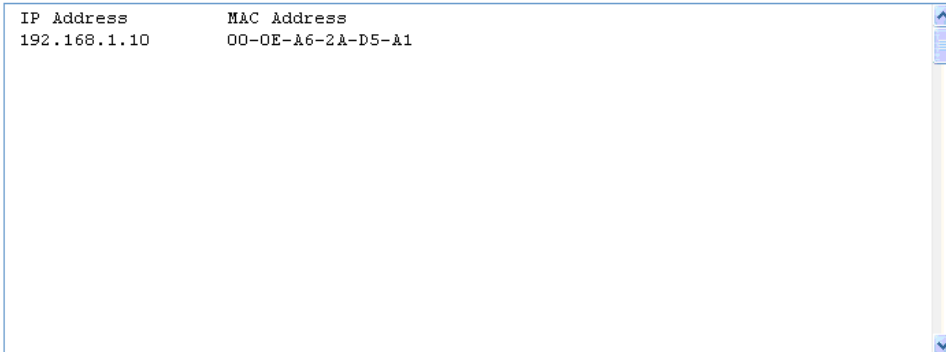
Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the modem. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.

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

---

**Ethernet ARP Cache Table** | [Clear](#) | [Refresh](#) |

IP Address	MAC Address
192.168.1.10	00-0E-A6-2A-D5-A1



**Refresh**

Click it to reload the page.

**Clear**

Click it to clear the whole table.

### 3.8.4 DHCP Table

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

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

[Diagnostics >> View DHCP Assigned IP Addresses](#)

DHCP IP Assignment Table				
DHCP server: Running				
Index	IP Address	MAC Address	Leased Time	HOST ID

- 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.

### 3.8.5 NAT Sessions Table

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

[Diagnostics >> NAT Sessions Table](#)

NAT Active Sessions Table			
Private IP :Port	#Pseudo Port	Peer IP :Port	Interface

- Private IP:Port** It indicates the source IP address and port of local PC.

<b>#Pseudo Port</b>	It indicates the temporary port of the modem used for NAT.
<b>Peer IP:Port</b>	It indicates the destination IP address and port of remote host.
<b>Interface</b>	It displays the representing number for different interface.
<b>Refresh</b>	Click it to reload the page.

### 3.8.6 Ping Diagnosis

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

[Diagnostics >> Ping Diagnosis](#)

#### Ping Diagnosis

**Note:** If you want to ping a LAN PC or you don't want to specify which WAN to ping through, please select "Unspecified".

Ping to:  IP Address:

**Result** [Clear](#)

<b>Ping to</b>	Use the drop down list to choose the destination that you want to ping.
<b>IP Address</b>	Type in the IP address of the Host/IP that you want to ping.
<b>Run</b>	Click this button to start the ping work. The result will be displayed on the screen.
<b>Clear</b>	Click this link to remove the result on the window.



### 3.8.7 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



Host / IP Address:

**Result** | [Clear](#)

**Host/IP Address**

It indicates the IP address of the host.

**Run**

Click this button to start route tracing work.

**Clear**

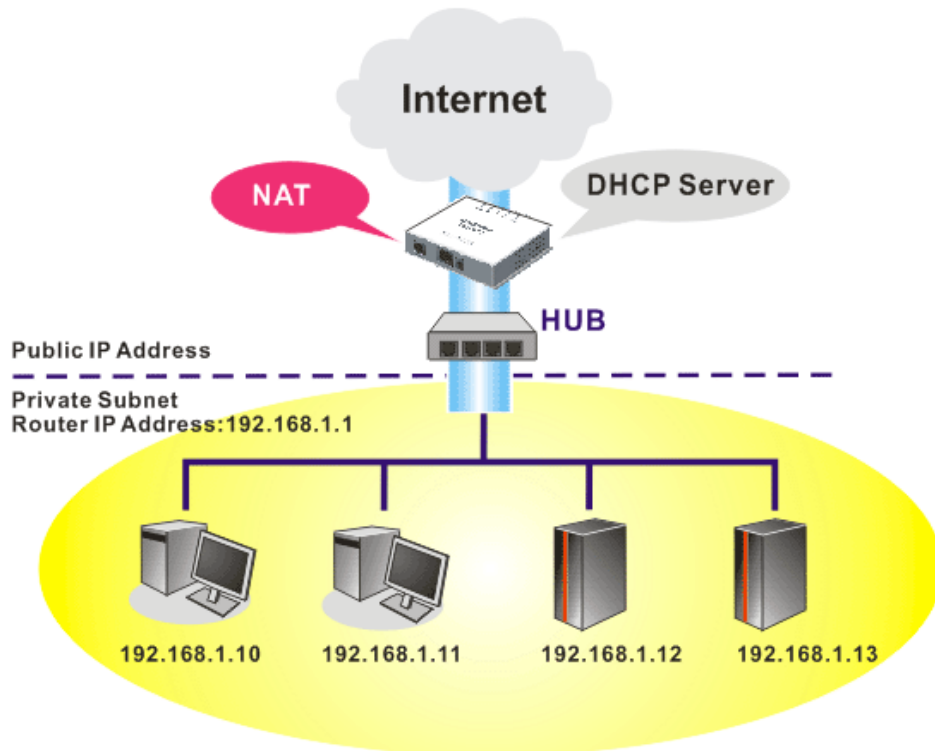
Click this link to remove the result on the window.

# 4

## Application and Examples

### 4.1 LAN – Created by Using NAT

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



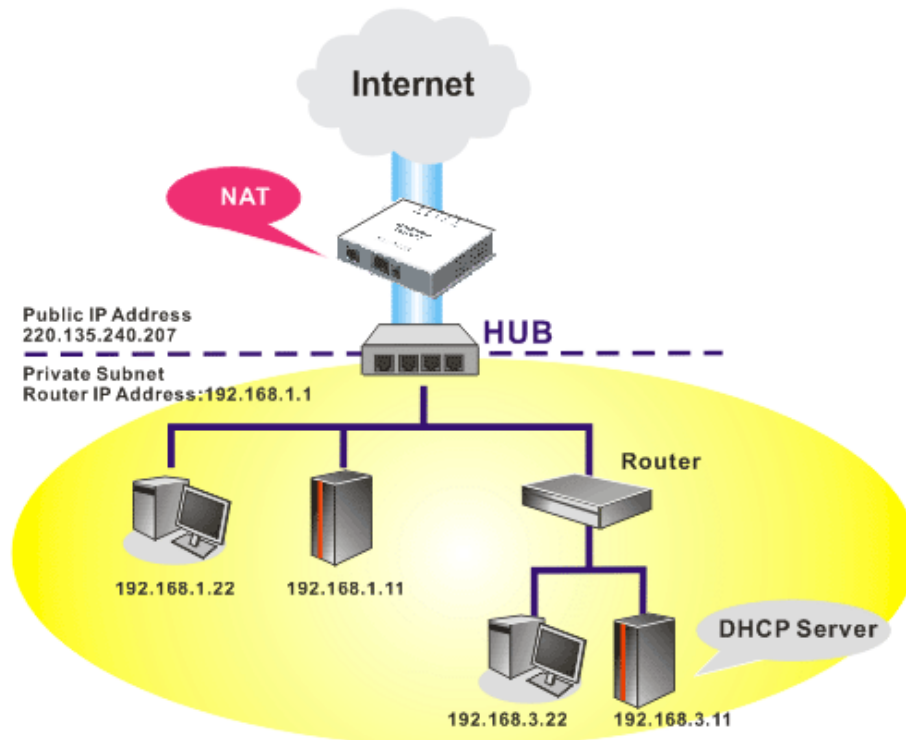
You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.

LAN >> General Setup

**Ethernet TCP / IP and DHCP Setup**

<b>LAN IP Network Configuration</b>		<b>DHCP Server Configuration</b>	
For NAT Usage		<input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server	
IP Address	<input type="text" value="192.168.1.5"/>	Start IP Address	<input type="text" value="192.168.1.10"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>	IP Pool Counts	<input type="text" value="50"/>
		Gateway IP Address	<input type="text" value="192.168.1.5"/>
		<b>DNS Server IP Address</b>	
		Primary IP Address	<input type="text"/>
		Secondary IP Address	<input type="text"/>

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



## LAN >> General Setup

**Ethernet TCP / IP and DHCP Setup**

<b>LAN IP Network Configuration</b> For NAT Usage IP Address: <input type="text" value="192.168.1.5"/> Subnet Mask: <input type="text" value="255.255.255.0"/>	<b>DHCP Server Configuration</b> <input type="radio"/> Enable Server <input checked="" type="radio"/> Disable Server Start IP Address: <input type="text" value="192.168.1.10"/> IP Pool Counts: <input type="text" value="50"/> Gateway IP Address: <input type="text" value="192.168.1.5"/>
	<b>DNS Server IP Address</b> Primary IP Address: <input type="text"/> Secondary IP Address: <input type="text"/>

## 4.2 Upgrade Firmware for Your Modem

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

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

Please remember to set as follows in your DrayTek Router :

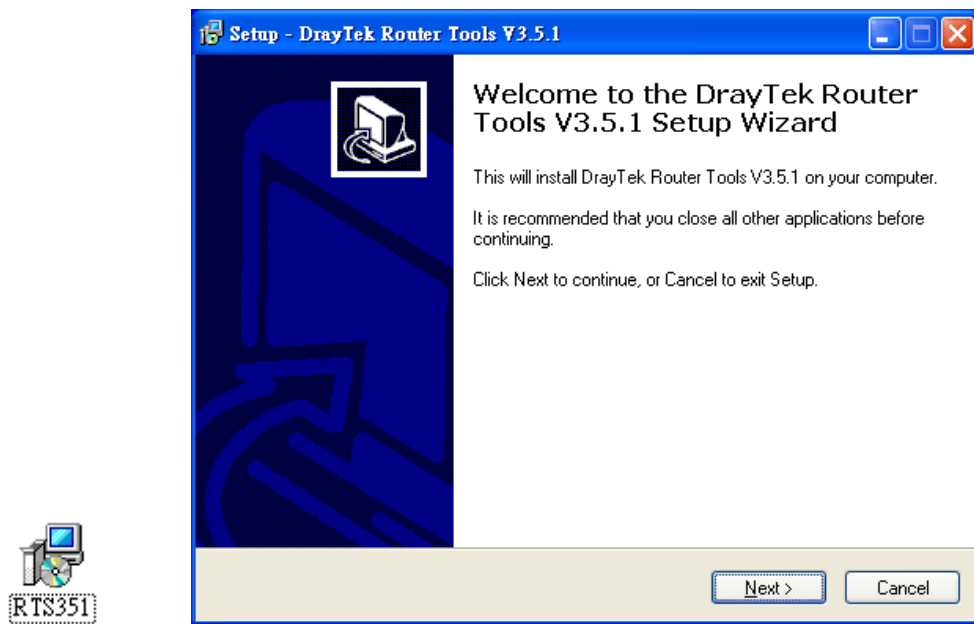
- Server IP Address : IP address of the PC that runs the Syslog
- Port Number : Default value 514

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

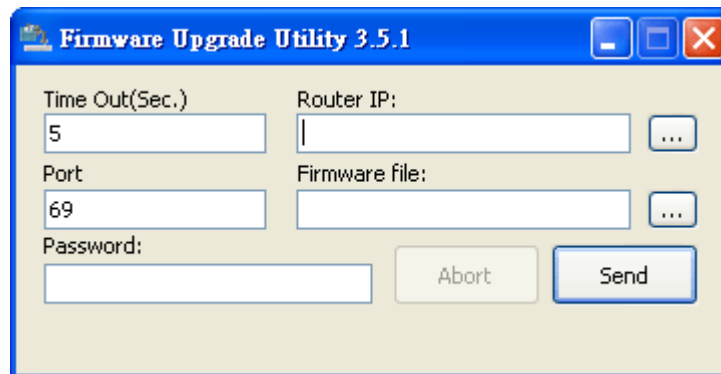
Tools Name	Released Date	Version	OS	Support Model	Download
Router Tools	21/12/2006	3.5.1	MS-Windows	All Model	<a href="#">zip</a>
SmartVPN Client	18/08/2006	3.2.6	MS-Windows	All Model	<a href="#">zip</a>
LPR	27/06/2005	1.0	MS-Windows	For Print Function	<a href="#">zip</a>
VTA	15/09/2005	2.8	Windows2000/XP	For ISDN Model	<a href="#">zip</a>
DialPlan	26/01/2006	2.5_lite	MS-Windows	For VoIP Model	<a href="#">zip</a>

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

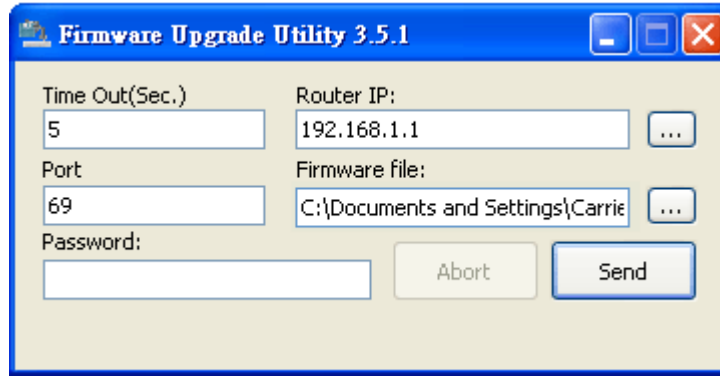
9. Double click on the icon of modem tool. The setup wizard will appear.



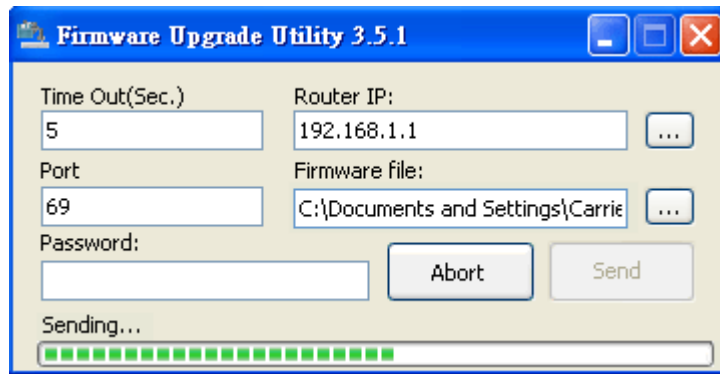
10. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.
11. From the **Start** menu, open **Programs** and choose **Modem Tools XXX >> Firmware Upgrade Utility**.



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



14. Click **Send**.



15. Now the firmware update is finished.

# 5

## 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 **POWER LED**, **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

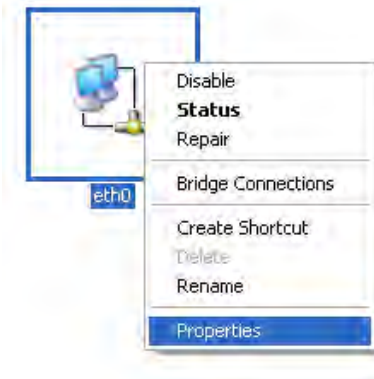


The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in [www.draytek.com](http://www.draytek.com).

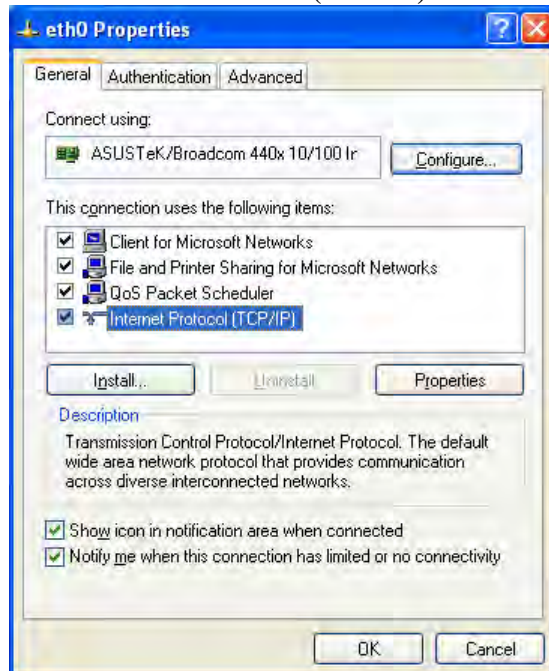
1. Go to **Control Panel** and then double-click on **Network Connections**.



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

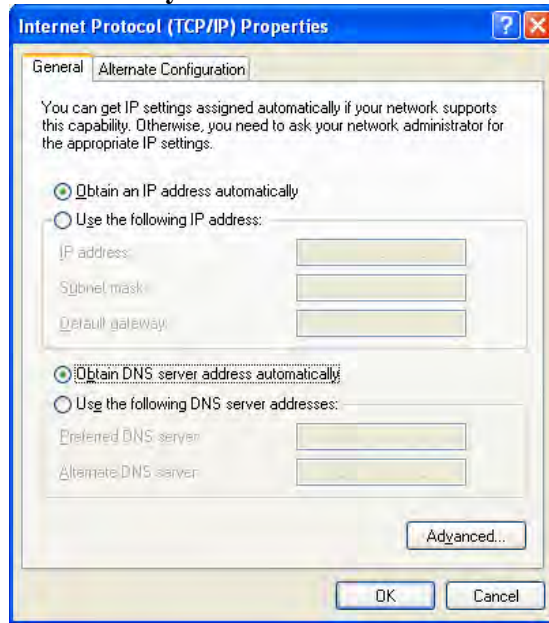


3. Select **Internet Protocol (TCP/IP)** and then click **Properties**.



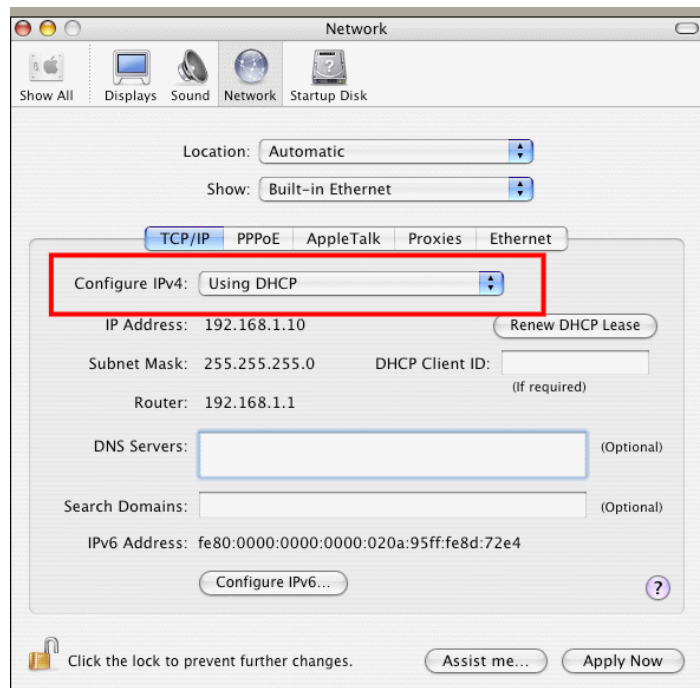


4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



### 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.



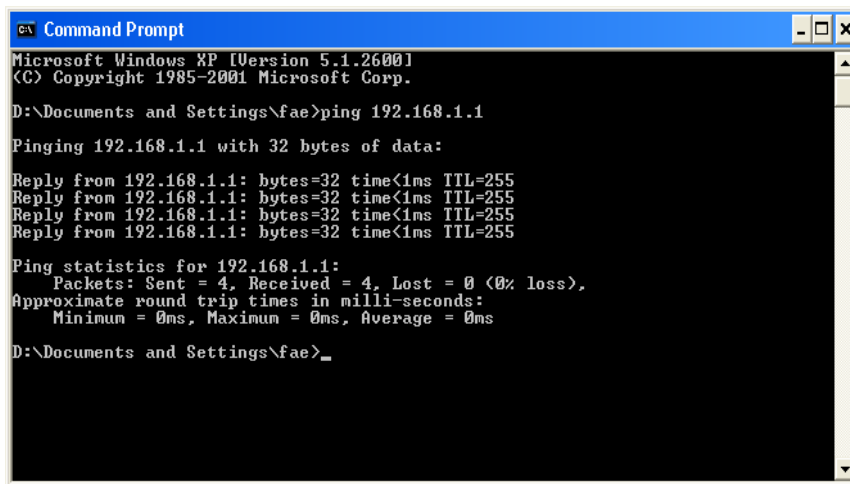
## 5.3 Pinging the Modem from Your Computer

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.



```
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 ttys1
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.



### For PPPoE/PPPoA Users

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

[Internet Access >> PPPoE / PPPoA](#)

**PPPoE / PPPoA Client Mode**

<b>PPPoE/PPPoA Client</b> <input checked="" type="radio"/> Enable <input type="radio"/> Disable		<b>ISP Access Setup</b>	
<b>DSL Modem Settings</b>		ISP Name <input type="text"/>	
VPI	<input type="text" value="0"/>	Username <input type="text"/>	
VCI	<input type="text" value="33"/>	Password <input type="text"/>	
Encapsulating Type	<input type="text" value="LLC/SNAP"/>	PPP Authentication <input type="text" value="PAP or CHAP"/>	
Protocol	<input type="text" value="PPPoE"/>	<input checked="" type="checkbox"/> Always On	
Modulation	<input type="text" value="Multimode"/>	Idle Timeout <input type="text" value="-1"/> second(s)	
<b>PPPoE Pass-through</b>		<b>IP Address From ISP</b> <input type="text" value="WAN IP Alias"/>	
<input type="checkbox"/> For Wired LAN		Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)	
<b>Note:</b> 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.		Fixed IP Address <input type="text"/>	
		<input checked="" type="radio"/> Default MAC Address	
		<input type="radio"/> Specify a MAC Address	
		MAC Address: <input type="text" value="00"/> <input type="text" value=".50"/> <input type="text" value=".7F"/> <input type="text" value=":"/> <input type="text" value="12"/> <input type="text" value=".34"/> <input type="text" value=".57"/>	
		Index(1-15) in <a href="#">Schedule</a> Setup:	
		=> <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>	

OK

## For MPoA Users

1. Check if the **Enable** option is selected.
2. Check if all parameters of **DSL Modem Settings** are entered with correct value that provided by your ISP. Especially, check if the encapsulation is selected properly or not (it should be the same with the setting on **Quick Start Wizard**).
3. Check if **IP Address**, **Subnet Mask** and **Gateway** are set correctly (must identify with the values from your ISP) if you choose **Specify an IP address**.

[Internet Access >> MPoA \(RFC1483/2684\)](#)

**MPoA (RFC1483/2684) Mode**

MPoA (RFC1483/2684)  Enable  Disable

---

**DSL Modem Settings**

Multi-PVC channel

Encapsulation

VPI

VCI

Modulation

---

**RIP Protocol**

Enable RIP

---

**Bridge Mode**

Enable Bridge Mode

---

**WAN IP Network Settings**

Obtain an IP address automatically

Router Name \*

Domain Name \*

\*: Required for some ISPs

Specify an IP address

IP Address

Subnet Mask

Gateway IP Address

---

Default MAC Address

Specify a MAC Address

MAC Address:

---

**DNS Server IP Address**

Primary IP Address

Secondary IP Address

## 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.

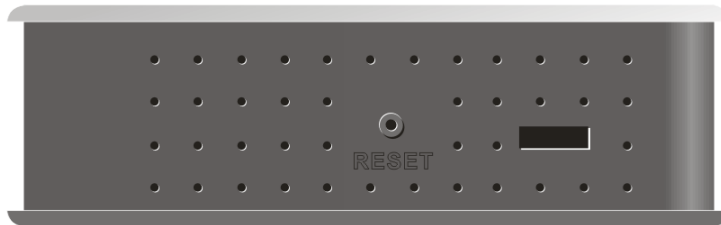
### Reboot System

**Do you want to reboot your router ?**

Using current configuration  
 Using factory default configuration

## Hardware Reset

While the modem is running, press the **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](mailto:support@draytek.com).