



Vigor 110

ADSL2/2+ Firewall Router

User's Guide

Version: 1.0

Date: 2007/11/01

Copyright 2007 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. The scope of delivery and other details are subject to change without prior notice.

Microsoft is a registered trademark of Microsoft Corp.

Windows, Windows 95, 98, Me, NT, 2000, XP 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.

Table of Contents

1

Preface	1
1.1 Panel Explanation	1
1.2 Hardware Installation	2

2

Configuring Basic Settings	3
2.1 Changing Password	3
2.2 Quick Start Wizard	5
2.2.1 Adjusting Protocol/Encapsulation	5
2.2.2 PPPoE/PPPoA	6
2.2.3 Bridged IP	8
2.2.4 Routed IP	9
2.3 Online Status	10
2.4 Saving Configuration	10

3

Advanced Web Configuration	11
3.1 Internet Access	11
3.1.1 Basics of Internet Protocol (IP) Network	11
3.1.2 PPPoE/PPPoA	12
3.1.3 MPoA	14
3.2 LAN	16
3.2.1 Basics of LAN	16
3.2.2 General Setup	17
3.2.3 Static Route	18
3.3 NAT	22
3.3.1 Port Redirection	22
3.3.2 DMZ Host	24
3.3.3 Open Ports	26
3.3.4 Well-Known Ports List	28
3.4 Firewall	29
3.4.1 Basics for Firewall	29
3.4.2 General Setup	32
3.4.3 Filter Setup	33
3.4.4 IM Blocking	37
3.4.5 P2P Blocking	37
3.4.6 DoS Defense	38
3.4.7 URL Content Filter	41
3.5 Applications	43
3.5.1 Dynamic DNS	43
3.5.2 Schedule	45

3.5.3 UPnP.....	47
3.5.4 IGMP.....	48
3.5.5 Wake on LAN.....	49
3.6 System Maintenance.....	49
3.6.1 System Status.....	49
3.6.2 Administrator Password.....	50
3.6.3 Configuration Backup	50
3.6.4 Syslog/Mail Alert.....	52
3.6.5 Time and Date	54
3.6.6 Management.....	55
3.6.7 Reboot System	56
3.6.8 Firmware Upgrade.....	56
3.7 Diagnostics.....	57
3.7.1 WAN Connection	57
3.7.2 Dial-out Trigger.....	58
3.7.3 Routing Table	58
3.7.4 ARP Cache Table.....	59
3.7.5 DHCP Table.....	59
3.7.6 NAT Sessions Table.....	60
3.7.7 Ping Diagnosis.....	60
3.7.8 Data Flow Monitor.....	61
3.7.9 Trace Route	62

4

Application and Examples	65
4.1 LAN – Created by Using NAT	65
4.2 Upgrade Firmware for Your Router	66

5

Trouble Shooting	69
5.1 Checking If the Hardware Status Is OK or Not.....	69
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	69
5.3 Pinging the Router from Your Computer	72
5.4 Checking If the ISP Settings are OK or Not.....	73
5.5 Backing to Factory Default Setting If Necessary	74
5.6 Contacting Your Dealer	75

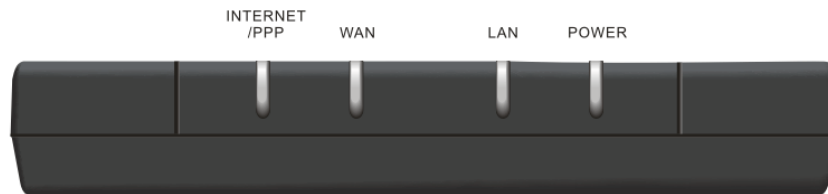
1

Preface

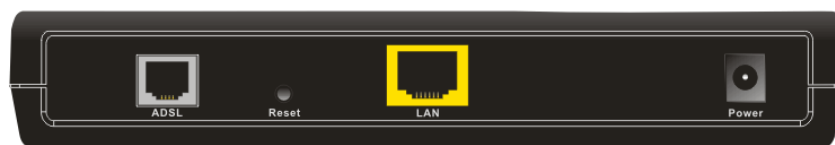
Targeting requirement for residential users, Vigor110 is an ADSL2/2+ enabled integrated access device. With downstream speed up to 12Mbps (ADSL2) or 24Mbps (ADSL2+), Vigor110 provides exceptional bandwidth for Internet access.

To secure your network, the Vigor110 provides an advanced firewall with advanced features, such as Stateful Packet Inspection (SPI) to offer network reliability by detecting and prohibiting malicious penetrating packets or DoS attacks, user-configurable web filtering for parental control against network abuse etc.

1.1 Panel Explanation



LED	Status	Explanation
INTERNET/PPP	On	PPPoE connection is established.
WAN	On	WAN connection is established.
	Blinking	Data is transmitting (sending/receiving).
LAN	On	A normal connection is through its corresponding port.
	Blinking	Data is transmitting (sending/receiving).
Power	On	The router is powered on.
	Off	The router is powered off.

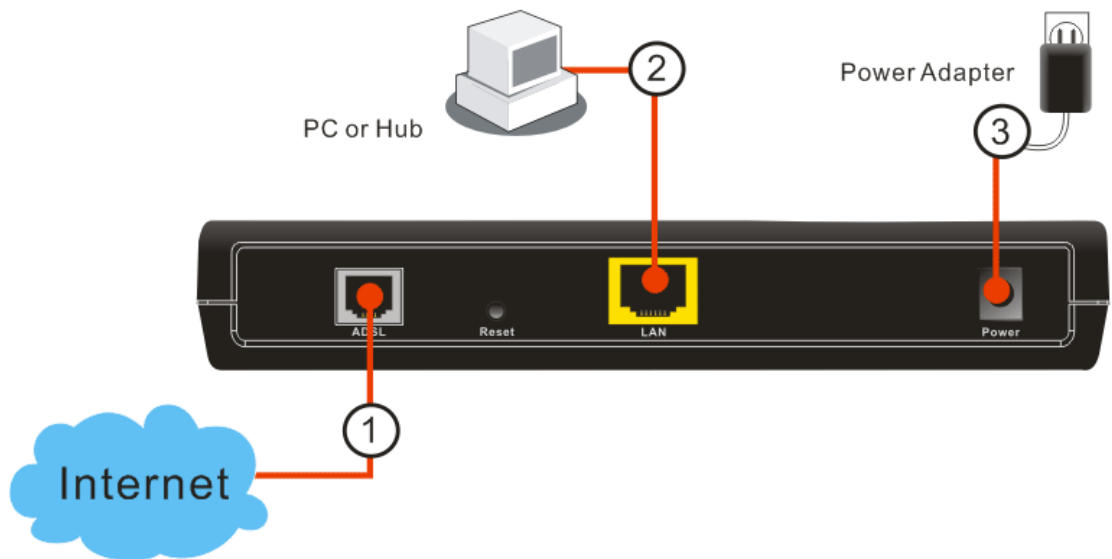


Interface	Description
ADSL	Connector for accessing the Internet through ADSL 2+.
Reset	Restore the default settings. Usage: Turn on the router. Press the button and keep for more than 10 seconds. Then the router will restart with the factory default configuration.
LAN	Connector for local networked devices.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

1.2 Hardware Installation

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

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



2

Configuring Basic Settings

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

This chapter explains how to setup a password for an administrator and how to adjust basic settings for accessing Internet successfully. Be aware that only the administrator can change the router configuration.

2.1 Changing Password

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

1. Make sure your computer connects to the router correctly.

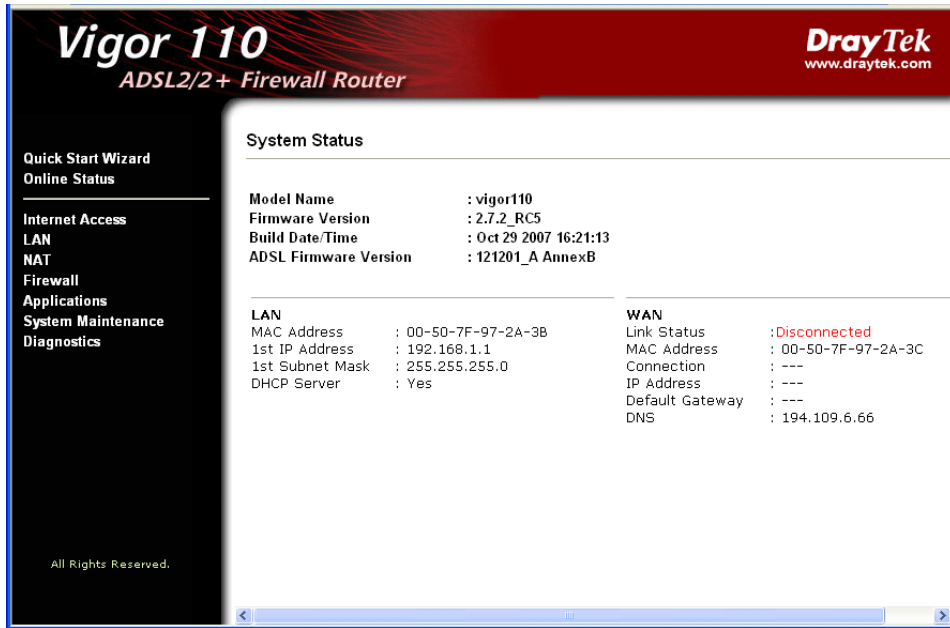


Notice: You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be the same subnet as **the default IP address of Vigor router 192.168.1.1**. For the detailed information, please refer to the later section - Trouble Shooting of this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

2. Open a web browser on your PC and type **http://192.168.1.1**. A pop-up window will open to ask for username and password. Please type default values (both username and password are Null) on the window for the first time accessing and click **OK** for next screen.



- Now, the **Main Screen** will pop up.



- Go to **System Maintenance** page and choose **Administrator Password**.

System Maintenance >> Administrator Password Setup

Administrator Password

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

- Enter the login password (the default is blank) on the field of **Old Password**. Type a new one in the field of **New Password** and retype it on the field of **Retype New Password**. Then click **OK** to continue.
- Now, the password has been changed. Next time, use the new password to access the Web Configurator for this router.



2.2 Quick Start Wizard

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

Quick Start Wizard

1. Enter login password

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

New Password

Confirm Password

< Back Next > Finish Cancel

2.2.1 Adjusting Protocol/Encapsulation

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

Quick Start Wizard

2. Connect to Internet

VPI

VCI

Protocol / Encapsulation

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 router according to the settings that your ISP provided.

VPI

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

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

2.2.2 PPPoE/PPPoA

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

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

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

Quick Start Wizard

3. Set PPPoE / PPPoA

ISP Name	<input type="text"/>
User Name	<input type="text" value="84005755@hinet.net"/>
Password	<input type="password" value="••••••••"/>
Confirm Password	<input type="password" value="••••••••"/>
<input checked="" type="checkbox"/> Always On	
Idle Timeout	<input type="text" value="-1"/> Seconds

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

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

Quick Start Wizard

4. Please confirm your settings:

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

Click **Finish**.

2.2.3 Bridged IP

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

Quick Start Wizard

2. 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 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"/>	

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

Quick Start Wizard

4. Please confirm your settings:

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

Click **Finish**.

2.2.4 Routed IP

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

Quick Start Wizard

2. Connect to Internet

VPI	<input type="text" value="0"/>	<input type="button" value="Auto detect"/>
VCI	<input type="text" value="34"/>	
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" value="0.0.0.0"/>	
Subnet Mask	<input type="text" value="0.0.0.0"/>	
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

4. Please confirm your settings:

VPI	:	0
VCI	:	34
Protocol / Encapsulation	:	1483 Route LLC
Fixed IP	:	No
Primary DNS	:	
Secondary DNS	:	

Click **Finish**.

2.3 Online Status

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

Online Status

System Status			System Uptime:19:15:2			
LAN Status		Primary DNS: 194.109.6.66		Secondary DNS: 194.98.0.1		
IP Address	TX Packets	RX Packets				
192.168.1.1	1102	112391				
WAN Status			GW IP Addr: ---			<input type="button" value="Dial PPPoE"/>
Mode	IP Address	TX Packets	TX Rate	RX Packets	RX Rate	Up Time
---	---	0	0	0	0	00:00:00
Message [PPP Shutdown]						
ADSL Information			(ADSL Firmware Version: 121201_A)			
ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks		
	0	0	0	0		
ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	----	READY	0	0	0	0

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

2.4 Saving Configuration

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



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

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

3

Advanced Web Configuration

After finished basic configuration of the router, you can access Internet with ease. For the people who want to adjust more settings for suiting his/her request, please refer to this chapter for getting detailed information about the advanced configuration of this router. As for other examples of application, please refer to Chapter 4.

3.1 Internet Access

3.1.1 Basics of Internet Protocol (IP) Network

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

From 10.0.0.0 to 10.255.255.255

From 172.16.0.0 to 172.31.255.255

From 192.168.0.0 to 192.168.255.255

What are Public IP Address and Private IP Address

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

Get Your Public IP Address from ISP

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

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

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

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

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

Internet Access >> PPPoE / PPPoA

PPPoE / PPPoA Client Mode

PPPoE/PPPoA Client Enable Disable

DSL Modem Settings

VPI

VCI

Encapsulating Type

Protocol

Modulation

PPPoE Pass-through

For Wired LAN

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

ISP Access Setup

ISP Name

Username

Password

PPP Authentication

Always On

Idle Timeout second(s)

IP Address From ISP

Fixed IP Yes No (Dynamic IP)

Fixed IP Address

Default MAC Address

Specify a MAC Address

MAC Address:

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

=> , , ,

OK

PPPoE/PPPoA Client Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.

DSL Modem Settings Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP.

VPI - Type in the value provided by ISP.

VCI - Type in the value provided by ISP.

Encapsulating Type - Drop down the list to choose the type provided by ISP.

Protocol - Drop down the list to choose the one provided by ISP.

If you have already used **Quick Start Wizard** to set the protocol, then it is not necessary for you to change any settings in this group.

PPPoE Pass-through The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your

ISP via the Vigor router.

For Wired LAN – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet.

ISP Access Setup

Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check **Always On**.

ISP Name – Type in the ISP Name provided by ISP in this field.

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

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

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

Always On – Check this box if you want the router keeping connecting to Internet forever.

Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action.

IP Address From ISP

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

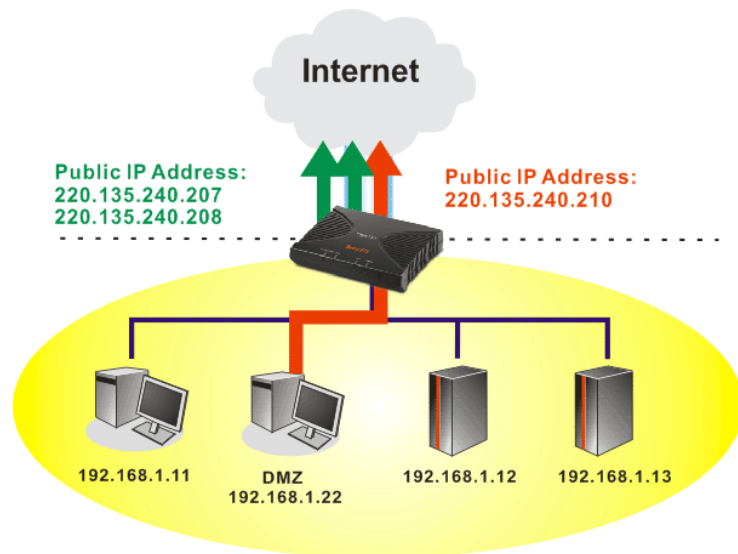
Fixed IP – Click **Yes** to use this function and type in a fixed IP address in the box.

WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.

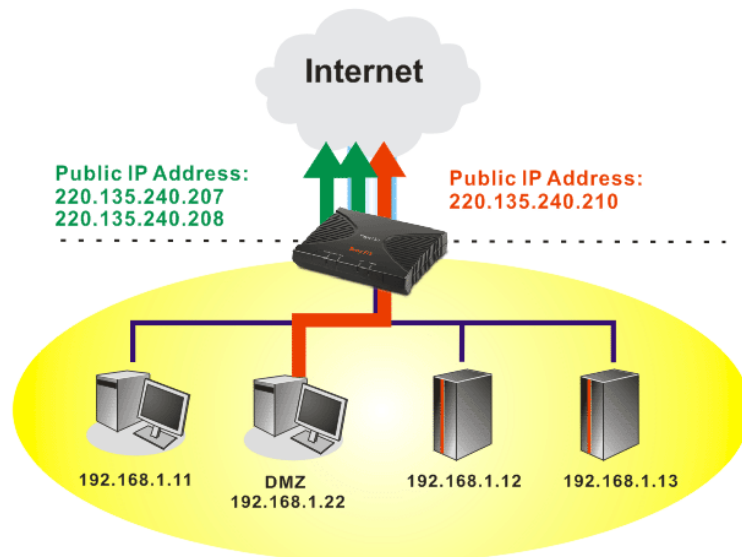
Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	<input checked="" type="checkbox"/>	---	<input checked="" type="checkbox"/>
2.	<input type="checkbox"/>	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	<input type="checkbox"/>
3.	<input type="checkbox"/>	<input type="text"/>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

OK Clear All Close

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



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



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

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

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

3.1.3 MPoA

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

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

Internet Access >> MPoA (RFC1483/2684)

MPoA (RFC1483/2684) Mode
 Enable Disable

DSL Modem Settings
Encapsulation: 1483 Routed IP LLC
VPI: 0
VCI: 34
Modulation: Multimode

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: 0.0.0.0
Subnet Mask: 0.0.0.0
Gateway IP Address:

Default MAC Address
 Specify a MAC Address
MAC Address: 00 .50 .7F .97 .2A .3C

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.

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.

Bridge Mode

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

WAN IP Network Settings

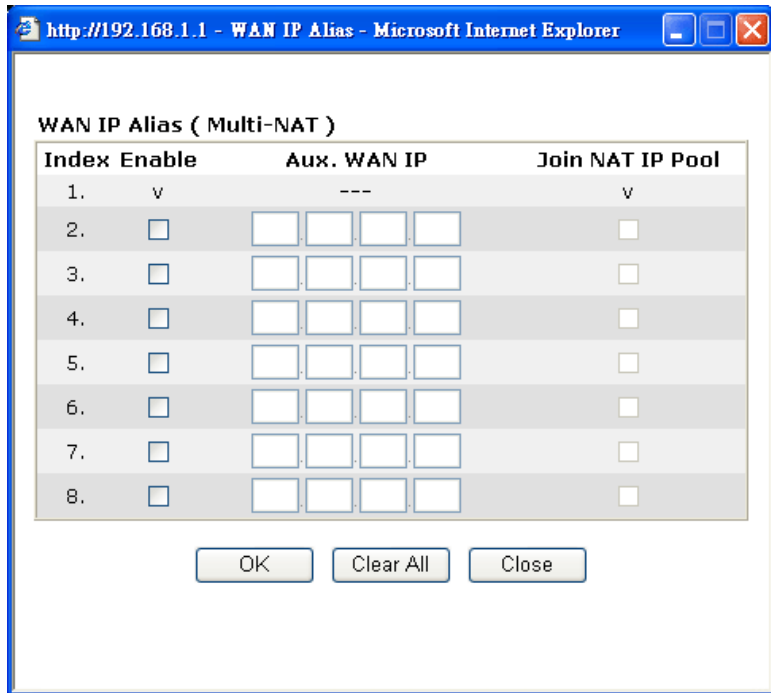
This group allows you to obtain an IP address automatically and allows you type in IP address manually.

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

Router Name – Type in the router name provided by ISP.

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

WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.



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

IP Address – Type in the private IP address.

Subnet Mask – Type in the subnet mask.

Gateway IP Address – Type in gateway IP address.

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

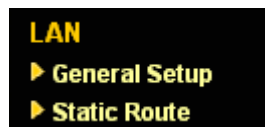
DNS Server IP Address Type in the primary IP address for the router. If necessary, type in secondary IP address for necessity in the future.

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

3.2 LAN

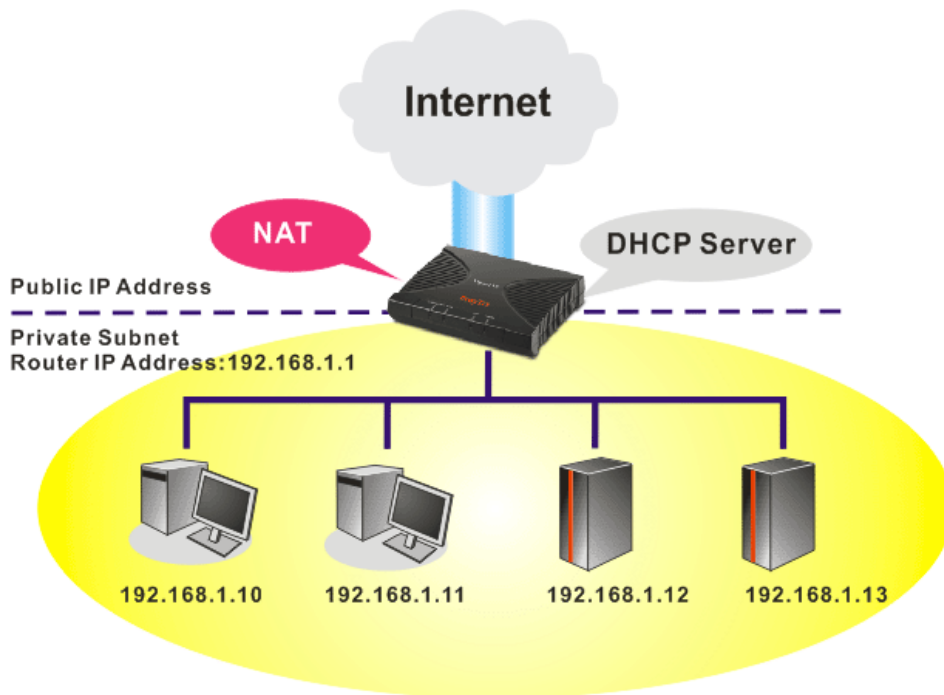
Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

Below shows menu items for LAN:



3.2.1 Basics of LAN

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



What is Routing Information Protocol (RIP)

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

What is Static Route

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

3.2.2 General Setup

This page provides you the general settings for LAN.

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

LAN >> General Setup

Ethernet TCP / IP and DHCP Setup	
LAN IP Network Configuration	
For NAT Usage	
IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
DHCP Server Configuration	
<input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server	
Relay Agent: <input type="radio"/> 1st Subnet	
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="192.168.1.1"/>
DHCP Server IP Address for Relay Agent	<input type="text"/>
<input type="button" value="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 router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.

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

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

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

Relay Agent – Specify the subnet that DHCP server is located the relay agent should redirect the DHCP request to.

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

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

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

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

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			View Routing Table		
Index	Destination Address	Status	Index	Destination Address	Status
<u>1.</u>	???	?	<u>6.</u>	???	?
<u>2.</u>	???	?	<u>7.</u>	???	?
<u>3.</u>	???	?	<u>8.</u>	???	?
<u>4.</u>	???	?	<u>9.</u>	???	?
<u>5.</u>	???	?	<u>10.</u>	???	?

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

Index The number (1 to 10) under Index allows you to open next page to setup static route.

Destination Address Displays the destination address of the static route.

Status Displays the status of the static route.

Viewing Routing Table Displays the routing table for your reference.

Diagnostics >> View Routing Table

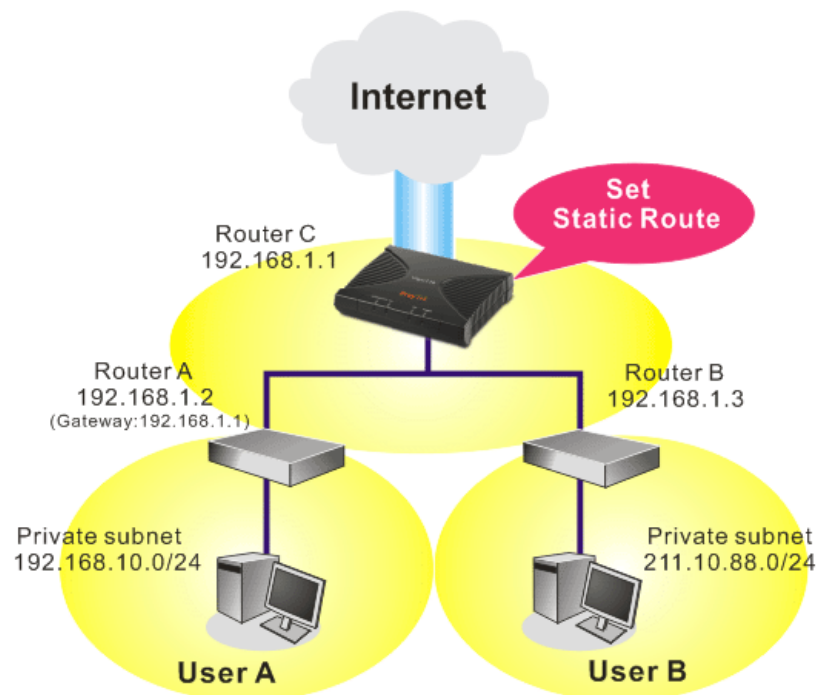
```
Current Running Routing Table Refresh  
Key: C - connected, S - static, R - RIP, * - default, ~ - private  
C~      192.168.1.0/  255.255.255.0 is directly connected, IF0
```

Add Static Routes to Private and Public Networks

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

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

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



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

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

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

LAN >> Static Route Setup

Index No. 1

Status/Action	Active/Add
Destination IP Address	192.168.10.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.2
Network Interface	LAN

3. Return to **Static Route Setup** page. Click on another **Index Number** to add another static route as show below, which regulates all packets destined to 211.100.88.0 will be forwarded to 192.168.1.3.

LAN >> Static Route Setup

Index No. 2

Status/Action	Active/Add
Destination IP Address	211.100.88.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.3
Network Interface	LAN

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

Diagnostics >> View 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, IFO
C~      192.168.1.0/      255.255.255.0 is directly connected, IFO
S~      211.100.88.0/     255.255.255.0 via 192.168.1.3, IFO
```

Disable Static Route

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

LAN >> Static Route Setup

Index No. 1

Status/Action	Active/Add
Destination IP Address	Empty/Clear
Subnet Mask	Active/Add
Gateway IP Address	192.168.1.2
Network Interface	LAN

OK

Cancel

3.3 NAT

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

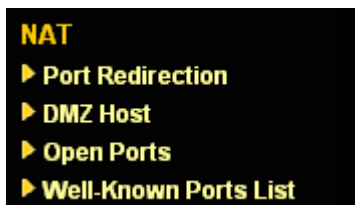
When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize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

The benefit of the NAT includes:

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

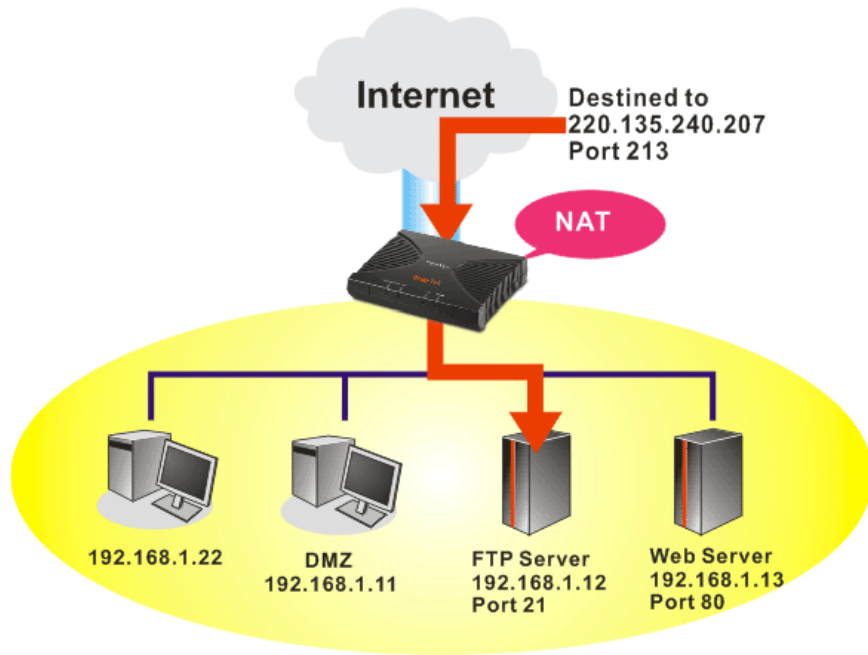
Note: On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved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

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 router, and identified by its private IP address/port, the goal of Port Redirection function is to forward all access request with public IP address from external users to the mapping private IP address/port of the server.



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

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

NAT >> Configure Port Redirection Table

Port Redirection Table

Index	Service Name	Protocol	Public Port	Private IP	Private Port	Active
1	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
2	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
3	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
4	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
5	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
6	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
7	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
8	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
9	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
10	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>

Service Name

Enter the description of the specific network service.

Protocol

Select the transport layer protocol (TCP or UDP).

Public Port

Specify which port can be redirected to the specified **Private IP and Port** of the internal host.

- Private IP** Specify the private IP address of the internal host providing the service.
- Private Port** Specify the private port number of the service offered by the internal host.
- Active** Check this box to activate the port-mapping entry you have defined.

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

For example, the built-in web configurator in the router is with default port 80, which may conflict with the web server in the local network, http://192.168.1.13:80. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080. This can be set in the **System Maintenance >>Management 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.

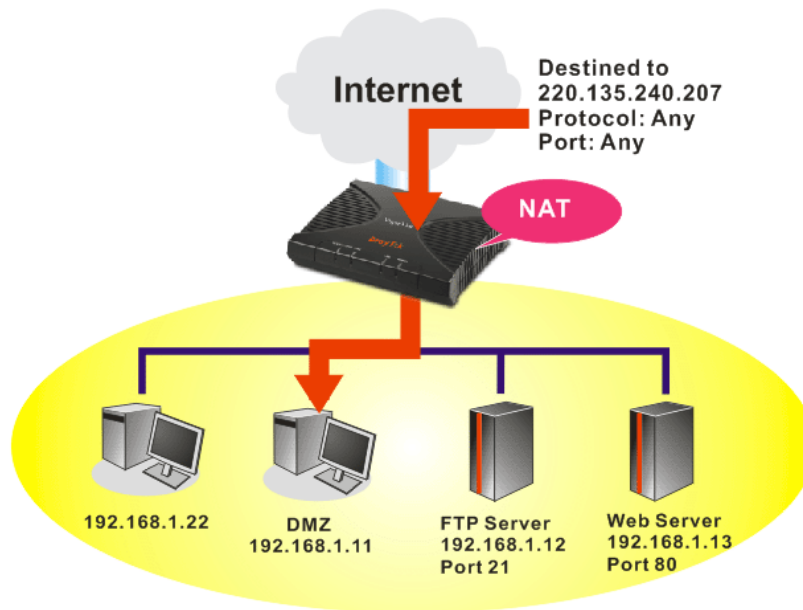
System Maintenance >> Management

Management Setup

<p>Management Access Control</p> <p><input type="checkbox"/> Enable remote firmware upgrade(FTP)</p> <p><input type="checkbox"/> Allow management from the Internet</p> <p><input checked="" type="checkbox"/> Disable PING from the Internet</p> <hr/> <p>Access List</p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">List</th> <th style="text-align: left;">IP</th> <th style="text-align: left;">Subnet Mask</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input style="width: 100%;" type="text"/></td> <td><input style="width: 100%;" type="text"/> <input type="button" value="v"/></td> </tr> <tr> <td>2</td> <td><input style="width: 100%;" type="text"/></td> <td><input style="width: 100%;" type="text"/> <input type="button" value="v"/></td> </tr> <tr> <td>3</td> <td><input style="width: 100%;" type="text"/></td> <td><input style="width: 100%;" type="text"/> <input type="button" value="v"/></td> </tr> </tbody> </table>	List	IP	Subnet Mask	1	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/> <input type="button" value="v"/>	2	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/> <input type="button" value="v"/>	3	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/> <input type="button" value="v"/>	<p>Management Port Setup</p> <p><input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports</p> <p>Telnet Port <input style="width: 50px;" type="text" value="23"/> (Default: 23)</p> <p>HTTP Port <input style="width: 50px;" type="text" value="80"/> (Default: 80)</p> <p>FTP Port <input style="width: 50px;" type="text" value="21"/> (Default: 21)</p> <hr/> <p>SNMP Setup</p> <p><input type="checkbox"/> Enable SNMP Agent</p> <p>Get Community <input style="width: 100%;" type="text" value="public"/></p> <p>Set Community <input style="width: 100%;" type="text" value="private"/></p> <p>Manager Host IP <input style="width: 100%;" type="text"/></p> <p>Trap Community <input style="width: 100%;" type="text" value="public"/></p> <p>Notification Host IP <input style="width: 100%;" type="text"/></p> <p>Trap Timeout <input style="width: 50px;" type="text" value="10"/> seconds</p>
List	IP	Subnet Mask											
1	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/> <input type="button" value="v"/>											
2	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/> <input type="button" value="v"/>											
3	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/> <input type="button" value="v"/>											

3.3.2 DMZ Host

As mentioned above, **Port Redirection** can redirect incoming TCP/UDP or other traffic on particular ports to the specific private IP address/port of host in the LAN. However, other IP protocols, for example Protocols 50 (ESP) and 51 (AH), do not travel on a fixed port. Vigor router provides a facility **DMZ Host** that 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.



Note: 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

Private IP

Private IP

MAC Address of the True IP DMZ Host

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

DMZ Host

You can set Private IP or Active True IP as the DMZ host.

Active True IP

None

Private IP

Active True IP

Private IP

If you choose Private IP as the selection for DMZ host, please type in private IP or select any one by clicking the Choose PC button.

MAC Address of the True IP DMZ Host

If you choose Active True IP as the selection for DMZ host, please type in MAC address in these fields.

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

NAT >> DMZ Host Setup

DMZ Host Setup

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

Enable

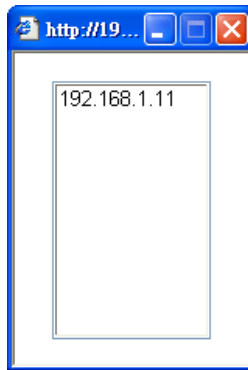
Check to enable the DMZ Host function.

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

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

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 Setup

Open Ports Setup

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

Clear All

- Index** Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
- Comment** Specify the name for the defined network service.
- Aux. WAN IP** Display the private IP address of the local host that you specify in WAN Alias.
- Local IP Address** Display the private IP address of the local host offering the service.
- Status** Display the state for the corresponding entry. X or V is to represent the **Inactive** or **Active** state.

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

NAT >> Open Ports Setup >> Edit Open Ports Setup

Index No. 1

Enable Open Ports

Comment: WAN IP:

Local Computer:

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	TCP	4500	4700	6.	-----	0	0
2.	UDP	4500	4700	7.	-----	0	0
3.	-----	0	0	8.	-----	0	0
4.	-----	0	0	9.	-----	0	0
5.	-----	0	0	10.	-----	0	0

OK Clear Cancel

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

- Enable Open Ports** Check to enable this entry.
- Comment** Make a name for the defined network application/service.

- Local Computer** Enter the private IP address of the local host or click Choose PC to select one.
- Choose PC** Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.
- Protocol** Specify the transport layer protocol. It could be **TCP**, **UDP**, or **-----** (none) for selection.
- Start Port** Specify the starting port number of the service offered by the local host.
- End Port** Specify the ending port number of the service offered by the local host.

NAT >> Open Ports Setup

Open Ports Setup

Index	Comment	Aux. WAN IP	Local IP Address	Status
1.	P2P-Emule	192.168.1.55	192.168.1.10	v
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x

Clear All

3.3.4 Well-Known Ports List

This page provides you a view of well-known ports.

NAT >> View Well-Known Ports List

Well-Known Ports List

Service/Application	Protocol	Port Number
File Transfer Protocol (FTP)	TCP	21
SSH Remote Login Protocol (ex. pcAnywhere)	UDP	22
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name Server (DNS)	UDP	53
WWW Server (HTTP)	TCP	80
Post Office Protocol ver.3 (POP3)	TCP	110
Network News Transfer Protocol (NNTP)	TCP	119
Point-to-Point Tunneling Protocol (PPTP)	TCP	1723
pcANYWHEREdata	TCP	5631
pcANYWHEREstat	UDP	5632
WinVNC	TCP	5900

3.4 Firewall

3.4.1 Basics for Firewall

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

The most basic security concept is to set user name and password while you install your router. The administrator login will prevent unauthorized access to the router configuration from your router.

Quick Start Wizard

1. Enter login password

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

New Password

Confirm Password

If you did not set password during installation; you can go to **System Maintenance** to set up your password.

System Maintenance >> Administrator Password Setup

Administrator Password

Old Password

New Password

Retype New Password

IP Filters

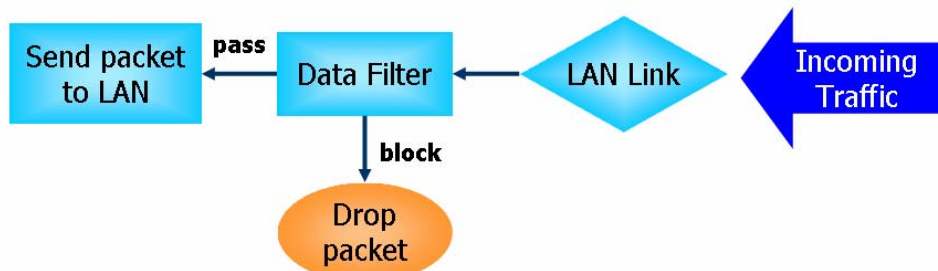
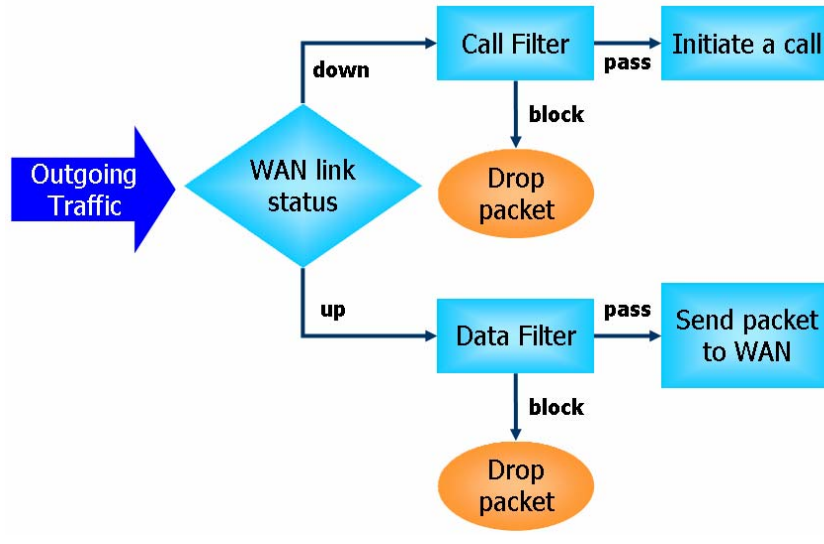
Depending on whether there is an existing Internet connection, or in other words “the WAN link status is up or down”, the IP filter architecture categorizes traffic into two: **Call Filter** and **Data Filter**.

- **Call Filter** - When there is no existing Internet connection, **Call Filter** is applied to all traffic, all of which should be outgoing. It will check packets according to the filter rules.

If legal, the packet will pass. Then the router shall **“initiate a call”** to build the Internet connection and send the packet to Internet.

- **Data Filter** - When there is an existing Internet connection, **Data Filter** is applied to incoming and outgoing traffic. It will check packets according to the filter rules. If legal, the packet will pass the router.

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



Stateful Packet Inspection (SPI)

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

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

As the popularity of all kinds of instant messenger application arises, communication cannot become much easier. Nevertheless, while some industry may leverage this as a great tool to connect with their customers, some industry may take reserve attitude in order to reduce employee misuse during office hour or prevent unknown security leak. It is similar situation for corporation towards peer-to-peer applications since file-sharing can be convenient but insecure at the same time. To address these needs, we provide IM and P2P blocking functionality.

Denial of Service (DoS) Defense

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

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

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

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

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

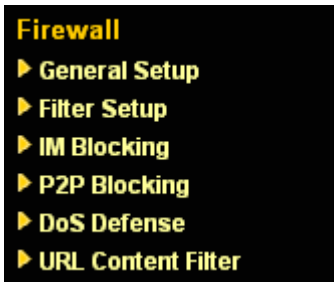
URL Content Filtering

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

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

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

Below shows the menu items of Firewall:



3.4.2 General Setup

General Setup allows you to adjust settings of IP Filter and common options. Here you can enable or disable the **Call Filter** or **Data Filter**. Under some circumstance, your filter set can be linked to work in a serial manner. So here you assign the **Start Filter Set** only. Also you can configure the **Log Flag** settings, **Enable Stateful packet inspection**, **Drop non-http connection on TCP port 80**, and **Accept incoming fragmented UDP packets**.

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

Firewall >> General Setup

General Setup

Call Filter	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Start Filter Set Set#1 ▼
Data Filter	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Start Filter Set Set#2 ▼
Log Flag	None ▼	

Enable stateful packet inspection
 Drop non-http connection on TCP port 80
 Accept incoming fragmented UDP packets (for some games, ex. CS)

OK

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

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

Log Flag For troubleshooting needs you can specify the filter log here.
None - The log function is not activated.
Block - All blocked packets will be logged.
Pass - All passed packets will be logged.
No Match - The log function will record all packets that are not matched.
 Note that the filter log will be displayed on the Telnet terminal when you type the *log -f* command.

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

3.4.3 Filter Setup

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

Firewall >> Filter Setup

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

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
<input type="button" value="1"/>	<input checked="" type="checkbox"/>	Block NetBios
<input type="button" value="2"/>	<input type="checkbox"/>	
<input type="button" value="3"/>	<input type="checkbox"/>	
<input type="button" value="4"/>	<input type="checkbox"/>	
<input type="button" value="5"/>	<input type="checkbox"/>	
<input type="button" value="6"/>	<input type="checkbox"/>	
<input type="button" value="7"/>	<input type="checkbox"/>	

Next Filter Set

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

Active Enable or disable the filter rule.

Comment Enter filter set comments/description. Maximum length is 23-character long

Next Filter Set Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.

(=) If the End Port is empty, the filter rule will set the port number to be the value of the Start Port. Otherwise, the port number ranges between the Start Port and the End Port (including the Start Port and the End Port).

(!=) If the End Port is empty, the port number is not equal to the value of the Start Port. Otherwise, this port number is not between the Start Port and the End Port (including the Start Port and End Port).

(>) Specify the port number is larger than the Start Port (includes the Start Port).

(<) Specify the port number is less than the Start Port (includes the Start Port).

Keep State

This function should work along with Direction, Protocol, IP address, Subnet Mask, Operator, Start Port and End Port settings. It is used for Data Filter only.

Keep State is in the same nature of modern term Stateful Packet Inspection. It tracks packets, and accept the packets with appropriate characteristics showing its state is legal as the protocol defines. It will deny unsolicited incoming data. You may select protocols from any, TCP, UDP, TCP/UDP, ICMP and IGMP.

Fragments

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

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

Unfragmented - Apply the rule to unfragmented packets.

Fragmented - Apply the rule to fragmented packets.

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

Example

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

Log Flag None

Enable stateful packet inspection

Drop non-http connection on TCP port 80

Accept incoming fragmented UDP packets (for some games, ex. C)

OK

Firewall >> Filter Setup

Filter Setup | Set to Factory Default |

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

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1

Comments : Default Call Filter

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

OK Clear Cancel

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 1

Comments : Block NetBios Check to enable the Filter Rule

Pass or Block: Block Immediately Branch to Other Filter Set: None Log

Direction: IN Protocol: TCP/UDP

	IP Address	Subnet Mask	Operator	Start Port	End Port
Source	any	255.255.255.255 (32)	=	137	139
Destination	any	255.255.255.255 (32)	=		

Keep State Fragments: Don't Care

OK Clear Cancel

3.4.4 IM Blocking

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

Firewall >> IM Blocking Setup

Instant Messenger Applications Blocking Setup

Enable IM Blocking

Block MSN Messenger

Block Yahoo Messenger

Block ICQ/AOL

Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

3.4.5 P2P Blocking

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

Firewall >> P2P Blocking Setup

Peer-to-Peer file-sharing Applications Blocking Setup

Enable P2P Blocking

Protocol	Applications	Action
eDonkey	eDonkey, eMule, Shareaza, MLDonkey	<input checked="" type="radio"/> Allow <input type="radio"/> Disallow <input type="radio"/> Disallow upload
FastTrack	KazaA, iMesh, MLDonkey	<input checked="" type="radio"/> Allow <input type="radio"/> Disallow
Gnutella	BearShare, Gnucleus, Limewire, Phex, Swapper, XoloX, Shareaza, MLDonkey	<input checked="" type="radio"/> Allow <input type="radio"/> Disallow
BitTorrent	BitTorrent	<input checked="" type="radio"/> Allow <input type="radio"/> Disallow

Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

Action

Specify the action for each protocol.

Allow – Allow the client to access into the application through the specified protocol.

Disallow – Forbid the client to access into the application through the specified protocol.

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

3.4.6 DoS Defense

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

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

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

Block IP options Block TCP flag scan
 Block Land Block Tear Drop
 Block Smurf Block Ping of Death
 Block trace route Block ICMP fragment
 Block SYN fragment Block UnknownProtocol
 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 router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router. By default, the threshold and timeout values are set to 50 packets per second and 10 seconds, respectively.

Enable UDP flood defense

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

Enable ICMP flood defense

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

Enable PortScan detection	Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning. By default, the Vigor router sets the threshold as 150 packets per second.
Block IP options	Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages...etc. An eavesdropper outside might learn the details of your private networks.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.
Block trace router	Check the box to enforce the Vigor router not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.
Block Fraggle Attack	Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked. Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.
Block TCP flag scan	Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include <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> .
Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.

Block Land

Check the box to enforce the Vigor router to defend the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.

Block Unknown Protocol

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

Warning Messages

We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client. (Refer to Chapter 13 System Maintenance Syslog Access Setup for detail information.)

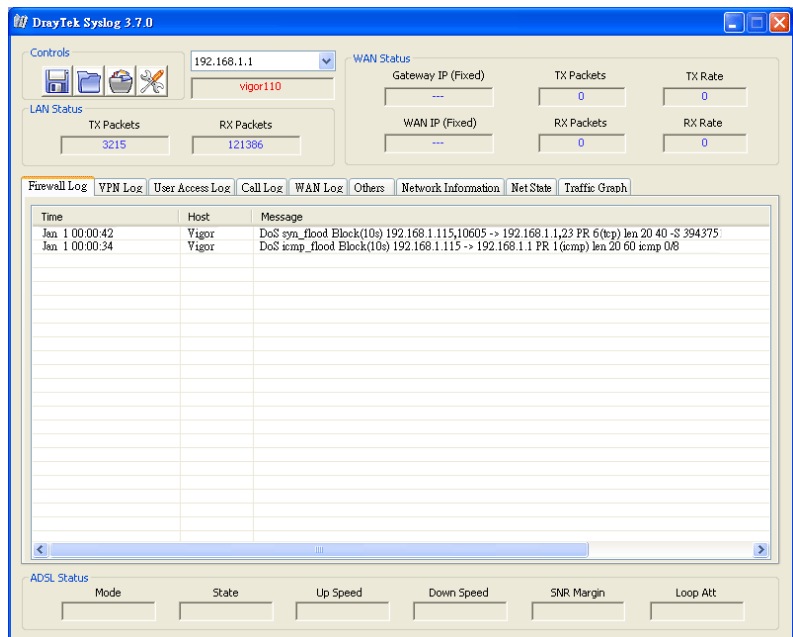
All the warning messages related to **DoS defense** will be sent to user and user can review it through Syslog daemon. Look for the keyword **DoS** in the message, followed by a name to indicate what kind of attacks is detected.

System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

SysLog Access Setup	Mail Alert Setup
<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
Server IP Address: 192.168.1.10	SMTP Server: <input type="text"/>
Destination Port: 514	Mail To: <input type="text"/>
Enable syslog message:	Return-Path: <input type="text"/>
<input checked="" type="checkbox"/> Firewall Log	<input type="checkbox"/> Authentication
<input checked="" type="checkbox"/> VPN Log	User Name: <input type="text"/>
<input checked="" type="checkbox"/> User Access Log	Password: <input type="text"/>
<input checked="" type="checkbox"/> Call Log	
<input checked="" type="checkbox"/> WAN Log	
<input checked="" type="checkbox"/> Router/DSL information	

OK Clear Cancel



3.4.7 URL Content Filter

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

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

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

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

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.

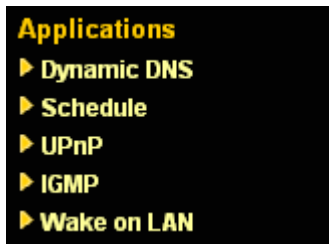
Black List (block those matching keyword) Click this button to restrict accessing into the corresponding webpage with the keywords listed on the box below.

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	<p>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.</p> <p>You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.</p>
Enable Restrict Web Feature	<p>Check the box to activate the function.</p> <p>Java - Check the checkbox to activate the Block Java object function. The Vigor router will discard the Java objects from the Internet.</p> <p>ActiveX - Check the box to activate the Block ActiveX object function. Any ActiveX object from the Internet will be refused.</p> <p>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. .</p> <p>zip, rar, .arj, .ace, .cab, .sit</p> <p>Executable file - Check the box to reject any downloading behavior of the executable file from the Internet.</p> <p>.exe, .com, .scr, .pif, .bas, .bat, .inf, .reg</p> <p>Cookie - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy.</p> <p>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.</p> <p>.mov .mp3 .rm .ra .au .wmv .wav .asf .mpg .mpeg .avi .ram</p>
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 <i>URL Access Control</i> . 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 Applications

Below shows the menu items of Application:



3.5.1 Dynamic DNS

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

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

Enable the Function and Add a Dynamic DNS Account

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

Applications >> Dynamic DNS Setup

Dynamic DNS Setup

Enable Dynamic DNS Setup

Accounts :

Index	Domain Name	Active
<u>1.</u>	---	×
<u>2.</u>	---	×
<u>3.</u>	---	×

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 router updates its information to DDNS server.

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

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

Index : 1

Enable Dynamic DNS Account

Service Provider:

Service Type:

Domain Name: .

Login Name: (max. 23 characters)

Password: (max. 23 characters)

Wildcards

Backup MX

Mail Extender:

OK Clear Cancel

Enable Dynamic DNS Account Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).

Service Provider Select the service provider for the DDNS account.

Service Type Select a service type (Dynamic, Custom, Static).

Domain Name Type in a domain name that you applied previously.

Login Name Type in the login name that you set for applying domain.

Password Type in the password that you set for applying domain.

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

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

Disable the Function and Clear all Dynamic DNS Accounts

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

Delete a Dynamic DNS Account

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

3.5.2 Schedule

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

You have to set your time before set schedule. In **System Maintenance>> Time Setup** menu, press **Inquire Time** button to set the Vigor router's clock to current time of your PC. The clock will reset once if you power down or reset the router. There is another way to set up time. You can inquiry an NTP server (a time server) on the Internet to synchronize the router's clock. This method can only be applied when the WAN connection has been built up.

Applications >> Schedule

Schedule:

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

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

Clear All

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

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.

3.5.3 UPnP

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

Applications >> UPnP

UPnP

Enable UPnP Service

Enable Connection control Service

Enable Connection Status Service

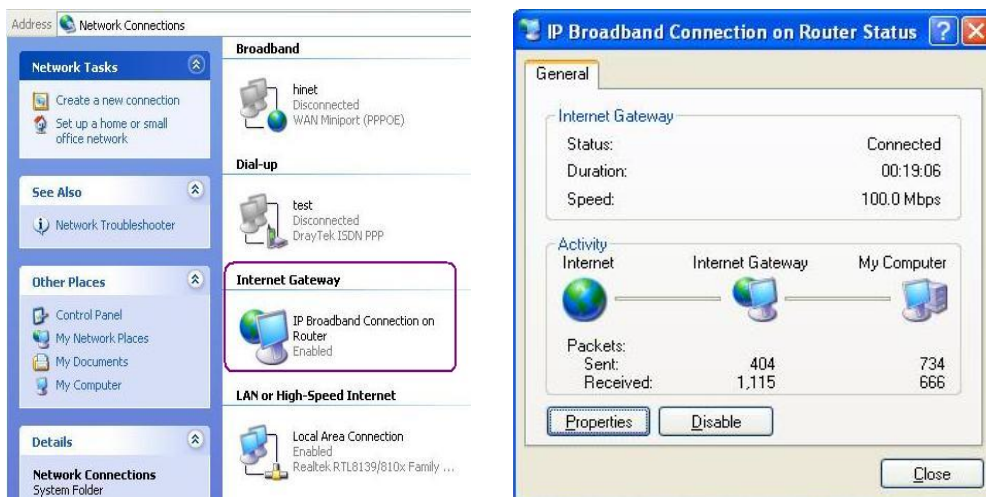
Note: If you intend running UPnP service inside your LAN, you should check the appropriate service above to allow control, as well as the appropriate UPnP settings.

OK Clear Cancel

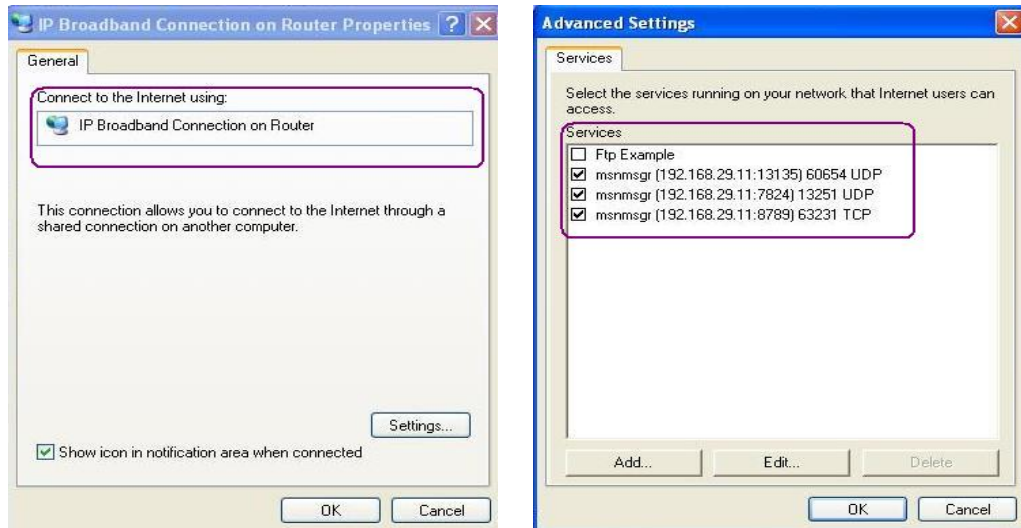
Enable UPNP Service

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 Router** on Windows XP/Network Connections will appear. The connection status and control status will be able to be activated. The NAT Traversal of UPnP enables the multimedia features of your applications to operate. This has to manually set up port mappings or use other similar methods. The screenshots below show examples of this facility.



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



The reminder as regards concern about Firewall and UPnP:

Can't work with Firewall Software

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

Security Considerations

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

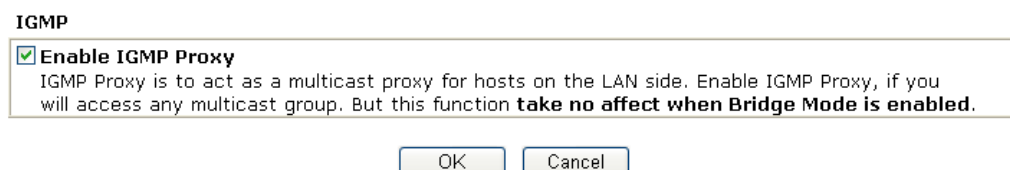
- Some Microsoft operating systems have found out the UPnP weaknesses and hence you need to ensure that you have applied the latest service packs and patches.
- Non-privileged users can control some router functions, including removing and adding port mappings.

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

3.5.4 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. For invoking IGMP Snooping function, you have to check the Enable IGMP Proxy box first for activating the IGMP proxy function.

Applications >> IGMP



Enable IGMP Proxy

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

3.5.5 Wake on LAN

A PC client on LAN can be woken up by the router it connects. When a user wants to wake up a specified PC through the router, he/she must type correct MAC address of the specified PC on this web page of **Wake On LAN** of this router.

In addition, such PC must have installed a network card supporting WOL function. By the way, WOL function must be set as “Enable” on the BIOS setting.

Application >> Wake on LAN

Wake on LAN

MAC Address: : : : : :

Result

MAC Address Type any one of the MAC address of the binded PCs.

Wake Up Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.

3.6 System Maintenance

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

3.6.1 System Status

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

System Status

Model Name : vigor110
Firmware Version : 2.7.2_RC4
Build Date/Time : Oct 23 2007 09:52:14
ADSL Firmware Version : 121201_A AnnexB

LAN
MAC Address : 00-50-7F-97-2A-3B
1st IP Address : 192.168.1.1
1st Subnet Mask : 255.255.255.0
DHCP Server : Yes

WAN
Link Status : **Disconnected**
MAC Address : 00-50-7F-97-2A-3C
Connection : ---
IP Address : ---
Default Gateway : ---
DNS : 194.109.6.66

Model Name Displays the model name of the router.

Firmware Version Displays the firmware version of the router.

Build Date/Time Displays the date and time of the current firmware build.

MAC Address Displays the MAC address of the LAN Interface.

1st IP Address Displays the IP address of the LAN interface.

1st Subnet Mask	Displays the subnet mask address of the LAN interface.
DHCP Server	Displays the current status of DHCP server of the LAN interface.
MAC Address	Displays the MAC address of the WAN Interface.
IP Address	Displays the IP address of the WAN interface.
Default Gateway	Displays the assigned IP address of the default gateway.
DNS	Displays the assigned IP address of the primary DNS.
MAC Address	Displays the MAC address of the wireless Interface.

3.6.2 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"/>
Retype New Password	<input type="text"/>

Old Password Type in the old password. The factory default setting for password is blank.

New Password Type in new password in this field.

Retype New Password Type in the new password again.

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

3.6.3 Configuration Backup

Backup the Configuration

Follow the steps below to backup your configuration.

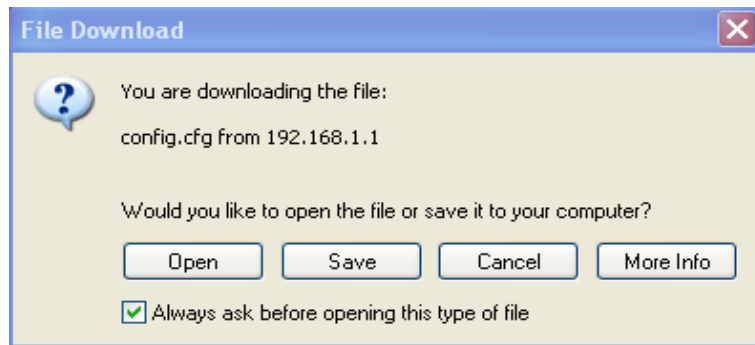
1. Go to **System Maintenance >> Configuration Backup**. The following windows will be popped-up, as shown below.

System Maintenance >> Configuration Backup

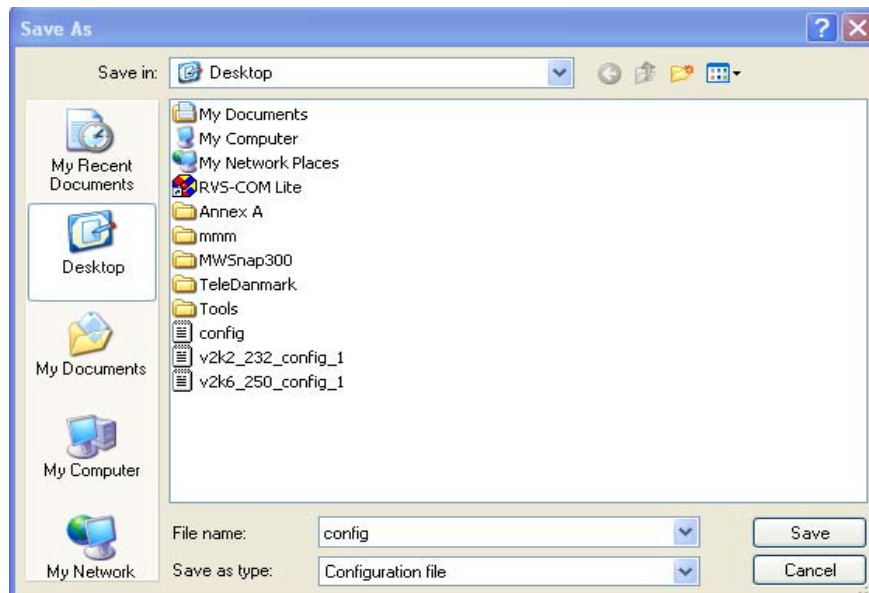
Configuration Backup / Restoration

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

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



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



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

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

Restore Configuration

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

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

3.6.4 Syslog/Mail Alert

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

System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

<p>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Server IP Address <input type="text" value="192.168.1.10"/></p> <p>Destination Port <input type="text" value="514"/></p> <p>Enable syslog message:</p> <p><input checked="" type="checkbox"/> Firewall Log</p> <p><input checked="" type="checkbox"/> VPN Log</p> <p><input checked="" type="checkbox"/> User Access Log</p> <p><input checked="" type="checkbox"/> Call Log</p> <p><input checked="" type="checkbox"/> WAN Log</p> <p><input checked="" type="checkbox"/> Router/DSL information</p>	<p>Mail Alert Setup</p> <p><input type="checkbox"/> Enable</p> <p>SMTP Server <input type="text"/></p> <p>Mail To <input type="text"/></p> <p>Return-Path <input type="text"/></p> <p><input type="checkbox"/> Authentication</p> <p>User Name <input type="text"/></p> <p>Password <input type="text"/></p>
--	---

- | | |
|------------------------------|---|
| Enable | Click “ Enable ” to activate this function. |
| 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, Router/DSL information to Syslog. |
| SMTP Server | The IP address of the SMTP server. |
| Mail To | Assign a mail address for sending mails out. |
| Return-Path | Assign a path for receiving the mail from outside. |
| Authentication | Check this box to activate this function while using e-mail application. |

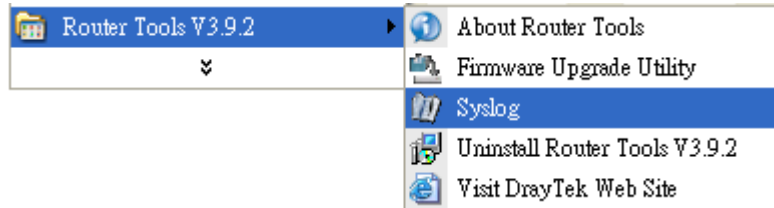
User Name Type the user name for authentication.

Password Type the password for authentication.

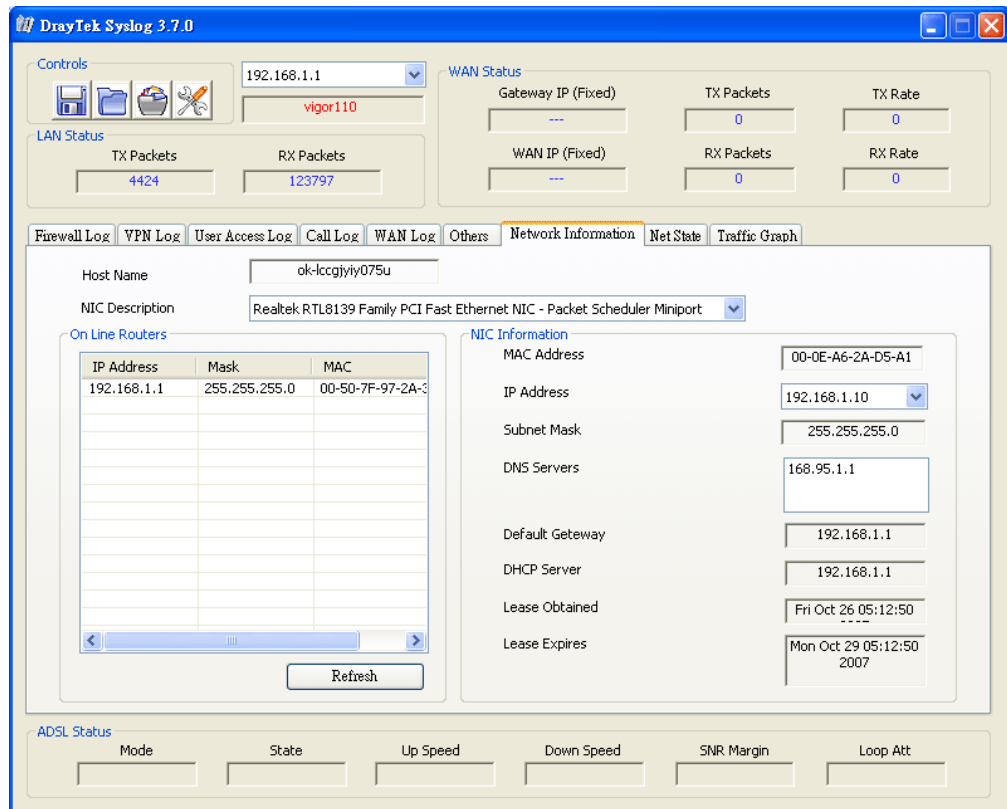
Click **OK** to save these settings.

For viewing the Syslog, please do the following:

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



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



3.6.5 Time and Date

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

System Maintenance >> Time and Date

Time Information

Current System Time	2000 Jan 1 Sat 21 : 55 : 20	Inquire Time
---------------------	-----------------------------	--------------

Time Setup

<input type="radio"/> Use Browser Time	
<input checked="" type="radio"/> Use Internet Time Client	
Time Protocol	NTP (RFC-1305) ▼
Server IP Address	
Time Zone	(GMT) Greenwich Mean Time : Dublin ▼
Enable Daylight Saving	<input type="checkbox"/>
Automatically Update Interval	30 sec ▼

OK Cancel

Current System Time Click **Inquire Time** to get the current time.

Use Browser Time Select this option to use the browser time from the remote administrator PC host as router's system time.

Use Internet Time Client Select to inquire time information from Time Server on the Internet using assigned protocol.

Time Protocol Select a time protocol.

Server IP Address Type the IP address of the time server.

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

Enable Daylight Saving Such function is useful for some area.

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

Click **OK** to save these settings.

3.6.6 Management

This page allows you to manage the settings for access control, access list, port setup, and SMP setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session.

System Maintenance >> Management

Management Setup

<p>Management Access Control</p> <input type="checkbox"/> Enable remote firmware upgrade(FTP) <input type="checkbox"/> Allow management from the Internet <input checked="" type="checkbox"/> Disable PING from the Internet		<p>Management Port Setup</p> <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports Telnet Port <input type="text" value="23"/> (Default: 23) HTTP Port <input type="text" value="80"/> (Default: 80) FTP Port <input type="text" value="21"/> (Default: 21)													
<p>Access List</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>SNMP Setup</p> <input type="checkbox"/> Enable SNMP Agent Get Community <input type="text" value="public"/> Set Community <input type="text" value="private"/> Manager Host IP <input type="text"/> Trap Community <input type="text" value="public"/> Notification Host IP <input type="text"/> Trap Timeout <input type="text" value="10"/> seconds	
List	IP	Subnet Mask													
1	<input type="text"/>	<input type="text"/>													
2	<input type="text"/>	<input type="text"/>													
3	<input type="text"/>	<input type="text"/>													

OK

Enable remote firmware upgrade

Click the checkbox to allow remote firmware upgrade through FTP (File Transfer Protocol).

Allow management from the Internet

Enable the checkbox to allow system administrators to login from the Internet. By default, it is not allowed.

Disable PING from the Internet

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

Access List

You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.

List IP - Indicate an IP address allowed to login to the router.

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

Default Ports

Check to use standard port numbers for the Telnet and HTTP servers.

User Defined Ports

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

Enable SNMP Agent

Check it to enable this function.

Get Community

Set the name for getting community by typing a proper character. The default setting is **public**.

Set Community

Set community by typing a proper name. The default setting is **private**.

Manager Host IP

Set one host as the manager to execute SNMP function. Please type in IP address to specify certain host.

- Trap Community** Set trap community by typing a proper name. The default setting is **public**.
- Notification Host IP** Set the IP address of the host that will receive the trap community.
- Trap Timeout** The default setting is 10 seconds.

3.6.7 Reboot System

The Web Configurator may be used to restart your router. 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 router using the current configuration, check **Using current configuration** and click **OK**. To reset the router settings to default values, check **Using factory default configuration** and click **OK**. The router will take 5 seconds to reboot the system.

3.6.8 Firmware Upgrade

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

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

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

System Maintenance >> Firmware Upgrade

Firmware Upgrade


Current Firmware Version : 2.7.2_RC4

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 ?

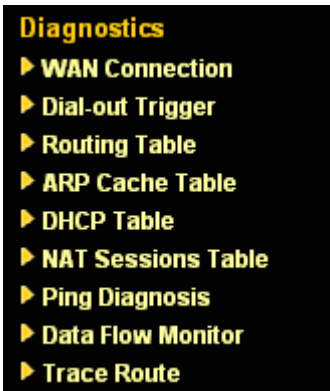
Click **OK**. The following screen will appear.

 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.

3.7 Diagnostics

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



3.7.1 WAN Connection

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

Diagnostics >> WAN Connection

PPPoE/PPPoA Diagnostics		Refresh
Broadband Access Mode/Status	---	
Internet Access	>> Dial PPPoE/PPPoA	
WAN IP Address	---	
Drop Connection	>> Drop PPPoE/PPPoA	

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

3.7.2 Dial-out Trigger

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

Diagnostics >> Dial-out Trigger

Dial-out Triggered Packet Header | Refresh |

HEX Format:
00 50 7F 97 2A 3B-00 0E A6 2A D5 A1-08 00

45 00 00 34 A7 49 40 00-7F 06 5B F3 C0 A8 01 0A
29 F9 0C DC 09 42 6E C9-DB 9F 22 FA 00 00 00 00
80 02 10 00 EF EB 00 00-02 04 05 B4 01 03 03 00
01 01 04 02 5F E4 80 3D-F6 11 00 00 01 0C 80 09
7B B4 00 00 00 00 00 00-00 00 00 00 00 00 00

Decoded Format:
192.168.1.10,2370 -> 41.249.12.220,28361
Pr tcp HLen 20 TLen 52 -S Seq 3684639482 Ack 0 Win 4096

Refresh

Click it to reload the page.

3.7.3 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, IFO
```

Refresh

Click it to reload the page.

3.7.4 ARP Cache Table

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

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

Clear Click it to clear the whole table.

Refresh Click it to reload the page.

3.7.5 DHCP Table

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

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

Diagnostics >> View DHCP Assigned IP Addresses

DHCP IP Assignment Table | [Refresh](#) |

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 router for specified PC.

MAC Address It displays the MAC address for the specified PC that DHCP assigned IP address for it.

Leased Time It displays the leased time of the specified PC.

HOST ID It displays the host ID name of the specified PC.

Refresh Click it to reload the page.

3.7.6 NAT Sessions Table

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

Diagnostics >> NAT Sessions Table

NAT Active Sessions Table | Refresh |

Private IP :Port	#Pseudo Port	Peer IP :Port	Info	Status
------------------	--------------	---------------	------	--------

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

#Pseudo Port It indicates the temporary port of the router used for NAT.

Peer IP:Port It indicates the destination IP address and port of remote host.

Interface It indicates the interface of the WAN connection.

Refresh Click it to reload the page.

3.7.7 Ping Diagnosis

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

Diagnostics >> Ping Diagnosis

Ping Diagnosis

Ping to: IP Address:

Result | Clear |

- Refresh** Click this link to refresh this page manually.
- Index** Display the number of the data flow.
- IP Address** Display the IP address of the monitored device.
- TX rate (kbps)** Display the transmission speed of the monitored device.
- RX rate (kbps)** Display the receiving speed of the monitored device.
- Sessions** Display the session number that you specified in Limit Session web page.
- Action** **Block** - can prevent specified PC accessing into Internet within 5 minutes.

Page: 1 | Refresh |

	Sessions	Action
	4	Block

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

Page: 1 | Refresh |

	Sessions	Action
	blocked / 299	Unblock

3.7.9 Trace Route

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

Diagnostics >> Trace Route

Trace Route

Host / IP Address:

Result | Clear |

Ping through	Use the drop down list to choose the interface that you want to ping through.
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.

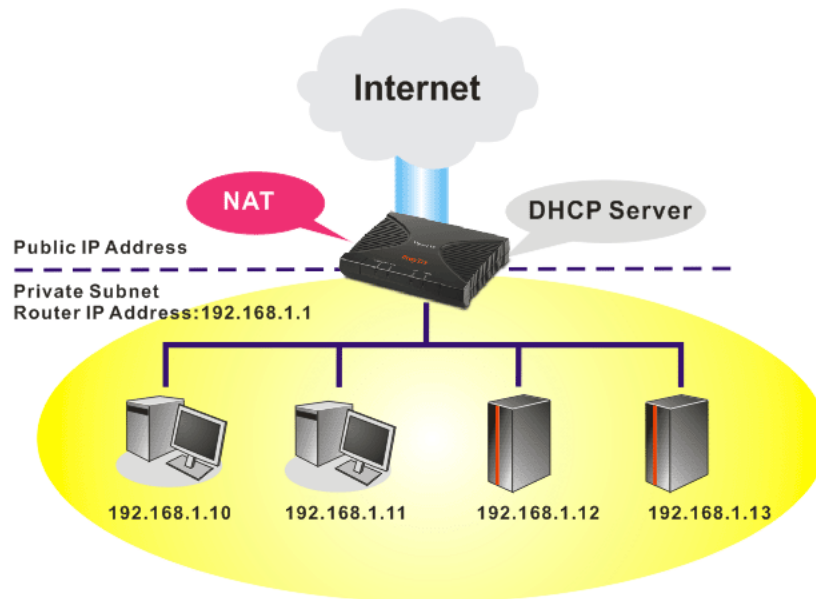
This page is left blank.

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 router private IP address/Subnet Mask is 192.168.1.1/255.255.255.0. The built-in DHCP server is enabled so it assigns every local NATed host an IP address of 192.168.1.x starting from 192.168.1.10.



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

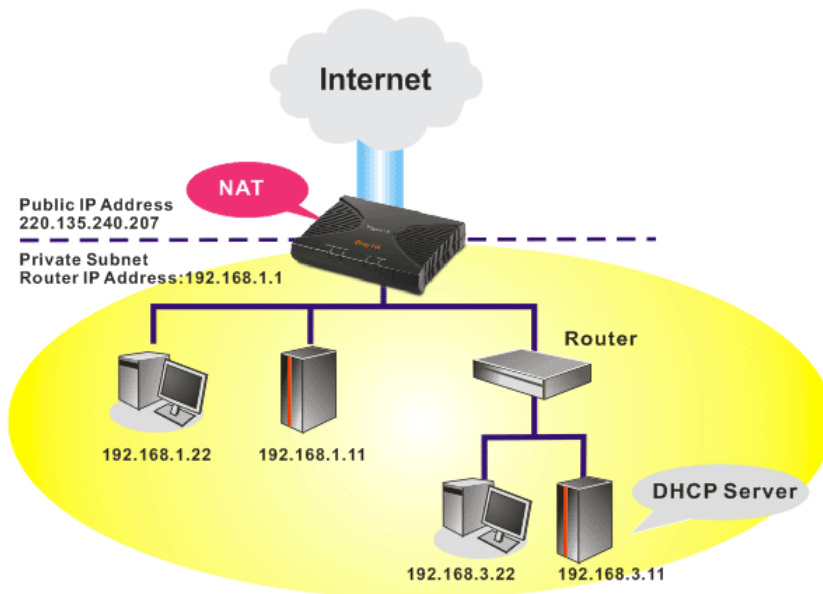
LAN >> General Setup

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: 192.168.1.1	Relay Agent: <input type="radio"/> 1st Subnet <input type="radio"/> 2nd Subnet
Subnet Mask: 255.255.255.0	Start IP Address: 192.168.1.10
	IP Pool Counts: 50
	Gateway IP Address: 192.168.1.1
	DHCP Server IP Address for Relay Agent: []

OK

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



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

LAN >> General Setup

Ethernet TCP / IP and DHCP Setup

LAN IP Network Configuration		DHCP Server Configuration	
For NAT Usage		<input type="radio"/> Enable Server <input checked="" type="radio"/> Disable Server	
IP Address	<input type="text" value="192.168.1.1"/>	Relay Agent: <input type="radio"/> 1st Subnet <input type="radio"/> 2nd Subnet	
Subnet Mask	<input type="text" value="255.255.255.0"/>	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="192.168.1.1"/>
		DHCP Server IP Address for Relay Agent	<input type="text" value="192.168.3.11"/>

OK

4.2 Upgrade Firmware for Your Router

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

1. Insert CD of the router 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

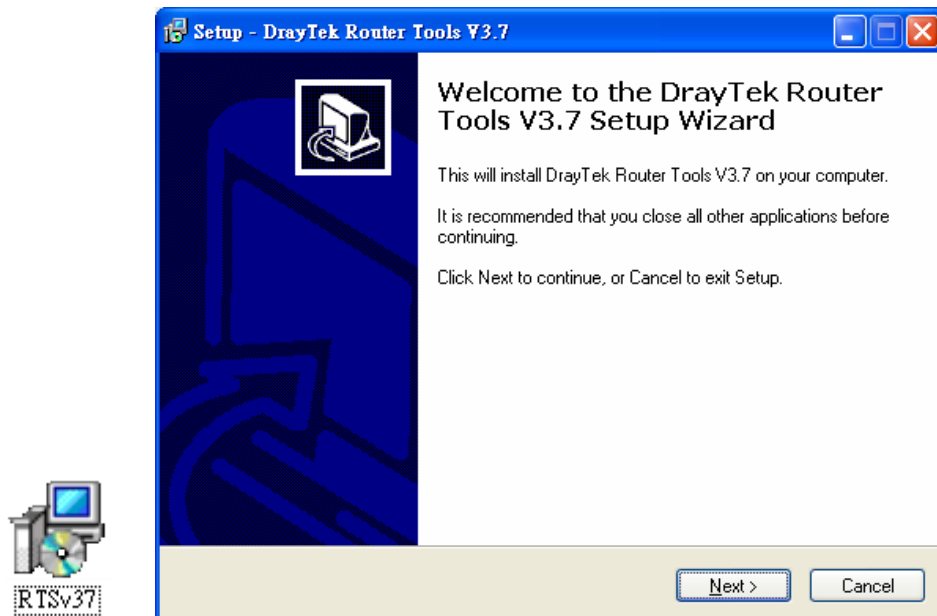
Install Now!

4. The file **RTSxxx.exe** will be asked to copy onto your computer. Remember the place of storing the execution file.

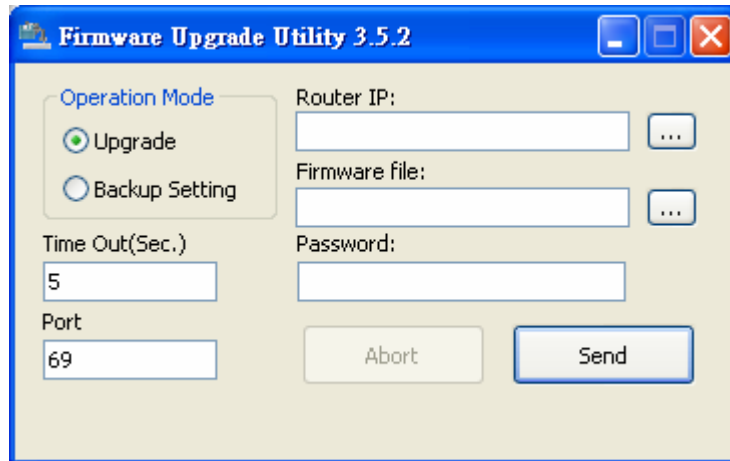
- Go to **www.draytek.com** to find out the newly update firmware for your router.
- Access into **Support Center >> Downloads**. Find out the model name of the router and click the firmware link. The Tools of Vigor router will display as shown below.

Tools Name	Released Date	Version	OS	Support Model	Download
Router Tools	28/03/2007	3.7	MS-Windows	All Model	zip
Smart VPN Client	18/08/2006	3.2.6	MS-Windows	All Model	zip
Smart VPN Client	21/06/2007	3.2.6	MS-Vista	All Model	zip
LPR	27/06/2005	1.0	MS-Windows	For Print Function	zip
VTA	15/09/2005	2.8	Windows2000/XP	For ISDN Model	zip
DialPlan	26/01/2006	2.5_lite	MS-Windows	For VoIP Model	zip

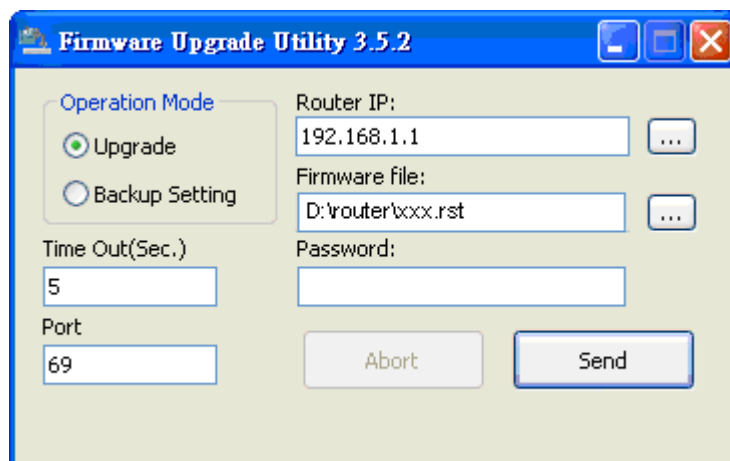
- Choose the one that matches with your operating system and click the corresponding link to download correct firmware (zip file).
- Next, decompress the zip file.
- Double click on the icon of router tool. The setup wizard will appear.



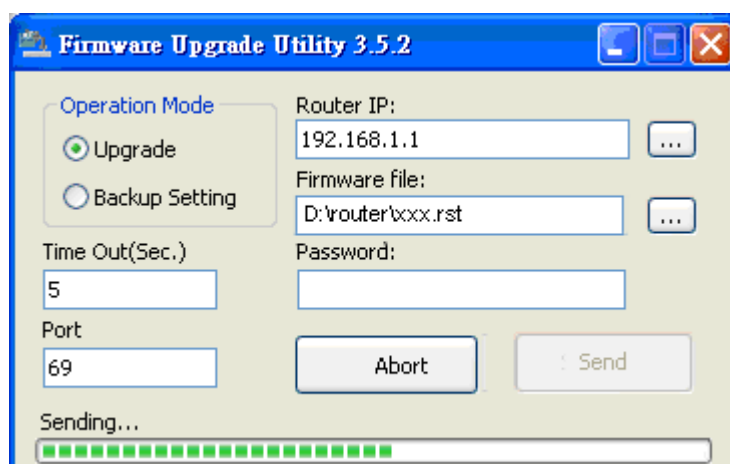
- Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.
- From the **Start** menu, open **Programs** and choose **Router Tools XXX >> Firmware Upgrade Utility**.



12. Type in your router 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 router 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 router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the router still cannot run normally, it is the time for you to contact 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 WAN/LAN cable connections.
Refer to “**2.1 Hardware Installation**” for details.
2. Turn on the router. Make sure the **POWER LED** and the correspondent **LAN LED** are bright.
3. If not, it means that there is something wrong with the hardware status. Simply back to “**2.1 Hardware Installation**” to execute the hardware installation again. And then, try again.

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

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

For Windows

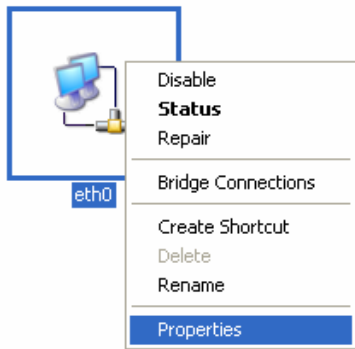


The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.draytek.com.

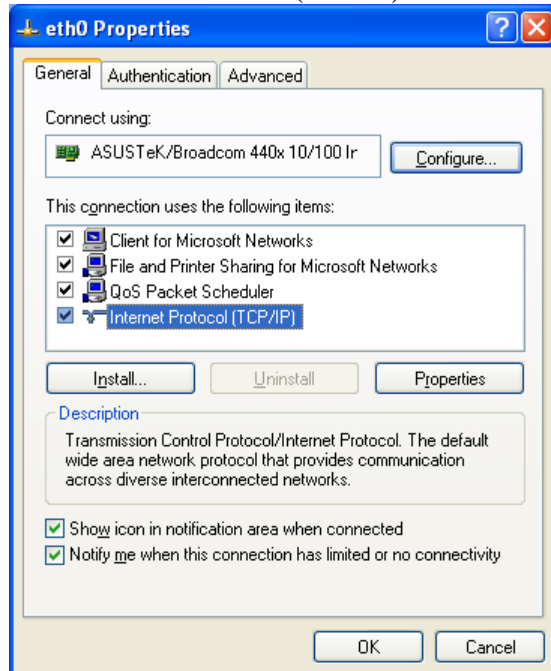
1. Go to Control Panel and then double-click on Network Connections.



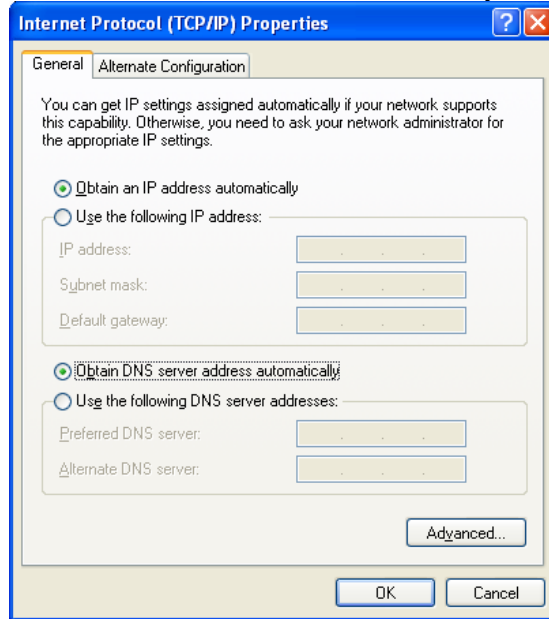
2. Right-click on Local Area Connection and click on Properties.



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

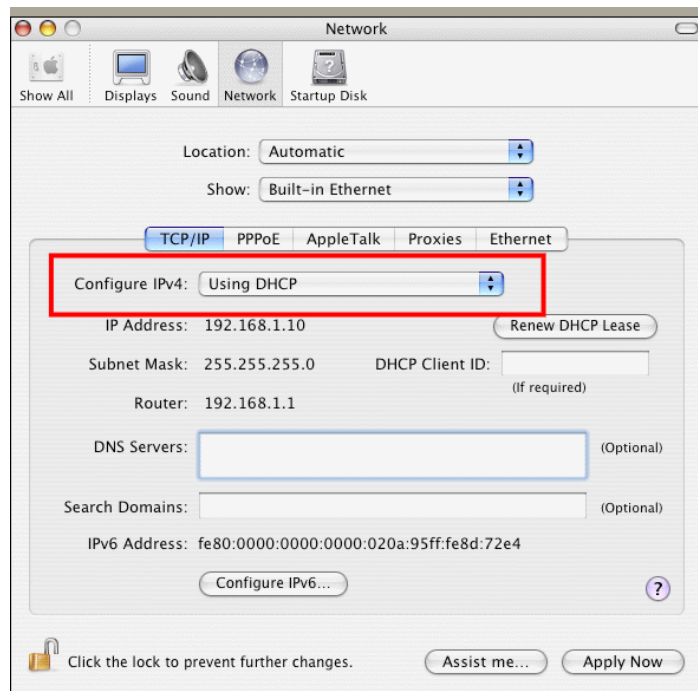


4. Select Obtain an IP address automatically and Obtain DNS server address automatically.



For MacOs

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



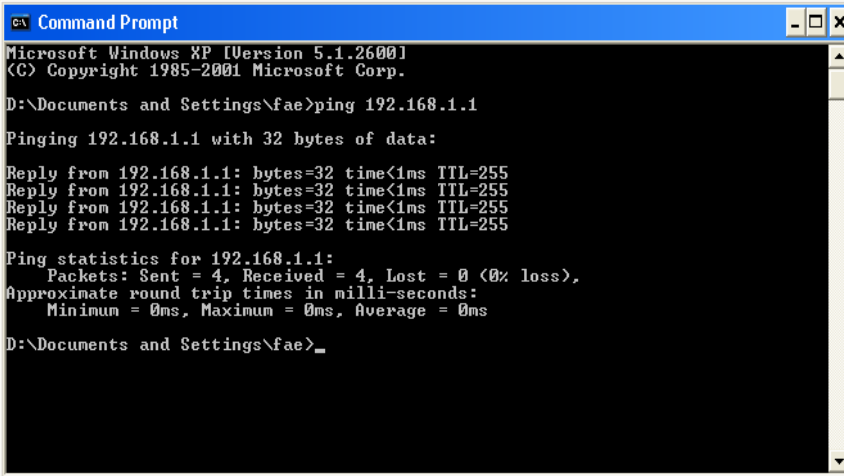
5.3 Pinging the Router from Your Computer

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

Please follow the steps below to ping the router correctly.

For Windows

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



```
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

PPPoE/PPPoA Client Enable Disable

DSL Modem Settings

VPI: 0
VCI: 33
Encapsulating Type: LLC/SNAP
Protocol: PPPoE
Modulation: Multimode

PPPoE Pass-through

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

ISP Access Setup

ISP Name:
Username:
Password:
PPP Authentication: PAP or CHAP
 Always On
Idle Timeout: 180 second(s)
IP Address From ISP WAN IP Alias
Fixed IP: Yes No (Dynamic IP)
Fixed IP Address:
 Default MAC Address
 Specify a MAC Address
MAC Address: 00 . 50 . 7F . 97 . 2A . 3C
Index(1-15) in **Schedule** Setup:
=> , , ,

OK

For MPoA Users

1. Check if the **Enable** option for Broadband Access is selected.

MPoA (RFC1483/2684) Mode

MPoA (RFC1483/2684) Enable Disable

DSL Modem Settings

Encapsulation: 1483 Routed IP LLC

VPI: 0

VCI: 34

Modulation: Multimode

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: 172.16.3.147

Subnet Mask: 255.255.0.0

Gateway IP Address: 172.16.3.4

Bridge Mode

Enable Bridge Mode

Default MAC Address

Specify a MAC Address

MAC Address: 00.50.7F:97.2A.3C

DNS Server IP Address

Primary IP Address:

Secondary IP Address:

OK

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**.

5.5 Backing to Factory Default Setting If Necessary

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



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

Software Reset

You can reset the router 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 router will return all the settings to the factory settings.

System Maintenance >> Reboot System

Reboot System

Do You want to reboot your router ?

Using current configuration
 Using factory default configuration

OK

Hardware Reset

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

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

5.6 Contacting Your Dealer

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